MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY
UKRAINIAN FEDERATION OF INFORMATICS

PROCEEDINGS

OF THE IV INTERNATIONAL SCIENTIFIC CONFERENCE

ADVANCED INFORMATION SYSTEMS AND TECHNOLOGIES

AIST-2016

May 25 –27, 2016
Sumy, Ukraine

Cloud Computing Security Issues

Dmytro Panteliuk, Volodymyr Romaka
Lviv Polytechnic National University, Ukraine, panteliuk.dmytro@gmail.com

Abstract. Features of cloud services are described. Different models of cloud deployment are compared. Analyzed the disadvantages of cloud computing.

Keywords. Cloud Computing System, Information Security Threat.

ВСТУП

На сьогоднішній день технології хмарних обчислень стають ключовою стратегією розвитку IT-індустрії. Аналітики оптимістично оцінюють перспективи ринку хмарних послуг.[1] Проте численні дослідження і опитування стверджують, що головним чинником, що уповільнює розвиток ринку хмарних послуг є сумніви потенційних користувачів в достатньому рівні інформаційної безпеки в хмарних моделях.

Дійсно, у сучасних умовах стає все складніше забезпечити захист критично важливих для бізнесу систем і додатків. З появою хмарних сервісів почалась масштабна міграція більшості систем на них, однак рішення задач забезпечення безпеки, пов'язаних з експлуатацією додатків в цьому новому середовищі, вимагає особливого підходу.

КЛАСИФІКАЦІЯ МОДЕЛЕЙ ОБСЛУГОВУВАННЯ

Існують три основні моделі розгортання хмарних сервісів[2]:

Інфраструктура як послуга (англ. Infrastructure as a service, IaaS) - надання обчислювальних ресурсів за запитом, на яких замовник має можливість розгорнути і запустити довільне програмне забезпечення, що включає в себе операційні системи і додатки.

Платформа як послуга (англ. Platform as a service, PaaS) - надання хмарної платформи для розгортання програмного забезпечення, створеного на базі мов програмування і інструментів, які підтримуються хмарним провайдером.

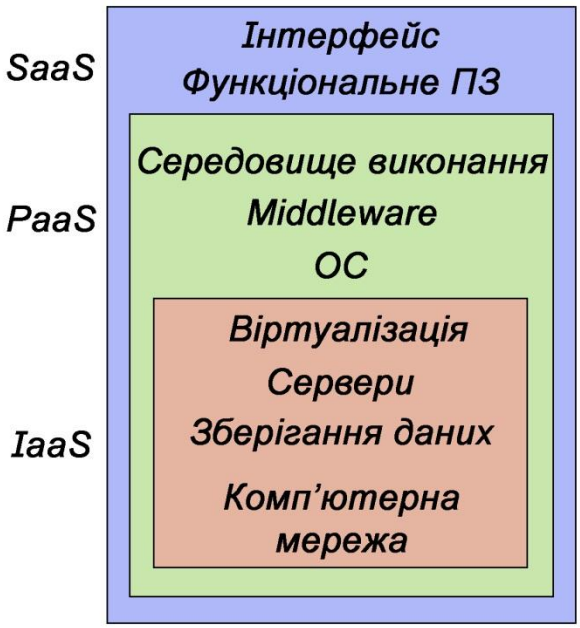

Рисунок 1 – Стек хмарних технологій

Програмне забезпечення як послуга (англ. Software as a service, SaaS) - надання в користування замовнику додатків, розгорнутих на хмарній інфраструктурі провайдера.

Таким чином, специфіка безпеки для трьох хмарних моделей обумовлена рівнем контролю над елементами хмарної інфраструктури (рис.1). Розподіл відповідальності виглядає наступним чином[2]:

SaaS: користувач - 1% (конфіденційність даних), провайдер - 99% (забезпечення всіх рівнів захисту);

PaaS: користувач - 20% (захист додатків), провайдер - 80% (захист інфраструктури і платформ);

IaaS: користувач - 80% (захист додатків і платформ), провайдер - 20% (захист інфраструктури).

Іншими словами, в SaaS користувач несе відповідальність тільки за дані, які завантажуються в хмару, причому за їх збереження теж відповідає провайдер. Саме тому модель SaaS відрізняється вищим рівнем безпеки, на відміну від PaaS і IaaS, оскільки практично знімається загроза порушень з боку користувачів. Тому доцільно розглянути загрози, які виникають при розгортанні бізнесу на SaaS платформі.

НЕДОЛІКИ ХМАРНИХ ОБЧИСЛЕНЬ

Забезпечення інформаційної безпеки хмарних послуг це завдання, яке стоїть перед провайдером. Контроль і управління хмарами складне завдання. Гарантій, що всі ресурси хмари пораховані і в ньому немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари немає.

Це високорівневий тип загроз, тому що він пов'язаний з керованістю хмарою, як єдиною інформаційною системою і для нього загальний захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

Проаналізувавши стан безпеки моделі хмарних обчислень [3,4], можна виділити наступні загрози:

Якщо в традиційних центрах обробки даних, доступ інженерів до серверів строго контролюється на фізичному рівні, то в хмарних обчисленнях доступ інженерів відбувається через Інтернет, що призводить до появи відповідних загроз. Відповідно, критично важливим є строгий контроль доступу для адміністраторів, а також забезпечення контролю і прозорості змін на системному рівні.

Віртуальні машини (ВМ) динамічні. Мінливість ВМ дуже сильно ускладнює створення і підтримання цілісної системи безпеки. Уразливості і помилки в налаштуваннях можуть неконтрольовано поширюватися. Крім цього, дуже непросто зафіксувати для подальшого аудиту стан систем захисту в будь-який певний момент часу.

Сервери хмарних обчислень використовують ті ж операційні системи і ті ж веб-застосунки, що і локальні віртуальні, і фізичні сервери. Відповідно, для хмарних систем загроза віддаленого зламування або зараження шкідливим кодом також висока.

Оскільки файли користувачів і ВМ використовують розподілене середовище зберігання даних, існує загроза цілісності даних (компрометація, втрата). Цілісність операційної системи і файлів додатків, а також внутрішня активність повинні контролюватися.

ВИСНОВКИ

Ґрунтуючись на аналізі можливих загроз в хмарних обчисленнях, можна запропонувати можливий програмно-апаратний комплекс захисту безпеки хмарних обчислень, що включає в себе 5 технологій: брандмауер, система виявлення та запобігання вторгнень (IDS), контроль цілісності, аналіз журналів і захист від шкідливого програмного забезпечення (антивірус).

REFERENCES

[1] Obemy i prognozy razvitiia mirovogo rynka oblachnykh vychislenii. (2014, June 11). Retrieved from http://mirtelecoma.ru/magazine/elektronnaya-versiya/30/

[2] Korneev, N. V. (2015). Analysis of models saas, iaas, paas crm-systems. Tekhnologii Tekhnosfernoi Bezopasnosti, (2), 8. Doi:ISSN: 2071-7342

[3] Kureichik, V. M., & Kovalenko, O. S. (2012). Review of problems and aspects about cloud computing and services. “izvestiya sfedu. Engineering sciences”, 132(7). Doi:issn 2311-3103

[4] Berdnik, A. V. (2013). Cloud computing security problems. Analysis of clouds protection methods suggested by cloud security alliance. Almanakh sovremennoi nauki i obrazovaniia, (10). Doi:ISSN 1993-555.