ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 67-78

Michał BALASA [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

CZY NASZE DANE W CHMURZE SĄ BEZPIECZNE?

Błyskawiczny rozwój technologii oprogramowania oraz zwiększenie wydajności urządzeń przyczynia się do tworzenia nowoczesnych rozwiązań problemów, z którymi borykają się korporacje, firmy jak i zwykli użytkownicy chmury. Obecnie większość przedsiębiorstw nie wyobraża sobie pracy bez wykorzystania chmury do przechowywania swoich danych. Jednak jednym z największych problemów wykorzystania chmury to jej bezpieczeństwo. W artykule przedstawiono modele usług wraz z modelem rozmieszczenia chmur oraz rodzaje ataków.

Słowa kluczowe: chmura obliczeniowa, bezpieczeństwo, ataki

1. Czym jest „*Cloud Computing*”?

Wykorzystanie słowa chmura *(ang. Cloud)* dla opisania pomysłu Cloud Computingu nie jest przypadkowe. Chmura kojarzy się ze środowiskiem, czyli dostępnością. W biznesie liczy się przede wszystkim łatwość dostępu do danych, usług, aplikacji itp. Większość instytucji nie interesuje jak przebiega przetwarzanie w chmurze, a jej efekt końcowy, czyli gotowa platforma z naszymi aplikacjami i danymi. Interesujące jest co uzyskamy wykorzystując technologię Cloud Computingu i koszt tej usługi. Technologia chmury powinna być dostępna na żądanie podobnie jak energia elektryczna, gaz czy dostęp do źródeł wody [1].

2. Modele usług chmury obliczeniowej

Każdy użytkownik ma odrębne potrzeby i zastosowania dla chmury obliczeniowej. Jedni potrzebują gotowych aplikacji, niektórzy potrzebują systemu

[1] Autor do korespondencji: Michał Balasa, Politechnika Rzeszowska, Zakład Systemów Złożonych, adres e-mail: mbalasa123@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

operacyjnego, aby móc tworzyć własne aplikacje inni zaś potrzebują jedynie zasobów sprzętowych, żeby implementować własne rozwiązania systemowe. Wybiegając naprzeciw wymaganiom konsumentów firmy wprowadziły podział chmur obliczeniowych na trzy główne modele udostępniania usług: SaaS (ang. *Software as a Service*), PaaS (ang. *Platform as a Service*), IaaS (ang. *Infrastructure as a Service*) [2].

Wykorzystując oprogramowanie jako usługę *(ang. Software as a Service)* użytkownik uzyskuje dostęp do gotowej aplikacji poprzez przeglądarkę internetową lub gotowego programu. Korzystający nie musi zarządzać lub sterować infrastrukturą chmury, a nawet niektórych funkcji aplikacji z wyjątkiem spersonalizowanych ustawień konfiguracyjnych. Dużą zaletą tego modelu jest zniwelowanie kosztów zatrudniania wyspecjalizowanych osób w zakresie serwisu IT. Przykładem usługi SaaS jest Google Apps udostępniający pakiet aplikacji biurowych, kalendarz, pocztę mailową oraz serwis społecznościowy Google+. Schemat odpowiedzialności modelu SaaS przedstawiono na rys. 1. [2].

Rys. 1. Schemat odpowiedzialności modelu SaaS

Fig. 1. Responsibility scheme of the SaaS model

Rys. 2. Schemat odpowiedzialności modelu PaaS

Fig. 2. Responsibility scheme of the PaaS model

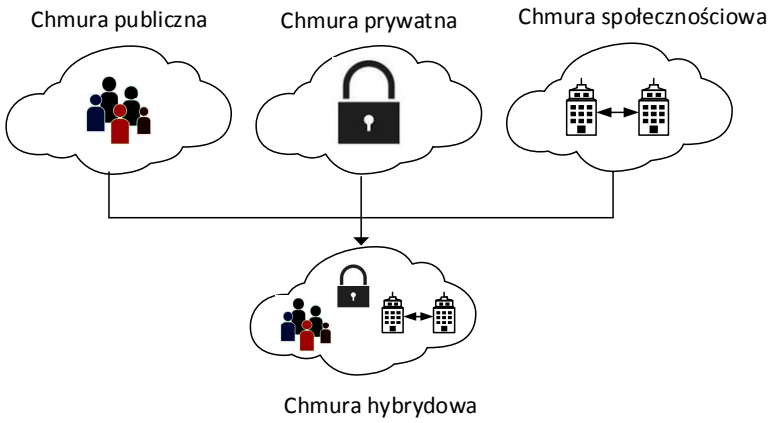
Wykorzystując platformę jako usługę *(ang. Platform as a Service)* użytkownik uzyskuje dostęp do całej usługi – najczęściej jest to zainstalowany system operacyjny z bazą danych. Deweloperzy oprogramowania oraz aplikacji internetowych mogą tworzyć i uruchamiać swoje oprogramowanie bez konieczności zakupu i serwisowania urządzeń fizycznych, a także infrastruktury sieciowej czy programowej. Przykładem usługi PaaS jest Microsoft Azure udostępniający swoje gotowe rozwiązania systemowe użytkownikom chcącym tworzyć aplikacje na systemie firmy Microsoft. Schemat odpowiedzialności modelu PaaS przedstawiono na rys. 2. [2].

W modelu infrastruktura jako usługa *(ang. Infrastructure as a Service)* użytkownik uzyskuje dostęp do gotowych zasobów obliczeniowych oraz infrastruktury sieciowej. Odbiorca może wdrażać dowolne oprogramowanie, które

może zawierać systemy operacyjne oraz aplikacje. Może także kontrolować systemy operacyjne, magazyny danych, a także zainstalowane oprogramowanie, lecz nie może zarządzać infrastrukturą chmury i ma ograniczony dostęp do kontroli ustawień sieci (np. Zapory sieciowej hosta) [2]. Przykładem usługi IaaS jest Amazon Elastic Compute Cloud, która pozwala na tworzenie własnych obrazów maszyn wirtualnych, dodawanie własnych instancji oraz zarządzanie nimi. Schemat odpowiedzialności modelu PaaS do funkcjonalności, za które odpowiada użytkownik wymienia: *Aplikacje, Środowisko, Bezpieczeństwo, Bazy danych oraz System operacyjny*. Pozostałe funkcje (*Wirtualizacja*, Serwery, *Pamięć masowa* i *Sieć* to odpowiedzialność dostawcy.

3. Modele rozmieszczenia chmury obliczeniowej

- **Chmura prywatna** (ang. *Private Cloud*) umiejscowiona jest najczęściej na terenie firmy, która ją wykorzystuje aby zapewnić najwyższe bezpieczeństwo danych. Chmura ta jest wykorzystywana oraz zarządzana przez jedną organizację, lecz w wyjątkowych przypadkach dopuszcza się możliwość umiejscowienia chmury w firmie zewnętrznej. Jedyny dostęp do zasobów chmury może mieć firma wykupująca usługę. Często do zaprojektowania chmury wykorzystywana jest istniejąca infrastruktura firmy.
- **Chmura publiczna** (ang. *Public Cloud*) w przeciwieństwie do chmury prywatnej umiejscowiona jest w firmie zewnętrznej. Organizacja wykupująca ofertę chmury publicznej nie musi być wyposażona w serwerownie, oprogramowanie jak również infrastrukturę, ponieważ jest własnością dostawcy, który odpowiada także za jej zarządzanie. Klient łącząc się poprzez sieć za odpowiednią opłatą uzyskuje dostęp do aplikacji lub zasobów sprzętowych chmury. Chmury publiczne cechują się większą podatnością na ataki z zewnątrz.
- **Chmura społecznościowa** (ang. *Community Cloud*) wykorzystywana jest do komunikacji grup pracujących nad wspólnym projektem, zadaniem lub celem. Znajduje zastosowanie w pojedynczych organizacjach jak i w kilku firmach, które łączą wspólne cele biznesowe. Chmurą zarządza jedna z organizacji wchodząca w skład chmury lub przez firmę zewnętrzną.
- **Chmura hybrydowa** (ang. *Hybrid Cloud*) jest połączeniem chmury publicznej, prywatnej i społecznościowej. Łącząc kilka chmur zachowujemy odrębność każdej z nich, umożliwiając zabezpieczoną komunikację, a także udostępnianie wybranych zasobów. Obecnie jest najczęściej wybieranym modelem przez przedsiębiorstwa ze względu na jej wszechstronność zastosowania – najważniejsze dane przechowujemy w chmurze prywatnej, dane mniej newralgiczne przechowujemy w chmurze publicznej.



Rys. 3. Model rozmieszczenia chmur

Fig. 3. Cloud deployment model

4. Bezpieczeństwo chmury obliczeniowej

Chmura obliczeniowa z założenia umożliwia dostęp do swoich zasobów z każdego miejsca oraz w każdej chwili przez wiele osób jednocześnie. Jednak z łatwością dostępu do chmury łączą się problemy z jej bezpieczeństwem co jest najczęstszym powodem rezygnacji z jej wdrożenia w firmie. Zdecydowana większość przedsiębiorstw nie wyobraża sobie aby ich dane wyciekły poza „mury" firmy. Użytkownicy wybierając oferty chmur obliczeniowych od różnych dostawców najczęściej wybierają dostawców w zależności od jakości bezpieczeństwa ich danych jak również ceny, którą proponują firmy w zamian za zasady bezpieczeństwa. Wiele publikacji uczula odbiorców cloud computingu na to aby na pierwszym miejscu stawiali bezpieczeństwo swoich danych. Największe zagrożenie upublicznienia danych stwarza chmura publiczna w modelu Software as a Service. Wszystkie dane oraz usługi w tym modelu są pod całkowitą kontrolą firmy oferującej usługę – provider zgodnie z umową zawartą z klientem musi zapewnić bezpieczeństwo całej infrastruktury sprzętowej jak i programowej [3].

Największe bezpieczeństwo naszych danych zapewnia chmura prywatna o modelu IaaS, ponieważ o bezpieczeństwo danych dba organizacja, która wykorzystuje daną chmurę. Dane z wykorzystanych usług nie są przekazywane do organizacji zewnętrznych, jednak zaprojektowanie tego modelu chmury wymaga od nas większych nakładów finansowych. Za bezpieczeństwo chmury (w zależności od wielkości instytucji) tzn. jej bezawaryjne działanie i zabezpieczenie transmisji danych odpowiedzialna jest grupa wykwalifikowanego personelu. Kolejną potrzebą jest inwestycja sporych środków finansowych na stwo-

rzenie własnych punktów przechowywania danych (serwerownie, infrastruktura sieciowa itd.).

W przypadku wdrożenia nowej usługi najczęściej nie wystarczy obecna infrastruktura, a modernizacja może się opłacić jeżeli projektant odpowiednio wyskalował sieć na przyszłe rozbudowy [3].

5. Rodzaje ataków na chmurę obliczeniową

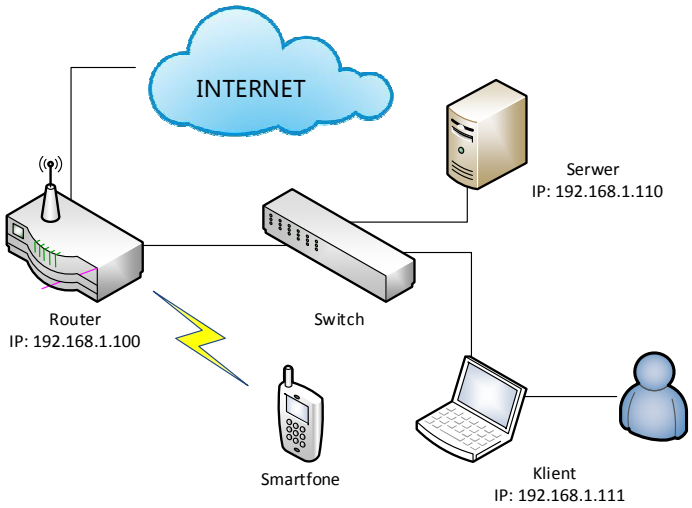
Zabezpieczenie chmury jest bardzo trudnym zadaniem, ponieważ na bezpieczeństwo chmury ma wpływ wiele czynników tzn. zaczynając od zabezpieczenia fizycznego poprzez politykę bezpieczeństwa w przedsiębiorstwie korzystającym z usługi przetwarzana w chmurze, zatem jest bardzo wiele możliwości potencjalnych sposobów zaatakowania chmury [4].

- **Application Attack** - jak sama nazwa wskazuje jest skierowany w aplikację. W celu jej zaatakowania tworzony jest exploit, który wykorzystuje luki w przestarzałym oprogramowaniu, aby uzyskać dostęp do aplikacji, która nie jest uruchomiona. Przykładowym i najbardziej popularnym tego typu atakiem jest przepełnienie bufora na stosie.
- **Brute Force** - atak służy do łamania haseł zabezpieczających chmurę. Polega na podjęciu dużej ilości prób złamania hasła dostępowego. Dobrym zabezpieczeniem przed tego typu włamaniem jest ograniczenie prób logowania z blokadą czasową. W ten sposób w 2014 roku złamano zabezpieczenia chmur firmy Apple uzyskując dostęp do prywatnych zasobów najsłynniejszych celebrytów.
- **Malware/botnet activity** - atak skierowany głównie w duże korporacje polegający na rozprzestrzenianiu szkodliwego oprogramowania na komputerach niszcząc lub pobierając informację jak również tworząc drogi dostępowe do komputera (ang. *back door*). Urządzenia infekowane są poprzez atak bezpośredni lub spam mailowy.
- **Misconfiguration** - atak wykorzystuje błędy w konfiguracji sieci, podłączonych komputerów oraz aplikacji. Przyczyną ataków jest brak zainstalowanych najnowszych poprawek, a także niedbałość administratorów sieci, ponieważ błędne skonfigurowanie aplikacji może spowodować utworzenie luki w systemie operacyjnym czyniąc go łatwym celem. Z roku na rok staje się coraz mniej spotykanym atakiem, ponieważ administratorzy maja coraz większą wiedzę na temat bezpieczeństwa i są wyczuleni na aktualizację oprogramowania.
- **Reconnaissance i Vulnerability scans** - do rozpoczęcia powyższych ataków wystarczy bardzo prosty i łatwo dostępny program do podsłuchu i skanowania sieci. Jednak wystarczy zaktualizowane oprogramowanie antywirusowe, aby ustrzec się tego rodzajów ataku.

- **Web Application Attack** - atak skierowany na aplikacje webowe jest jednym z najniebezpieczniejszych ataków, ponieważ w łatwy sposób uzyskuje dostęp do aplikacji jak również jest bardzo ciężki do powstrzymania. Wystarczy zainstalować odpowiednie oprogramowanie (np. HAVIJ), aby wykonać atak SQL Injection, które jest najpopularniejszym rodzajem ataku na aplikacje internetowe.

