УДК: 004.75:004.056.5

ПРОБЛЕМИ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СХОВИЩАХ

Леонова А.О.
Науковий керівник - ст. викл. Данилов А.Д.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: anna.leonova@nure.ua

Instead of storing files on your company's hard drive or local storage device, you can use cloud storage, which allows you to store them in a remote database. Cloud storage is becoming increasingly popular among people who need more storage space and for businesses looking for an efficient off-premises data backup solution. Due to the growing popularity and use of cloud storage, cloud security has become a major concern to protect data integrity, prevent hacking attempts, and prevent file or personal data theft.

У сучасному світі цифрових технологій хмарні сховища набули великого значення. Більшість приватних даних зберігається в хмарі, за власним бажанням співробітника або за рішенням компанії. Тому питання безпеки інформації в хмарних сховищах є серйозною проблемою [1].

Важливо мати стратегію безпеки в хмарі. Незалежно від того, чи має постачальник хмарних послуг вбудовані засоби безпеки, чи користувач співпрацює з провідними постачальниками хмарних технологій, можна отримати численні переваги від хмарної безпеки [2]. В іншому випадку, можуть з’явитися наступні проблеми:

– відсутність видимості. Легко втратити інформацію про те, як і хто отримує доступ до ваших даних, оскільки доступ до багатьох хмарних служб здійснюється за межами корпоративних мереж і через треті сторони;

– неправильні конфігурації. Частину зламаних записів можна віднести до неправильно налаштованих активів, що робить ненавмисне внутрішнє користування ключовою проблемою для середовищ хмарних обчислень [3];

– тіньові IT – це практика використання пристроїв, програм і систем без погодження з IT-відділом організації. Хмарна безпека має охоплювати всі точки доступу до хмари, щоб співробітники не могли порушити безпеку всієї організації, входячи в систему з приватних пристроїв;

– керування доступом. Як і в традиційних системах кібербезпеки, права доступу користувачів мають бути пропорційні їхнім посадовим обов’язкам. Співробітники з надлишковими правами можуть завдати шкоди даним через недосвідченість або через хакерські атаки на їхні облікові записи [4].

Для забезпечення надійної безпеки в хмарі можна використовувати різні підходи та інструменти, адаптовані до конкретних вимог і рівнів захисту. Ось деякі приклади заходів захисту в хмарних середовищах [4, 5]:

– шифрування даних. Шифрування є фундаментальним стовпом безпеки, перетворюючи дані в нерозбірливий формат за допомогою алгоритмів кодування та криптографічних ключів;

– ефективний контроль доступу. Впровадження суворого контролю доступу є необхідним для підтримки цілісності хмарних ресурсів. Сюди входить надійна автентифікація користувачів, політики авторизації та контроль доступу на основі ролей (RBAC);

– надійні брандмауери. Брандмауери слугують захисними бар'єрами між внутрішніми і зовнішніми мережами, ретельно фільтруючи вхідний і вихідний мережевий трафік;

– надійне резервне копіювання та відновлення. Впровадження надійних стратегій резервного копіювання та відновлення є важливим аспектом безпеки хмари, забезпечуючи доступність і цілісність даних;

– ефективні системи виявлення та запобігання вторгнень (IDPS). Засоби IDPS активно контролюють мережевий трафік і системи, відстежуючи підозрілі дії або потенційні порушення безпеки;

– централізоване управління інформацією та подіями безпеки (SIEM). Ці системи об'єднують і аналізують дані журналів із різних джерел у хмарній інфраструктурі, забезпечуючи централізоване спостереження за подіями безпеки.

Хмарні обчислення забезпечують зручний доступ до даних та стають об'єктом збільшеного ризику щодо безпеки. З метою запобігання можливим загрозам, необхідно вживати комплекс заходів безпеки (шифрування даних, контроль доступу та використання надійних брандмауерів та антивірусного програмного забезпечення). Надійна стратегія безпеки в хмарних обчисленнях є ключовим елементом для збереження цілісності та конфіденційності даних у цифровому середовищі.

Список використаних джерел

1. Cloud Security: Definition, How Cloud Computing Works, and Safety. investopedia.com: веб сайт. URL: https://www.investopedia.com/terms/c/cloud-security.asp(дата звернення: 2.03.2024).

2. CLOUD SECURITY. crowdstrike.com: веб сайт. URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/(дата звернення: 2.03.2024).

3. What is cloud security? ibm.com: веб сайт. URL: https://www.ibm.com/topics/cloud-security(дата звернення: 2.03.2024).

4. Що таке хмарна безпека? nordvpn.com: веб сайт. URL: https://nordvpn.com/uk/cybersecurity/cloud-security/ (дата звернення: 2.03.2024).

5. Рудий С.В., Сєвєрінов О.В. Дослідження моделі безпеки при використанні хмарних сервісів. 2022.