УДК 004.75

В. Б. Степовий[1]
Л. Б. Ліщинська[1]

БЕЗПЕКА У ХМАРНИХ СЕРВІСАХ

[1]Вінницький національний технічний університет;

Анотація

В роботі проведено аналіз найбільш поширених загроз при використанні хмарних сервісів, а також методик, які використовуються для забезпечення безпеки.

Ключові слова: хмарні сервіси, безпека даних, конфіденційність, цілісність, доступність, загрози безпеки.

Abstract

The paper analyzes mostly wide-spread cloud services vulnerabilities and methods used to assure cloud security.

Keywords: cloud services, data security, confidentiality, integrity, availability, security vulnerabilities.

Вступ

Безпека комп'ютерів і даних загалом базується на трьох основних поняттях: конфіденційності, цілісності і доступності.

Конфіденційність забезпечує приховування певного роду інформації від небажаних користувачів. Для забезпечення конфіденційності даних використовують криптографію, засоби контролю доступу.

Цілісність даних означає, що дані не були змінені неавторизованими користувачами.

Доступність забезпечує доступ до системи та її даних лише авторизованим користувачам і на певний час.

Загрози безпеки у хмарних сервісах подібні до традиційних загроз безпеки комп'ютерів, але хмарне середовище збільшує потенційну кількість вразливих місць і вплив атак. Оскільки хмарне середовище включає всі рівні абстракції: додаток, операційна система, архітектура і мережа, зловмисник має декілька способів для компрометації безпеки хмарного сервісу [1]. На рисунку 1 схематично зображено найбільш типові вразливі місця для різних рівнів абстракції.

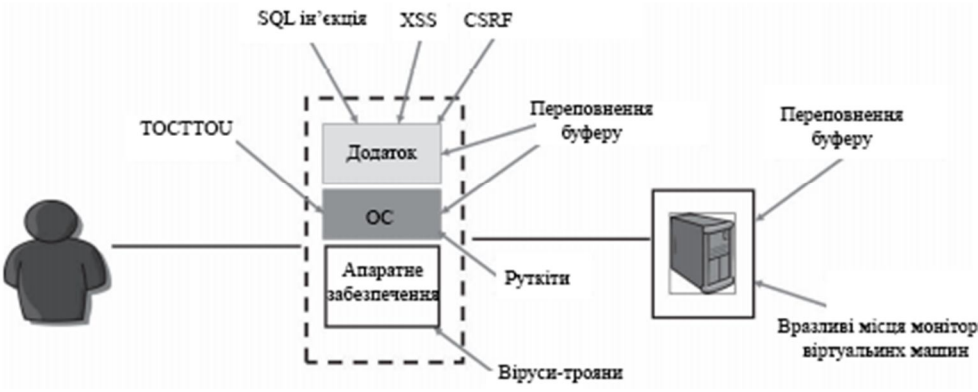

Рисунок 1 – Загрози безпеки хмарних сервісів

Результати досліджень

При використанні хмарних сервісів дані розміщуються на стороні зовнішнього постачальника послуг, що робить більш важким процес регулювання доступу і створює більше ризиків і труднощів, ніж у випадку, коли дані обробляються всередині самої компанії [2]. Оскільки відсутні прямі засоби контролю, клієнтам потрібне підтвердження того, що провайдер працює над забезпеченням безпеки і

цілісності даних. У дата-центрах провайдерів при організації захисту використовуються наступні методики [3]:

- брандмауер межі між приватною і публічною мережами,
- «демілітаризована зона», яка відділяє загальнодоступні сервіси від приватних,
- сегментація мережі,
- системи для виявлення і запобігання вторгнень,
- засоби моніторингу мережі.

Оскільки дані зберігаються у дата-центрах, доступ до критичних даних викликає занепокоєння. Доступ до хмарних сервісів забезпечується на основі прав доступу, які зарезервовані для певних користувачів. Також для забезпечення безпеки доступу до даних використовується двофакторна автентифікація, авторизація, аудит, облік і розподіл обов'язків з адміністрування безпеки, мережі та обслуговування.

Для забезпечення конфіденційності даних, які розміщуються у хмарних сервісах, зазвичай, використовується шифрування, яке передбачає перетворення даних математичними методами і використання секретного ключа. Доступ до даних можуть отримати лише користувачі, які мають код для дешифрування.

Відповідальність за безпеку даних покладається не лише на постачальника хмарних послуг, а й на користувача, незважаючи на те, що хмара обслуговується іншими людьми. Тому доцільно надати такі рекомендації [4]:

- обирати перевіреного постачальника хмарних послуг, якому можна довіряти,
- використовувати перевірене програмне забезпечення,
- перевіряти на відповідність угодам, законам щодо захисту даних,
- здійснювати управління життєвим циклом,
- вивчати можливість вилучення даних з одного хмарного середовища і перенесення в інше.
- постійно виконувати моніторинг ресурсів.

Основні аспекти безпеки у хмарних сервісах наведено на рисунку 2 [5].

Рисунок 2 – Основні аспекти безпеки у хмарних сервісах

Висновки

Підприємствам та організаціям, які впроваджують хмарні технології у свої робочі процеси, потрібно брати до уваги особливості обробки конфіденційних даних. Необхідно навчати персонал, який буде працювати з хмарними сервісами для запобігання додаткових загроз безпеки.

Також користувачі мають розуміти, що вони також відповідальні за безпеку даних, які обробляються у хмарі.

Оскільки ресурси у хмарі виділяються динамічно і надаються різними постачальниками, необхідно зробити цей процес більш прозорим для користувачів для розуміння ними, де і як обробляються їх дані. Також, у цілому, технології забезпечення безпеки даних потребують вдосконалення, як у галузі засобів для запобігання виникненню загроз, так і засобів для виявлення та усунення загроз [6].

Доцільно обирати постачальника хмарних послуг, який має відповідати таким вимогам [7]:

- використання актуальних стандартів безпеки в IT-індустрії,
- забезпечення функціональної сумісності і прозорості,
- забезпечення надійної системи контролю доступу з автентифікацією та авторизацією користувачів,
- використання системи обліку, яка враховує вимоги безпеки і конфіденційності,
- використання технік забезпечення безпеки інформаційних систем і метрик для визначення ефективності захисту апаратного і програмного забезпечення,
- застосування криптографічних методів управління правами на інформацію (IRM).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Daniela O., Squicciarini A., Lin D. Cloud Security Baselines from: Cloud Computing Security, Foundations and Challenges. London: CRC Press, 2016. 15 c.
2. Chandrasekaran K. Essentials of Cloud Computing. London: CRC Press, 2015. 396 c.
3. Furht B., Escalante A. Handbook of Cloud Computing. New York: Springer, 2010. 636 c.
4. What is different about cloud security. URL: https://www.redhat.com/en/topics/security/cloud-security
5. Mitchell I., Alcock J. White Book of Cloud Security. London: Fujitsu Services Ltd., 2011. 61 c.
6. Mather T., Kumaraswamy S., Latif S. Cloud Security and Privacy. Sebastopol: O`Reilly, 2009. 335 c.
7. Krutz R., VinesCloud R. Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley, 2010. 388 c.

Степовий Владислав Богданович — студент групи 3ПІ-17Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vlad.stepoviy1@gmail.com

Ліщинська Людмила Броніславівна — д-р техн. наук, професор, професор кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: llb@vntu.edu.ua

Stepovyj Vladyslav — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vlad.stepoviy1@gmail.com

Lishchynska Lyudmyla Bronislavivna — Dr. Sc. (Eng.), Full Professor, Professor of Program Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: llb@vntu.edu.ua