6. Test chmur do przechowywania danych

Test wydajności chmur przeprowadzono dla operacji przesyłania pliku o rozszerzeniu .7z (ok. 130 MB), 32 zdjęć JPEG (100 MB) oraz pobraniu pliku .7z, a także 32 zdjęć JPEG wcześniej przesłanych do chmury. W celu otrzymania dokładniejszych wyników testu, każdą procedurę powtórzono 10 krotnie, policzono z nich średnią arytmetyczną oraz ustawiono pobieranie danych dla Internetu jak również sieci lokalnej na poziomie pobierania i wysyłania plików – 10 Mbit/s.



Rys. 4. Topologia testowa dla przesyłania danych

Fig. 4. Test topology for data transfer

Eksperymenty przeprowadzono na przeglądarce Google Chrome 51.0.2704.79 oraz łączu internetowym osiągającym średnio wartość odbierania i wysyłania pakietów na poziomie 25 Mbit/s. Aby ograniczyć prędkość łącza internetowego/lokalnego wykorzystano program NetLimiter 4. Aby obliczyć czas potrzebny na pobranie/wysłanie pliku użyto programu Wireshark 2.0.4.

Na rysunku 4. przedstawiono topologię na której zostały przeprowadzone testy, a w tabeli 1 zestawiono otrzymane rezultaty.

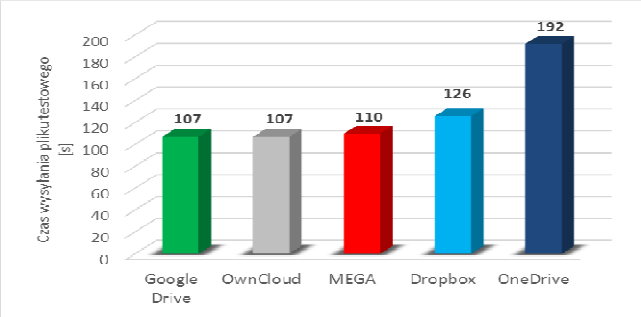
Tabela 1. Wyniki testów dla ograniczonego ruchu – 10 Mbit/s
Table 1. Test results for limited traffic – 10 Mbit/s

10 Mbit/s	Wysyłanie pliku 7z 130 MB	Wysyłanie 32 zdjęć JPEG 100 MB	Pobieranie pliku 7z 130 MB	Pobieranie 32 zdjęć JPEG 100 MB
Dropbox	Test 1: 127s Test 2: 126s … Test 10: 126s **Średnia: 126s**	Test 1: 143s Test 2: 145s … Test 10: 146s **Średnia: 145s**	Test 1: 107s Test 2: 108s … Test 10: 108s **Średnia: 108s**	Test 1: 85s Test 2: 85s … Test 10: 85s **Średnia: 85s**
Google Drive	Test 1: 108s Test 2: 107s … Test 10: 107s **Średnia: 107s**	Test 1: 105s Test 2: 106s … Test 10: 105s **Średnia: 105s**	Test 1: 108s Test 2: 107s … Test 10: 108s **Średnia: 108s**	Test 1: 96s Test 2: 96s … Test 10: 97s **Średnia: 96s**
MEGA	Test 1: 111s Test 2: 109s … Test 10: 111s **Średnia: 110s**	Test 1: 102s Test 2: 101s … Test 10: 104s **Średnia: 102s**	Test 1: 114s Test 2: 114s … Test 10: 115s **Średnia: 114s**	Test 1: 107s Test 2: 106s … Test 10: 105s **Średnia: 106s**
OneDrive	Test 1: 192s Test 2: 197s … Test 10: 187s **Średnia: 192s**	Test 1: 85s Test 2: 86s … Test 10: 86s **Średnia: 86s**	Test 1: 107s Test 2: 107s … Test 10: 106s **Średnia: 107s**	Test 1: 170s Test 2: 173s … Test 10: 175s **Średnia: 173s**
OwnCloud	Test 1: 106s Test 2: 107s … Test 10: 107s **Średnia: 107s**	Test 1: 82s Test 2: 82s … Test 10: 82s **Średnia: 82s**	Test 1: 108s Test 2: 107s … Test 10: 107s **Średnia: 82s**	Test 1: 87s Test 2: 88s … Test 10: 87s **Średnia: 87s**

6.1. Test wysyłania pliku 7z – ograniczenie ruchu 10 Mbit/s

Doświadczenie zostało przeprowadzone poprzez wysyłanie skompresowanego filmu z wykorzystaniem kompresji danych 7z. Najlepiej z zadaniem poradziły sobie chmury Google Drive, ownCloud, które wysłały pliki w czasie 107

sekund. Najgorszy rezultat uzyskała chmura OneDrive (czas przesyłania wyniósł 192 sekundy) prawdopodobnie przez słabą współpracę z plikami o 7z. Różnica pomiędzy najlepszym i najgorszym wynikiem wyniosła 85 sekund. Na rysunku 5. przedstawiono porównanie średniego czasu wysyłania pliku. Kolory na wykresie oznaczają kolor przewodni producenta chmury.

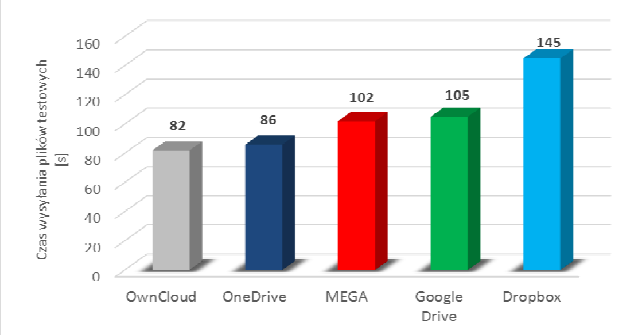


Rys. 5. Wysyłanie pliku 7z o rozmiarze 130 MB - 10 Mbit/s

Fig. 5. Sending 7z file of size 130 MB - 10 Mbit/s

6.2. Test wysyłania 32 zdjęć JPEG – ograniczenie ruchu 10 Mbit/s

Kolejny test został przeprowadzony z wykorzystaniem przesyłania 32 zdjęć o rozszerzeniu JPEG zrzuconych do jednego folderu, lecz nieskompresowanych, aby sprawdzić opcje kolejkowania poszczególnych platform. Najszybciej zdjęcia zostały przesłane w chmurze OwnCloud.



Rys. 6. Wysyłanie 32 zdjęć JPEG o rozmiarze 100 MB

Fig. 6. Sending 32 JPEG images of size 100 MB

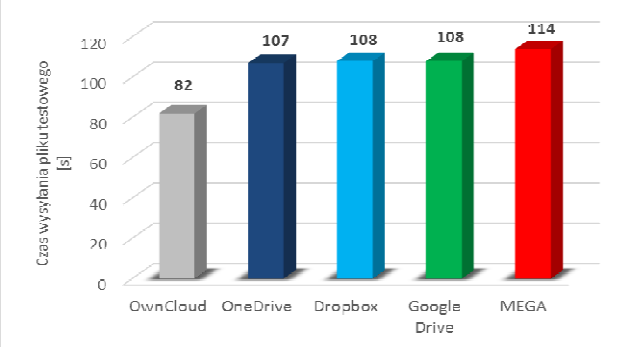
Do przesłania danych wystarczyło 82 sekundy. Najwolniej swoje zadanie wykonała chmura Dropbox, ponieważ po każdym przesłanym zdjęciu indeksowała pliki powodując opóźnienia w wysyłaniu (czas przekazywania – 145 sekund), jednak należy wyróżnić indeksowanie plików także jako zaletę, ponie-

waż pliki są dokładnie przesyłane do chmury zapewniając dokładność w przekazywaniu plików z komputera klienta na serwer. Różnica czasowa pomiędzy najlepszym i najgorszym rezultatem wyniosła 63 sekundy. Na rysunku 6. przedstawiono porównanie średniego czasu przekazywania zdjęć.

