Секція 1

АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ЗАХИСТУ ПІД ЧАС ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

Селіванова М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. На сьогодні поширеними є хмарні технології або хмарні обчислення. В них зацікавлені як звичайні користувачі, так і великі компанії. Усім потрібно зберігання даних, інформації, як конфіденційної, так і секретної, і для цього використовуються хмарні технології. Але паралельно з цим є потреба в чинному захисті таких технологій, бо з розвитком комп'ютерних технологій все більше є можливість крадіжки, злому та використання конфіденційних або секретних даних у хмарі.

Метою даної роботи є: вивчення та аналіз існуючих засобів та методів захисту хмарних технологій.

Основні положення. Хмарні обчислення охоплюють технології, які дозволяють окремим особам або компаніям отримувати доступ до певних даних або послуг без потреби у фізичній інфраструктурі.

Інтерфейс включає в себе все, що стикається з користувачем, те, що клієнти бачать безпосередньо. Наприклад, те, що ви бачите в цій роботі та/або на веб-сайті, все завдяки інтерфейсній веб-розробці на задній частині. Однак, є всі процеси та дані, які забезпечують безперебійну роботу цієї сторінки. Бекенд-розробка контролює сервери, бази даних і все, що допомагає підтримувати стабільність цієї веб-сторінки. Коли хмарні обчислення з'являються в картині, вони займають стійку позицію як накладання для всього, що відбувається на сервері. Іншими словами, все, що відбувається на сервері, тепер відбувається в хмарі.[1]

Зі збільшенням кількості віддалених працівників зростає потреба у захисті доступу та переміщенні даних компанії в різних відомих і невідомих мережах. Для того, щоб зробити безпечну та надійну хмарну систему, треба користуватись або одним з даних методів, або для кращої надійності всіма [2]:

- методи автентифікації та ідентифікації;
- методи контролю доступу;
- методи шифрування;
- методи безпечного видалення;
- методи відновлення даних.

Хмарні рішення безпеки поділяються на шість основних категорій, які виконують певну роль у захисті хмарних баз даних, програм і контейнерів:

- CASB – брокери безпеки доступу до хмари
- SAST – статичне тестування безпеки додатків

- SASE – Secure Access Service Edge
- CSPM – Cloud Security Posture Management
- CWPP – хмарні платформи захисту робочого процесу
- CIEM – Cloud Infrastructure Entitlement Management[4]

Плюсом захисту даних у хмарі є систематичне визначення уніфікованих політик, які застосовуються на всіх рівнях. Політики щодо зберігання даних, словника даних, правил доступу та дозволів на основі ролей запобігають будь-якій формі вторгнення, захищаючи конфіденційні дані. Сучасні хмарні рішення для захисту даних також завчасно виявляють ризики та аномалії даних, дозволяючи командам безпеки зупиняти будь-які спроби кібератак або впровадження шкідливого програмного забезпечення.[3]

Висновки. Захист даних є однією з головних проблем безпеки для багатьох організацій у хмарі. Без нього передача особистих даних на віддалені машини була б просто неможливою. Підбиваючи підсумки, методи захисту даних можна використати як окремо, так і всі разом. Щодо оглянутих інструментів безпеки, кожен з них має своє направлення захисту хмарної системи.

Список літератури

1. Cloud Technology: What Is Cloud Computing and How Does It Work? | Trio Developers. *Trio Developers - Stop searching. Start building.* URL – https://www.trio.dev/blog/cloud-technology (дата звернення: 28.10.2022);
2. Proven Security Techniques for Data Protection in Cloud. *LightEdge Solutions*. URL – https://www.lightedge.com/blog/proven-security-techniques-for-data-protection-in-cloud/ (дата звернення: 30.10.2022);
3. What Is Cloud Data Protection? Definition, Importance, and Best Practices |. *Business and Industry News, Analysis and Expert Insights | Spiceworks*. URL – https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-data-protection/#_001 (дата звернення: 03.11.2022);
4. Top 12 Cloud Security Tools for 2022 - Spectral. *Spectral*. URL – https://spectralops.io/blog/top-12-cloud-security-tools/ (дата звернення: 06.11.2022).

Відомості про авторів

Селіванова Марія Олександрівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, т. 099-230-48-13, m.selivanova@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu