Ekonomiczne Problemy Usług nr 123

ISSN: 1896-382X | www.wnus.edu.pl/pl/epu/
DOI: 10.18276/epu.2016.123-18 | strony: 193-201

PIOTR CZERWONKA, ŁUKASZ ZAKONNIK
Uniwersytet Łódzki[1]

BEZPIECZEŃSTWO PRYWATNYCH CHMUR OBLICZENIOWYCH **W KONTEKŚCIE** DYNAMICZNEGO ROZWOJU ICT

Streszczenie

Artykuł przedstawia ogólne trendy w rozwoju chmur obliczeniowych z naciskiem na aspekty bezpieczeństwa elektronicznego. Autorzy prezentują trzy trendy, które poprzez rozwój technologii chmurowych będą wpływać na ogólny poziom bezpieczeństwa systemów informatycznych w organizacjach. Przedstawiają również wyzwania stojące przed organizacjami, które będą chciały wdrażać technologie chmurowe w postaci prywatnych chmur obliczeniowych.
Słowa kluczowe: chmura obliczeniowa, open source, bezpieczeństwo.

Wprowadzenie

Chmura obliczeniowa jako rozwiązanie stosowane przez działy IT nie jest już czymś nowym. Właściwie wszystkie największe firmy oferujące rozwiązania informatyczne mają w zakresie swoich usług produkty powiązane z chmurą obliczeniową kierowane do szerokiej gamy odbiorców – poczynając od organizacji charakteryzujących się różnorodną wielkością, a na przeróżnie sprofilowanych użytkownikach indywidualnych kończąc.

Przez ostatnie kilka lat oprogramowanie obsługujące chmury obliczeniowe okrzepło i nabrało cech dojrzałego, dobrze umocowanego na rynku produktu. Użytkownicy często korzystają z usług oferowanych przez Amazon czy Microsoft, nawet nie zdając sobie z tego sprawy. Tendencją wzrostową charakteryzuje się rów-

[1] Piotr Czerwonka – Katedra Informatyki, Wydział Zarządzania; Łukasz Zakonnik – Katedra Informatyki Ekonomicznej, Wydział Ekonomiczno-Socjologiczny.

nież świadome wykorzystanie usług chmurowych – również w sektorze aplikacji dla przedsiębiorstw (trade.gov 2014). Chmura obliczeniowa z punktu widzenia marketingu jest często prezentowana jako wydajne i tanie rozwiązanie, które zmieni sposób spojrzenia na pracę typu klient – serwer. Taki model pracy to jednak nie tylko same zalety. Zmiana orientacji organizacji w stronę zasobów chmury obliczeniowe musi wziąć pod uwagę utratę kontroli nad danymi, nowe wyzwania dotyczące bezpieczeństwa i prywatności.