6.3. Test pobierania pliku 7z – ograniczenie ruchu 10 Mbit/s

Eksperyment wykonano za pomocą pobierania skompresowanego filmu z wykorzystaniem kompresji danych 7z. Chmura ownCloud pobrała plik w czasie 82 sekund, czyli najszybciej z testowanych rozwiązań. Pozostałe chmury uzyskały bardzo zbliżone rezultaty pobierania: OneDrive - 107 sekund, Dropbox – 108 sekund, Google Drive - 108 sekund i MEGA – 114 sekund. Różnica pomiędzy chmurami wyniosła 32 sekundy.

Na rysunku 7 przedstawiono porównanie średniego czasu pobierania pliku.

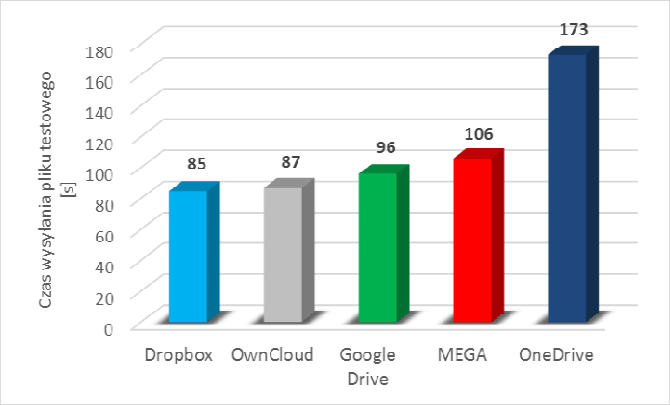


Rys. 7. Pobieranie pliku 7z o rozmiarze 130 MB - 10 Mbit/s

Fig. 7. Download 7z file size 130 MB - 10 Mbit/s

6.4. Test pobierania 32 zdjęć JPEG – ograniczenie ruchu 10 Mbit/s

Kolejny test został przeprowadzony za pomocą operacji pobierania 32 zdjęć o rozszerzeniu JPEG dodanych do jednego folderu. Dla dokładniejszego sprawdzenia pobierania zdjęć wybrano pobieranie razem z kompresją, więc platformy musiały dodatkowo skompresować zdjęcia. Wyniki eksperymentu wskazują, że chmura Dropobox osiągnęła najlepszy rezultat z czasem 85 sekund. O 2 sekundy wolnej pliki pobrano z platformy ownCloud. Najwolniej pliki pobrano z usługi OneDrive, ponieważ chmura bardzo długo „pakowała” pliki. Różnica pomiędzy najlepszym i najgorszym czasem wyniosła 88 s, czyli z chmury OneDrive dwukrotnie dłużej pobierano pliki niż z Dropboxa i OwnCloud. Na rysunku 8. przedstawiono porównanie średniego czasu pobierania zdjęć dla tego testu.



Rys. 8. Pobieranie 32 zdjęć JPEG o rozmiarze 100 MB - 10 Mbit/s

Fig. 8. Download 32 JPEG images of 100 MB - 10 Mbit/s

6.5. Porównanie bezpieczeństwa chmur do przechowywania danych

W celu przedstawienia różnic dotyczących bezpieczeństwa pomiędzy przedstawionymi rozwiązaniami stworzono tabelę 2. Porównanie bezpieczeństwa przeprowadzono dla chmur w darmowych pakietach. W tabeli 2. porównywano czy chmury mają możliwość weryfikacji dwuetapowej, zabezpieczenie SSL, rodzaj zabezpieczenie AES, czy indeksowane są pojedyncze pliki podczas przesyłania oraz możliwość przywracania usuniętych plików z kosza.

