Багаторівнева класифікація загроз безпеці хмарних обчислень

УДК 004.056.53 (043.2)

Оксана Коваль[1], Сергій Бондаровець[2], Марек Александер[3]

[1,2]Національний авіаційний університет,
[3]Державна вища технічна школа у Новому Сончі (Польща),
[1]oksanakoval@mail.ua, [2]bondss29@gmail.com, [3]aleksmar@pwsz-ns.edu.pl

Хмарні обчислення – широка парадигма, заснована на моделях надання послуг зберігання даних та доступу до програмних застосунків. У системах хмарних обчислень хмари можуть бути представлені на різних рівнях SaaS, PaaS і IaaS. Незважаючи на те, що застосунки для хмар знаходяться у фазі розробки, питання забезпечення безпеки даних та послуг у хмарі наразі є пріоритетним для дослідників. Саме тому виникає необхідність розглядати кожен шар хмари як можливий об'єкт для атаки. Звичайно, системи хмарних обчислень мають багато переваг, але великі організації все ще не наважуються повністю перенести свої IT та інформаційні системи в хмару через загрози інформаційній безпеці. Таким чином, нагальним є питання вирішення проблем безпеки хмарних обчислень та знаходження універсального рішення.

У науково-технічній літературі описано багато різних класифікацій загроз безпеці хмарних обчислень. Наприклад, Р. Бхадаурія пропонує власну класифікацію загроз та пов'язані з ними методи локалізації наслідків. У роботах С. Йео та Х. Парка описані проблеми та загрози, які можуть виникнути при віртуалізації інформаційних систем у хмарі. Також, вагомі дослідження присутні в роботі В. Джансена та Т. Гранса «Рекомендації з безпеки та конфіденційності в публічних хмарах». Тобто, наразі відомі класифікації націлені на конкретний хмарний сервіс або вид хмарної системи. Отже, є необхідність у більш узагальненій класифікації загроз для усіх хмарних сервісів на кожному шарі. З огляду на це, *метою* цієї роботи є представлення багаторівневої класифікації атак на різні хмарні сервіси і пов'язаних з ними ризиків у шарах хмари.

Системи хмарних обчислень мають багаторівневу архітектуру різних служб і рівнів управління. На рис. 1 представлено класифікацію загроз безпеці даних на кожному шарі хмарної системи.

Рис.1. Класифікація атак на безпеку даних на кожному шарі хмарної системи

Проблеми безпеки для платформи SaaS загалом можна розподілити на дві категорії: атаки на засоби розробки та атаки на засоби управління. Загалом усі загрози можна поділити на три групи: 1) загрози конфіденційності даних; 2) атаки на інтерфейс; 3) атаки на SSH. Проблеми безпеки для платформ IaaS та PaaS згруповані у чотири класи: атаки на хмарні сервіси, атаки на віртуалізацію, атаки на уніфіковані обчислення та атаки на SLA.

У табл. 1 показано багаторівневу класифікацію загроз для трьох шарів хмар, які є першим рівнем. На наступному рівні знаходяться хмарні сервіси, а на третьому – типи атак на ці сервіси.

Таблиця 1

Багаторівнева класифікація загроз безпеці і конфіденційності даних в хмарних обчисленнях

Шар хмари (послуга)	*Хмарний сервіс*	*Загроза безпеці*	*Тип атаки*	*Значення ризику*
SaaS	Веб-сервіс	Безпека даних	Конфіденційність	Середній
		Атаки на інтерфейс	Атаки на підписи	Низький
			Атаки на облікові дані	Середній
	API	Атаки на SSH	Атаки на API ключі	Середній
			Атаки на облікові дані користувачів	Середній
IaaS та PaaS	Платформа віртуалізації	Віртуалізація на апаратному рівні	ARP спуфінг на віртуальній комутації	Високий
			MAC спуфінг на віртуальній комутації	Високий
		Віртуалізація на програмному рівні	Злам обчислень	Низький
Сервіси розробки	Хмарні ПЗ	Шкідливе ПЗ	Скрипти	Високий
	Обчислювальні сервіси	Атаки на уніфіковані обчислення	Атаки під час обробки даних	Низький
		Атаки на SLA	Хакінг	Високий

Таким чином, запропонована у роботі класифікація загроз безпеці даних в хмарних обчисленнях висвітлює вплив різних атак на кожному шарі хмари. Також було визначено вимоги безпеки для різних хмарних сервісів: шифрування, забезпечення конфіденційності, авторизація та автентифікація. Такі вимоги повинні відображатися в усіх сервісах для забезпечення цілісності та узгодженості в хмарних системах. Перспективою подальшої роботи є розробка методу виявлення та захисту від атак на систему хмарних обчислень з урахуванням сформованої класифікації.

Науковий керівник – к.т.н., доцент, доцент кафедри БІТ Гнатюк С.О.