DOI 10.36074/logos-13.12.2024.054

ЗАГРОЗИ ДЛЯ БЕЗПЕКИ ХМАРНИХ ТЕХНОЛОГІЙ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ

Бусигін Костянтин Олександрович[1]

1. студент групи БСДМ-53
ННІЗІ ДУІКТ, Київ, УКРАЇНА

У нашій сучасній цифровій епосі, коли хмарні технології стали основною платформою для зберігання та обробки даних, безпека в хмарі вийшла на передній план у сфері кібербезпеки. За даними останніх досліджень, понад 90% компаній використовують хмарні сервіси для зберігання і обробки даних, що робить їх привабливими цілями для зловмисників. Високий попит на ці сервіси створює нові виклики для безпеки, адже багатьом компаніям бракує належного захисту в їхній хмарній інфраструктурі.

Основною проблемою є збереження конфіденційності та цілісності даних, що зберігаються в хмарі. Оскільки інформація часто зберігається на віддалених серверах, фізичний доступ до яких неможливо контролювати, існує ризик несанкціонованого доступу або крадіжки даних. Зловмисники можуть скористатися вразливостями в системах аутентифікації та безпеки доступу, зокрема через скомпрометовані облікові записи або невірно налаштовані політики доступу.

Особливо небезпечними є атаки на хмарні інфраструктури, які включають використання недостатньо захищених інтерфейсів програмування додатків (API). Вразливості в API дозволяють зловмисникам отримувати доступ до даних, маніпулювати ними або запускати шкідливі програми. Також не менш небезпечними є атаки типу "відмова в обслуговуванні" (DoS) або атаки на резервне копіювання даних, що можуть призвести до втрати або блокування важливої інформації.

Для протидії цим загрозам необхідно застосовувати комплексний підхід. По-перше, важливо ретельно налаштовувати та перевіряти політики доступу до хмарних ресурсів, забезпечуючи багатофакторну аутентифікацію та обмеження прав доступу. По-друге, організації повинні забезпечити шифрування даних як на етапі їх передачі, так і на етапі зберігання в хмарі, що дозволяє знизити ризики витоку інформації.

Також важливо використовувати сучасні системи моніторингу і виявлення загроз (SIEM) для оперативного виявлення аномалій у поведінці користувачів або підозрілих спроб доступу до критичних даних. Регулярне оновлення програмного забезпечення та виправлення вразливостей дозволяє запобігти використанню відомих експлойтів зловмисниками.

У світі, де хмарні технології стають основною частиною інформаційної інфраструктури, зокрема для зберігання великих обсягів даних, захист цих даних є одним із пріоритетів. Зважаючи на стрімкий розвиток таких технологій, важливо усвідомлювати нові ризики і активно застосовувати заходи безпеки, що дозволяють захистити дані в хмарному середовищі. Загалом, зважаючи на стрімкий розвиток хмарних технологій, важливо розуміти нові ризики, з якими стикаються організації, і вчасно реагувати на загрози. Тільки завдяки комплексному підходу та правильному управлінню безпекою можна забезпечити надійний захист даних у хмарному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Шевченко, В. В., & Коваленко, А. І. (2019). Проблеми безпеки в хмарних технологіях та шляхи їх вирішення. *Інформаційні технології та кібербезпека, 15*(2), 45–53.

[2] Лебедєв, О. П. (2021). Виклики та загрози кібербезпеки в умовах хмарних обчислень. *Вісник національної академії внутрішніх справ, 24*(1), 101–110.

[3] Харченко, Ю. С., & Іванова, І. М. (2020). Моделі забезпечення безпеки даних у хмарних середовищах. *Науковий вісник Київського університету права, 19*(4), 56–64.