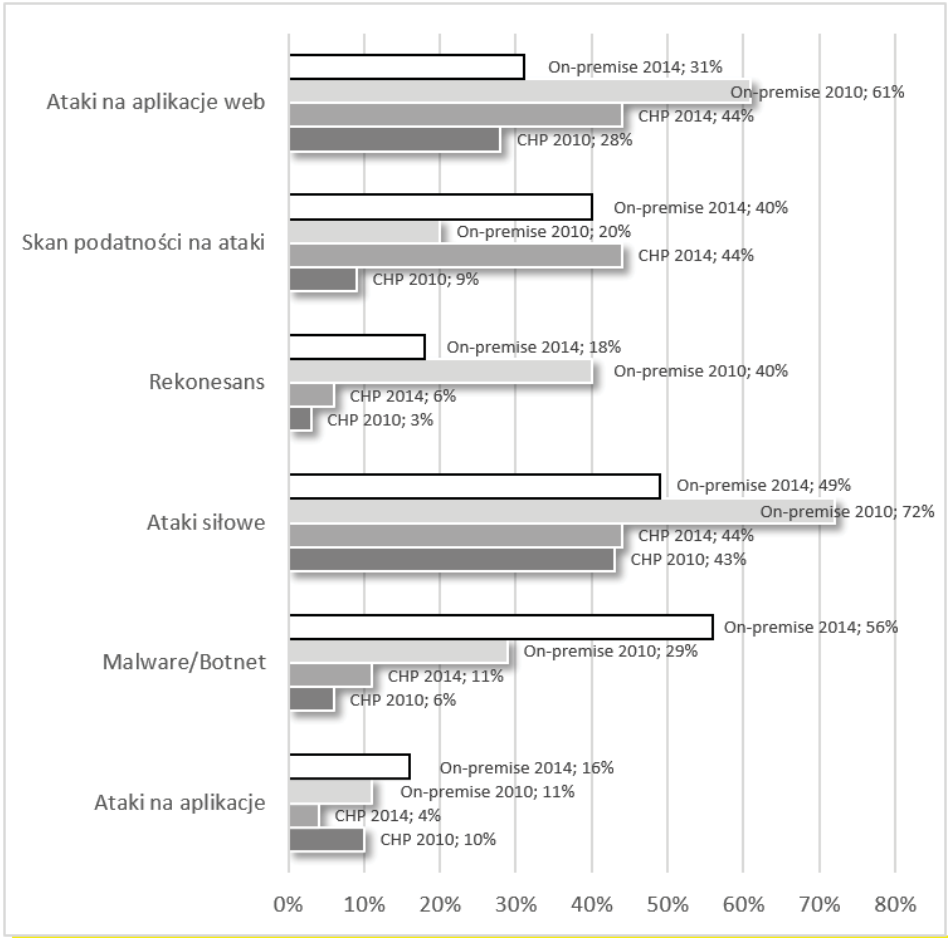
W przypadku organizacji, które nie mogą sobie pozwolić na umieszczenie danych w chmurze prywatnej, pozostaje możliwość wykorzystania potencjału rozwiązań chmurowych poprzez wdrożenie chmury publicznej lub hybrydowej. Nawet taki wybór wymaga jednak spojrzenia na aspekty dotyczące bezpieczeństwa infrastruktury IT.

1. Trzy oblicza chmury

Chmura obliczeniowa stała się popularną i w wielu przypadkach bardzo atrakcyjną alternatywą (Columbus 2014) dla tradycyjnego modelu przetwarzania danych opartego na posiadaniu własnego zaplecza serwerowego i całkowitej kontroli nad sposobem składowania i przetwarzania danych. W świadomości wielu użytkowników chmura ma status „niezdobytej twierdzy", zabezpieczonej przez najlepszych fachowców i bazującej na najnowocześniejszych rozwiązaniach sprzętowych (Gartner 2014). Być może nie jest to przekonanie całkowicie mylne, ale bez wątpienia systemy chmurowe mają swoje problemy.

W przypadku zagadnień dotyczących bezpieczeństwa i chmury obliczeniowej wyraźnie widać trzy zjawiska, które w znaczącym stopniu mogą wpływać na sposób jej postrzegania.

Pierwszym zjawiskiem jest wyraźna migracja wielu rodzajów zagrożeń dotyczących usług internetowych z tradycyjnych implementacji w stronę wdrożeń chmurowych. Popularyzacja rozwiązań chmurowych i przenoszenie do chmury zasobów użytkowników indywidualnych i organizacji w naturalny sposób wpłynęły na obranie usług chmurowych jako jednego z podstawowych celów cyberataków. Na rysunku 1 przedstawiono zmianę skali różnego rodzaju zagrożeń dotyczących bezpieczeństwa elektronicznego dla implementacji w siedzibach organizacji (on premise) i zasobów umieszczonych w chmurze obliczeniowej (CHP). Ze strony czynników atakujących zasoby elektronicznie wyraźnie wzrosło zainteresowanie aplikacjami webowymi umieszczonymi w chmurze i szukaniem potencjalnych luk w zabezpieczeniach aplikacji i systemów w chmurze. Charakterystyczna jest też intensyfikacja ataków typu malware na sieci komputerowe, które po przejęciu są często wykorzystywane do atakowania zasobów chmurowych.

