УДК 004.7:004.056

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ І МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФРАСТРУКТУРИ У ХМАРНОМУ СЕРЕДОВИЩІ

Красюкова В.В.
Науковий керівник – доц. Коваленко Т.М.
Харківский національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: valeriia.krasiukova@nure.ua

The use of cloud environments is an essential part of working with information technologies. The use of cloud technologies requires thorough security measures. Key methods include multifactor authentication, limiting user access to the necessary minimum, network protection, and data encryption. Recommendations include creating network tiers, securing networks, using certificates, and encrypting traffic. Traffic filtering and monitoring, automated response to threats, auditing, and adherence to standards such as ISO/IEC 27001 are crucial for ensuring a high level of security and trust in cloud environments.

Використання хмарних середовищ є важливою частиною роботи з інформаційними технологіями. Безпека інфраструктури в хмарному середовищі є ключовим аспектом в питанні довіри користувачів до сервісу.

Захист інфраструктури хмарного середовища включає в себе багатофакторну автентифікацію, захист мереж, журнали активності користувачів та шифрування даних.

Основоположним принципом забезпечення безпеки в хмарному середовищі є надання доступу користувачам до ресурсів та даних, зведених до необхідного мінімуму. Так завданням адміністратора є визначення потреб кожного конкретного користувача, або груп користувачів, та надання прав таким чином, щоб кожен користувач мав доступ до ресурсів які потрібні йому для роботи, але не більше. Облікові дані не повинні надаватись спільно жодному користувачу чи системі. Доступ користувачам слід надавати з найменшими привілеями, включаючи паролі та використання багатофакторної автентифікації. Програмний доступ має здійснюватись за допомогою тимчасових облікових даних з обмеженими привілеями [1]. Таким чином користувач не буде мати доступ до ресурсів та даних які не потрібні йому для роботи, а також у випадку компрометування певного користувача зловмисник не отримає доступ до всієї системи, а лише до певної її частини. Крім того варто встановити вимоги до паролів користувачів, періодичної їх заміни згідно з журналом паролів, та автоматично виявляти паролі з високим ризиком.

Для захисту мереж рекомендовано створювати мережеві рівні, де компоненти які мають спільні вимоги до чутливості будуть згруповані. Трафік при цьому має надходити лише від сусіднього наступного найменш чутливого рівня. Розробляючи топологію мережі необхідно вивчити вимоги до підключення кожного компонента. Для ефективного захисту трафіку використовуються групи безпеки, мережеві списки дозволів, підмережі та таблиці маршрутів [2].

Для захисту даних під час передачі необхідно впровадити використання сертифікатів безпеки транспортного рівня. Крім того для захисту даних варто шифрувати ці дані при зберіганні та транспортуванні, що допоможе забезпечити їх конфіденційність і цілісність. Мережевий трафік між інфраструктурою хмари та Інтернетом має бути обов’язково зашифрований. Мережевий трафік у внутрішньому середовищі має шифруватись за допомогою TLS там де це можливо.

Для фільтрування трафіку що виходить за периметр приватної інфраструктури необхідно налаштувати брендмауер. Так трафік можна фільтрувати за певними критеріями, білими та чорними списками, чи налаштування тихих перевірок за допомогою CAPTCHA для зменшення трафіку ботів [1].

Для виявлення потенційних загроз та аномальних подій необхідно впроваджувати системи моніторингу інфраструктури, що дозволить оперативно виявляти та реагувати на виявлені загрози. Використання автоматизованих систем реагування на події дозволить масштабувати та прискорити можливості моніторингу та зменшить вплив людського фактору.

Крім описаних методів варто зауважити що важливе значення має також аудит та впровадження стандартів безпеки, таких як ISO/IEC 27001, SOC 2. Впровадження даних стандартів допомагає забезпечити високий рівень безпеки, відповідність законодавства у сфері забезпечення інформаційної безпеки та підвищить довіру партнерів та користувачів до організації. Регулярне проведення внутрішніх та зовнішніх аудитів є частиною вимог стандартів безпеки та дозволить виявити потенційні загрози та слабкі місця в захисті, підвищить ефективність впроваджених підходів до забезпечення безпеки а також перевірить інфраструктуру на відповідність стандартам безпеки.

Список використаних джерел:

1. Security Pillar - AWS Well-Architected Framework. URL : https://docs.aws.amazon.com/pdfs/wellarchitected/latest/framework/wellarchitected-framework.pdf

2. Data classification models and schemes. URL : https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-models-and-schemes.html