Tabela 2. Porównanie bezpieczeństwa chmur

Table 2. Comparison of cloud security

Nazwa dostawcy	Weryfikacja dwuetapowa	SSL	Rodzaj AES	Indeksowanie pojedynczych plików	Przywracanie plików z kosza
Dropbox	TAK	TAK	AES-256	TAK	TAK
Google Drive	TAK	TAK	AES-256	NIE	TAK
MEGA	NIE	TAK	AES-256	NIE	TAK
OneDrive	NIE	TAK	BRAK	NIE	TAK
OwnCloud	NIE	TAK	AES-256	NIE	TAK

Z przeprowadzonego porównania wynika że najbezpieczniejszym rozwiązaniem dla naszych plików jest wykorzystanie chmury Dropbox, a najmniej bezpieczną chmurą jest rozwiązanie firmy Microsoft – OneDrive.

7. Podsumowanie

Wykorzystanie chmury do przechowywania danych wiąże się z koniecznością wykorzystania sieci do przesłania danych (często bardzo ważnych lub prywatnych). Korzystając z rozwiązań chmury prywatnej mamy dużo większą szansę, że nasze dane nie wejdą w posiadanie osób trzecich, ponieważ cała infrastruktura opiera się na zasobach sprzętowych oraz topologii sieciowej naszej firmy. Rozwiązanie to jednak łączy się z dużymi kosztami utrzymania infrastruktury oraz kosztami przygotowania urządzeń, które umożliwią swobodne korzystanie z naszych danych. Chmura publiczna umożliwia nam dostęp do naszych danych z każdego miejsca, ponieważ za dystrybucję odpowiada firma zewnętrzna. Zatem za miesięczny/roczny abonament uzyskujemy dostęp do danych bez konieczności dbania o naszą infrastrukturę. Wiąże się to jednak z tym że firma zewnętrzna ma na swoich serwerach nasze dane, a my nie mamy wpływu na zabezpieczenia takiego serwera. Podczas ataku na serwery takiej firmy nasze dane mogą zdobyć osoby trzecie lub możemy je po prostu utracić. Przeglądając oferty oraz możliwości chmur musimy podjąć decyzję jak istotne będą przechowywane tam dane. Tworząc chmurę dla naszej firmy powinniśmy też zastanowić się na utworzeniem kopii zapasowej danych, które przesyłamy do chmury.

Decyzję o rodzaju wykorzystanej chmury należy podjąć po analizie ilości przesyłanych danych, ilości użytkowników wykorzystujących oprogramowanie oraz możliwości finansowych do utworzenia oraz utrzymania ewentualnej infrastruktury. Podczas wykorzystywania chmury należy pamiętać o przestrzeganiu podstawowych zasad bezpieczeństwa: przestrzegania zasad bezpiecznych haseł, posiadania aktualnego oprogramowania antywirusowego oraz zablokowanie dostępności osobom trzecim do własnego konta. Bezpieczeństwo naszych danych w większości przypadków zależy od nas i od tego w jaki sposób dbamy o ich zabezpieczenie.

Literatura

[1] Aljawarneh S.: *Cloud Computing Advancements in Design, Implementation and Technologies*, Isra University, Jordan 2013.
[2] Mell P., Grance T.: *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg 2011.
[3] Mather T., Kumaraswamy S., Latif S.: *Cloud Security and Privacy. An Enterprise Perspective on Risks and Comliance*, O'Reilly Media Inc. United States of America 2009.
[4] http://websecurity.pl/tag/chmura-zagrozenia/, [dostęp: 10.04.2017].

IS OUR DATA SAFE IN THE CLOUD?

S u m m a r y

Rapid development in software technology and increase in efficiency of devices lead to finding new solutions for problems that corporations, companies, as well as common users of the cloud faced for years. Currently, most companies cannot imagine working without the cloud, where their data can be stored. One of the biggest issues concerning the cloud is the safety of its usage. The article shows various service and deployment models along with types of attacks.

Keywords: computing cloud, cloud security, attacks on the cloud

DOI: 10.7862/re.2017.12

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017