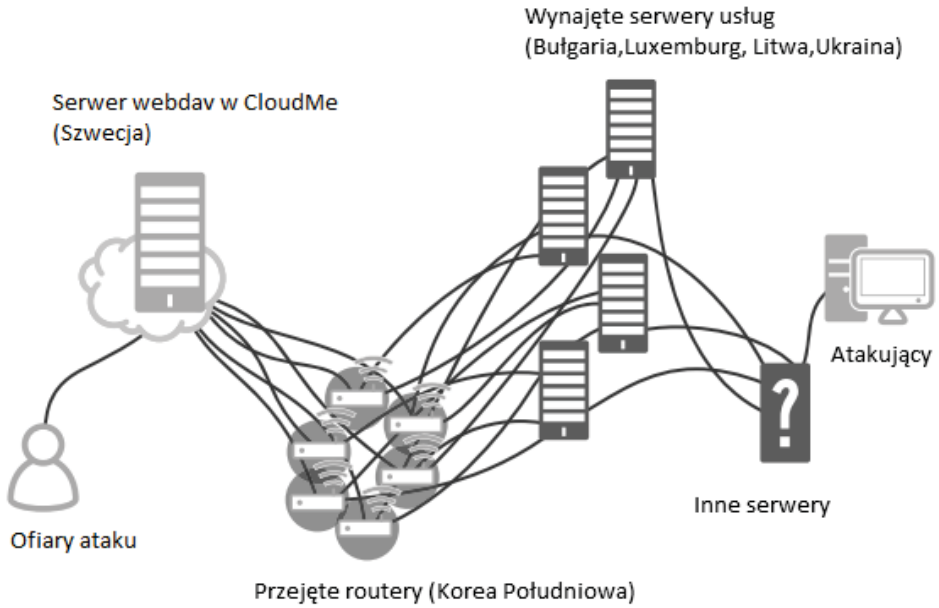


Rys. 1. Częstotliwość incydentów: ilość incydentów na jednego klienta w przypadku usług w chmurze i systemów własnych

Źródło: opracowanie własne na podstawie www.alertlogic.com.

Drugim zjawiskiem jest wykorzystanie zasobów chmury obliczeniowej do przeprowadzania lub koordynowania ataków na cele informatyczne. Potencjalnie nieograniczone zasoby obliczeniowe, duża elastyczność zasobowa i ogromna gama dostępnych usług (poczynając od zwykłych dysków sieciowych, a kończąc na kompletnych platformach deweloperskich, pozwalających na uruchamianie w sieci dowolnego kodu) dają wielkie możliwości podmiotom, które chciałyby ich użyć do szkodzenia innym użytkownikom sieci. Cechy chmury mogą być wykorzystane do przeprowadzania ataków na dużą skalę, ale co nawet ważniejsze, dają duże możliwości w komplikowaniu warstw ataku i ukrywaniu prawdziwej tożsamości atakującego. Jeden z najbardziej wysublimowanych i wykrytych przez organizacje zajmu-

jące się bezpieczeństwem sieciowym ataków został przeprowadzony z zaplanowanym i aktywnym wykorzystaniem produktu jednego z usługodawców chmury obliczeniowej (Fagerland i Grance 2015). W tym przypadku usługi chmury zostały użyte jako jeden z elementów kontrolujących komputery ofiar. Pewne standardowe ataki z zasobów chmurowych, jak masowe wysyłanie spamu, czy ataki DDOS, są łatwo wykrywalne przez tradycyjne mechanizmy usługodawcy i mogą zostać szybko zablokowane, ale opanowanie tego typu procederu wymaga długotrwałego śledztwa i kooperacji wielu organizacji i państw. Łatwo można sobie wyobrazić, że potencjał chmury obliczeniowej w tym zakresie nie został jeszcze wyczerpany.



Rys. 2. Uproszczona struktura mechanizmu ataku sieciowego wykrytego przez Blue Coat w 2014 roku

Źródło: (Fagerland i Grance 2015).

Trzecim zjawiskiem, które ze względów bezpieczeństwa zasługuje na uwagę, jest rozwój technologii chmur prywatnych i coraz częstsze implementacje tego typu rozwiązań w organizacjach (Weins 2015). Szukając połączenia lepszego wykorzystania zasobów, niezbędnej w obecnych czasach elastyczności funkcjonalności i utrzymania kontroli nad własnymi danymi, firmy mogą z zainteresowaniem spoglądać w stronę tego typu rozwiązań. Jest to tym prostsze, że oferta tego typu produktów jest bardzo szeroka, a w wielu przypadkach bazuje na rozwiązaniach open source, dzięki czemu można wykorzystać profesjonalne możliwości produktów takich jak OpenStack czy CloudFoundry bez ponoszenia wysokich

kosztów licencji. Daje to większe możliwości wypróbowania i zaznajomienia się z nową technologią.

Jest to jednak oprogramowanie o bardzo wysokim stopniu skomplikowania, którego wdrożenie, a co ważniejsze poprawne utrzymanie wymaga bardzo wysokich kwalifikacji.

2. Rozwój platform chmurowych typu open source a bezpieczeństwo

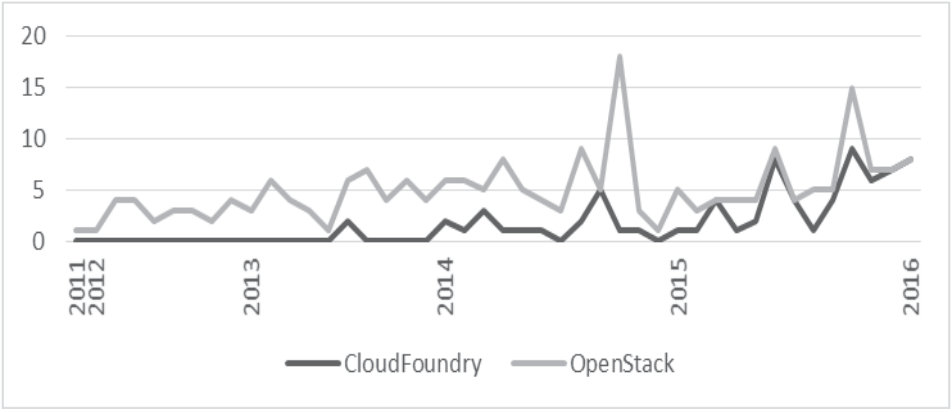
Zakładając, że nie ma oprogramowania pozbawionego wad i każdy system operacyjny (GFI 2014) każdego roku musi borykać się z licznymi usterkami, które mogą prowadzić nawet do krytycznych luk w mechanizmach bezpieczeństwa systemu, skupmy się na dwóch popularnych produktach. OpenStack i CloudFoundry to rozwiązania, które oferują odpowiednio platformę IaaS i PaaS w przestrzeni systemów chmurowych. Oba produkty bazują na dystrybucjach Linuxa i są tak bezpiecznie, jak tworzony kod sterujący mechanizmami chmury i odpowiednie jądro systemu (Prysmakou 2015). Biorąc pod uwagę przykład implementacji chmury obliczeniowej przy pomocy tych dwóch produktów i poziom jej komplikacji (Czerwonka i Zakonnik), warto zwrócić uwagę na poziom bezpieczeństwa i konieczność ich aktualizacji i monitorowania.

CloudFoundry i OpenStack spełniają wiele międzynarodowych wymagań dotyczących bezpieczeństwa informacji i posiadają liczne certyfikaty, które uprawniają do uruchamiania w ramach infrastruktury aplikacji bezpiecznie przetwarzających m.in. dane finansowe, np.:

- HIPAA,
- PCI DSS.

Same certyfikaty nie zabezpieczają jednak przed złą konfiguracją lub pozostawionymi lukami bezpieczeństwa. Na rysunku 3 przedstawiono liczbę wykrywanych i naprawianych błędów w usługach obu produktów, które mogły doprowadzić do poważnych naruszeń zabezpieczeń całej infrastruktury chmury zaimplementowanej przy pomocy tych rozwiązań.

