ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ: АКТУАЛЬНІ ЗАВДАННЯ ТА ВИКЛИКИ

Саєнко Олена Олександрівна
ORCID ID: 0000-0002-6558-2772
канд. техн. наук, старший викладач кафедри ІКІ ім. В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Хмарні сервіси займають все більш важливе місце у сучасному світі, надаючи зручний доступ до обчислювальних ресурсів та зберігання даних. Зростання використання хмарних технологій приводить до збільшення обсягу даних, які зберігаються та обробляються в хмарних сервісах. Тому забезпечення надійності та безпеки даних, які зберігаються та обробляються в хмарних сервісах, стає основним завданням.

Однак, разом зі зростанням використання хмарних технологій, з'являються нові виклики в галузі кібербезпеки. Основними завданнями кіберзебпеки в хмарних сервісах є:

- аутентифікація та авторизація користувачів: важливим завданням є впевненість у тому, що тільки правомірні користувачі мають доступ до ресурсів хмарних сервісів та даних. Тут важливим кроком є використання сильних механізмів аутентифікації та авторизації;

- шифрування даних: захист конфіденційності даних є одним з ключових аспектів кібербезпеки для запобігання несанкціонованому доступу та зламу;

- моніторинг та виявлення вторгнень, що допомагає вчасно реагувати на потенційні загрози [1].

Для вибору належних заходів безпеки в хмарних сервісах варто враховувати існуючі виклики кібербезпеки [2]. По перше, необхідно розв'язувати питання щодо захисту даних та мережевої інфраструктури в умовах розподілених середовищ. По друге, у хмарних сервісах можуть виникати загрози від внутрішніх користувачів, таких як зламаний акаунт або зловживання привілеями доступу. Необхідно розробляти сувору політику доступу та контролювати привілеї користувачів, щоб запобігти внутрішнім загрозам.

Хмарні сервіси постійно стикаються з різними видами кібератак, такими як віруси, злочинні програми, фішинг, DDoS-атаки та інші. Зловмисники можуть намагатися отримати доступ до конфіденційних даних, які зберігаються в хмарних сервісах, шляхом атак на систему або за допомогою соціального інженерінгу.

Серед основних викликів до забезпечення кібербезпеки в хмарних технологіях можна виділити наступні:

- розвиток штучного інтелекту, який стає інструментом для кіберзлочинців. Технології Deepfake, зокрема клонування голосу, були одними з перших методів штучного інтелекту, які хакери використовували у своїх атаках на голосовий фішинг, щоб успішно змусити співробітників повірити, що вони розмовляють із членами власної організації. Штучний інтелект може створювати переконливі фішингові електронні листи, на які натискають частіше, ніж ті, що створюють люди;

- стрес, відсутність мотивації та недостатня активність експертів з кібербезпеки створюють ідеальну картину для кіберзлочинців. Перевантажені професіонали легко пропускають ознаки атаки або навіть помилки, які створюють уразливість для хакерів, наприклад, нездатність оновити програмне забезпечення. Кіберзлочинці

спеціально націлюються на компанії з командами, які більш вразливі. 60% компаній мали труднощі з утриманням кваліфікованих спеціалістів із кібербезпеки у 2022 році, а стрес на роботі був однією з п'яти основних причин для звільнення [3];

- завдяки різкому збільшенню кількості послуг-вимагачів (RaaS), кіберзлочинці зараз диверсифікують свої бізнес-моделі. Оператори RaaS зараз пропонують будь-кому можливість проводити широкомасштабні атаки, що призвело до астрономічного збільшення потенційної кількості кіберзлочинців. З 2021 по 2022 рік кількість програм-вимагачів зросла на 13% – це зростання вище, ніж за п'ять попередніх років разом узятих [4];

- кіберзлочинці застосовують тактику MFA fatigue або MFA push spam, яка полягає у заповненні цільових робітників з кіберзахисту повторюваними спливаючими сповіщеннями, доки вони врешті-решт не приймуть їх помилково або через виснаження. Цей метод нещодавно використовувався під час масового витоку даних Uber, Microsoft і Cisco [5].

Забезпечення стійкості до таких атак і вчасне виявлення та реагування на них є ключовими завданнями для забезпечення кібербезпеки. Для цього рекомендується використовувати багатофакторну аутентифікацію, шифрування з використанням сильних алгоритмів та механізми керування доступом для забезпечення безпеки вхідного доступу до хмарних сервісів. Крім того, точна ідентифікація користувачів дозволяє відокремити легітимних користувачів від потенційних зловмисників. Постачальники хмарних сервісів повинні регулярно оновлювати та патчити свої системи, програмне забезпечення та інфраструктуру для запобігання використанню вразливостей; мають використовувати системи моніторингу, виявлення аномалій та вторгнень для постійного контролю за безпекою хмарних сервісів.

Налагодження моніторингу можливо шляхом використання систем IDS, що дозволяє виявляти незвичайну активність, включаючи намагання несанкціонованого доступу до даних чи спроби атаки на систему. Це дозволяє оперативно реагувати на потенційні загрози та запобігати їхньому втіленню.

Не менш важливим є питання систематичної освіти та навчання користувачів щодо основних правил кібербезпеки, таких як створення сильних паролів, усвідомлення ризиків фішингу та інших загроз. Рекомендується проводити періодичні перевірки та аудит безпеки хмарних сервісів, щоб виявляти потенційні слабкі місця, виявляти помилки та вдосконалювати системи безпеки.

Висновки. Кібербезпека в хмарних сервісах є критичним аспектом, оскільки обсяги даних і значимість хмарних сервісів продовжують зростати. Актуальні завдання та виклики, пов'язані з кібербезпекою в хмарних сервісах, потребують системного підходу та впровадження відповідних заходів безпеки.

Список використаних джерел:

1. Nogueira, M., Sun, X., & De Sousa, R. T. (2019). Cybersecurity in Cloud Computing: Threats and Solutions. IEEE Communications Surveys & Tutorials, 21(1), 836-880.
2. Kshetri, N. (2019). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Journal of Business Research, 92, 317-325.
3. ISACA (2022). State of cybersecurity 2022: cyber workforce challenges.
4. Verizon (2023). 2023 Data Breach Investigations Report.
5. Bleeping Computer (2022). MFA fatigue: hackers 'new favorite tactic in high-profile breaches.