Biorąc pod uwagę złożoność takich systemów, które stanowią środowisko składające się często z kilkudziesięciu i więcej serwerów fizycznych, dedykowanych routerów i przełączników, należy pamiętać, że proces ich aktualizacji jest nieporównywalnie bardziej skomplikowany niż w przypadku komputerów osobistych lub pojedynczych serwerów. System jest tak bezpieczny jak jego najsłabsze ogniwo. W przypadku chmury mamy do czynienia z setkami takich wrażliwych ogniw.



Rys. 3. Liczba wykrytych i naprawionych poważnych luk mechanizmów zabezpieczeń w OpenStack i CloudFoundry

Źródło: opracowanie własne na podstawie https://www.cvedetails.com/vulnerability-list/vendor_id-11727/Openstack.html i http://pivotal.io/security.

3. Wyzwania przed chmurami prywatnymi

Kwestie dotyczące zabezpieczeń chmury obliczeniowej były wielokrotnie poruszane w literaturze (Reed, Rezek i Simmonds 2011) i są dobrze znane, ale jest oczywiste, że wymagają procesu ciągłej aktualizacji, który powinien reagować na bardzo dynamiczny rozwój technologii i przekraczanie kolejnych barier funkcjonalności i dostępności. Szczególną uwagę warto zwrócić na pewne aspekty prywatnych implementacji i ich szczególne cechy w kontraście do chmury publicznej.

Różnice dotyczące bezpieczeństwa publicznych i prywatnych chmur można podzielić na trzy ogólne kategorie:

- biznesowe,
- prawne,
- techniczne.

Z punktu widzenia biznesowego należy pamiętać, że usługodawca chmury w ramach umowy zapewnia dokument SLA (ang. *Service Level Agreement*), który powinien gwarantować odpowiednie czynności w zakresie m.in.:

- skanowania infrastruktury pod kątem luk bezpieczeństwa,
- aplikowania poprawek i aktualizacji platformy,
- zagwarantowania ochrony antywirusowej,
- wykonywania kopii bezpieczeństwa danych,
- szyfrowania danych,
- zarządzania procedurami modyfikacji infrastruktury.

W przypadku chmury prywatnej wszystkie powyższe czynności należy wyegzekwować od działu IT odpowiedzialnego za utrzymanie chmury, co biorąc pod

uwagę zaawansowanie i komplikację implementacji, z pewnością może być dużym obciążeniem dla zasobów ludzkich i technicznych.

Z punktu widzenia obowiązującego prawa implementacja chmury prywatnej rozwiązuje wszystkie wątpliwości i dylematy, które w wielu przypadkach uniemożliwiają lub stawiają pod znakiem zapytania możliwość wykorzystania zasobów chmury publicznej, która wymyka się granicom państwowym i jurysdykcji poszczególnych krajów czy Unii Europejskiej (curia.europa.eu 2015). Pozostawiamy w ramach organizacji kontrolę nad bezpieczeństwem informacji i dostępem do danych. Wiemy również, gdzie znajdują się nasze dane, zarówno logicznie, jak i fizycznie.

Biznesowe i prawne rozważania dotyczące bezpieczeństwa informacji nie mogą się obyć bez warstwy technicznej, która do istniejących problemów dodaje wiele nowych elementów. Błędem jest twierdzenie, że implementacja chmurowa z założenia jest bezpieczniejsza niż tradycyjne wdrożenie. Z punktu widzenia technicznego chmura obliczeniowa to nic innego jak połączenie odpowiedniej skali zasobów sprzętowych, odpowiedniego oprogramowania, które umożliwia zautomatyzowane zarządzanie infrastrukturą i koncepcji efektywnego wykorzystania takich zasobów w nowy i atrakcyjny sposób. Taka infrastruktura – czy to prywatna, czy publiczna – boryka się jednak z problemami charakterystycznymi dla standardowych wdrożeń i do tego zwielokrotnionym efektem skali. Można do nich zaliczyć:

- złożoność i zabezpieczenie sieci wirtualnych (warstwa wirtualnych switchów, routerów, zaawansowanych firewalli) na warstwie odpowiadających urządzeń fizycznych;
- konieczność zabezpieczenia, konfiguracji i utrzymania setek wirtualnych serwerów w jednej lub w wielu serwerowniach;
- konieczność monitorowania, logowania i reagowania na incydenty w rozległej infrastrukturze setek serwerów i urządzeń, zarówno wirtualnych, jak i fizycznych;
- korelację monitorowanych danych z urządzeń fizycznych i wirtualnych;
- monitorowanie i zabezpieczenie hypervisorów odpowiedzialnych za pracę serwerów wirtualnych.

Potencjalnie możliwości wykorzystania są ogromne i mogą dać organizacjom zupełnie nowe możliwości rozwoju, ale mogą być też źródłem wielu problemów i wyzwań.

Podsumowanie

Zdaniem autorów ekspansja chmury obliczeniowej, a w tym implementacja chmur prywatnych, jest nieunikniona. Ich zastosowanie daje zbyt wiele atrakcyj-

nych możliwości dla podmiotów przetwarzających duże ilości danych (np. w zakresie e-commerce), aby łatwo z nich zrezygnować.

Obecnie pomimo intensywnego rozwoju są to technologie raczej hermetyczne, a proces uczenia się filozofii systemów chmurowych przez działy IT może trwać wiele lat. Taka konieczność wydaje się jednak nieunikniona. Rozwój takich systemów w ciągu najbliższych lat może doprowadzić do ich uproszczenia, radykalnego upowszechnienia i uproszczenia mechanizmów zarządzania. Obecnie opanowanie czynników technicznych może być jednak największą przeszkodą w zagwarantowaniu bezpieczeństwa tych implementacji i danych w nich przetwarzanych.

Literatura

1. (July 2015), *2015 Top Markets Report Cloud Computing, A Market Assessment Tool for U.S. Exporters*, http://trade.gov/topmarkets/pdf/ Cloud_Computing_ Top_Markets_Report.pdf.
2. Columbus, L. (2014), *IDC Predicts SaaS Enterprise Applications Will Be A $50.8B Market By 2018*, http://www.forbes.com/sites/louiscolumbus/2014/ 12/20/idc-predicts-saas-enterprise-applications-will-be-a-50-8b-market-by-2018.
3. Czerwonka P., Zakonnik Ł., *Ewolucja i perspektywy rozwoju prywatnych chmur obliczeniowych. Mity i fakty*, „Przedsiębiorczość i Zarządzanie", 16(9) (w druku).
4. Fagerland S., Grance W. (2015), *The Inception framework: Cloud Hosted APT*, https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2% 80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware.
5. Florian C. (2014), *Most vulnerable operating systems and applications in 2014*, http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/.
6. Meulen R., Rivera J. (2014), *Gartner Highlights the Top 10 Cloud Myths*, http://www.gartner.com/newsroom/id/2889217.
7. Prysmakou A. (2015), *Cloud Foundry Security Overview*, http://events. linuxfoundation.org/sites/events/files/slides/CFSummit_Security.pdf.
8. Reed A., Rezek C., Simmonds P. (2011), *Security guidance for critical areas of focus in cloud computing V3.0*, https://cloudsecurityalliance.org/download/ security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/.
9. Rovelli P. (2015), *Don't believe these four myths about Linux security*, https://blogs.sophos.com/2015/03/26/dont-believe-these-four-myths-about-linux-security/.
10. State of cloud security report, AlertLogic 2014, https://www.alertlogic.com/ resources/cloud-security-report-2014.
11. State of cloud security report, AlertLogic 2010, https://www.alertlogic.com/ resources/cloud-security-report-2010

12. Weins K. (2015), *Cloud Computing Trends: 2015 State of the Cloud Survey*, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey.
13. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 października 2015 roku, http://curia.europa.eu/juris/document/document.jsf?text=&docid= 169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031.

PRIVATE CLOUDS SECURITY IN THE CONTEXT OF ICT DYNAMIC DEVELOPMENT

Summary

The article presents general trends in the development of cloud computing with an emphasis on aspects of security. The authors present three trends that through the development of cloud computing technology will affect the overall safety level of information systems in organizations. The study also outlines the challenges facing organizations that wish to deploy cloud technologies in the form of private cloud computing.
Keywords: cloud computing, open source, security.

Translated by Piotr Czerwonka