УДК 004.7:004.056

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ І МЕТОДІВ ОЦІНКИ 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 integral part of working with information technologies. Analyzing modern methods of assessing infrastructure security in cloud environments is one of the key aspects to ensure a high level of data and resource protection. To assess security, methods such as security audits, penetration testing, risk assessment, and event log analysis can be utilized. These methods can be used separately, but to ensure maximum accuracy in security assessment, combining them is recommended. Security assessment of the infrastructure in the cloud environment needs to be conducted periodically to identify security threats and address them.

Використання хмарних середовищ є невід'ємною частиною роботи з інформаційними технологіями. Аналіз сучасних методів оцінки безпеки інфраструктури в хмарних середовищах є одним з ключових аспектів для забезпечення високого рівня захисту даних і ресурсів. Для оцінки безпеки можна використовувати такі методи як аудит безпеки, тест на проникнення, оцінка ризиків та аналіз журналів подій.

Перш за все для оцінки безпеки інфраструктури варто почати з оцінки ризиків. Для цього необхідно визначити потенційні загрози та вразливості, та оцінити потенційні наслідки від реалізації зловмисником цих загроз. Класифікація ризиків допомагає визначити пріоритети для розробки стратегії управління ризиками. Ці стратегії приймаються після оцінки ризиків, які можуть включати в себе технічні та організаційні заходи для зменшення вразливостей [1].

Ефективніше всього оцінювати захищеність інфраструктури можна за допомогою перевірки її на відповідність міжнародним стандартам безпеки, наприклад ISO/IEC 27001 [2]. Стандарт є по суті списком параметрів які мають бути втілені у системі. Внутрішній аудит власної організації означає що співробітник служби безпеки має перевірити чи втілені у компаній всі вимоги, та вказати всі відмінності у звіті. Таким чином власник організації отримає інформацію про оцінку захищеності інфраструктури. Зовнішній аудит проводиться консалтинговою компанією і відбувається аналогічним чином, проте зазвичай він може стати більш об'єктивним, тому що виключає можливість того що співробітник служби безпеки приховає певні недоліки через те що відповідальність за їх усунення може бути покладене на нього. Тож зовнішній аудит виключає

власну зацікавленість співробітника в певних результатах. Після усунення виявлених недоліків варто провести повторний аудит.

Крім аудиту організація може оцінити захищеність власної інфраструктури у хмарному середовищі за допомогою тесту на проникнення. Зазвичай для цього наймають консалдингову компанію, яка намагається проникнути в систему з метою виявити слабкі місця в захисті та оцінити рівень захисту інфраструктури. Перед початком проникнення укладається договір зі всіма умова проведення тесту, а після власне тесту компанія надає детальний звіт про виявлені вразливості.

Аналіз журналів подій включає в себе вивчення журналів подій з метою виявлення аномальних активностей та інцидентів у хмарному середовищі. Журнали подій можуть містити в собі інформацію про те хто та коли входив до інфраструктури, до яких ресурсів звертався чи намагався звернутись, які дії були зроблені (успішні та неуспішні). Зазвичай інформацію в цих журналах можна відфільтрувати для зручного вивчення, а також даний аналіз можна автоматизувати. На успішні дії варто звертати увагу для того щоб перевірити чи правильно налаштовано надання доступу користувачам, чи не отримують користувачі доступ до ресурсів, до яких вони не повинні мати доступ. Проте аналіз неуспішних спроб може показати які користувачі намагались отримати доступ до ресурсів яі для них закриті, що є підозрілою поведінкою. Також за допомогою аналізу неуспішних спроб входу в систему можна побачити чи не намагався хтось отримати несанкціонований доступ до облікових записів певних користувачів. Також підзрілою можна вважати якщо певний обліковий запис здійснює активність в неробочий час працівника. Це також може свідчити про потенційну компроментацію облікового запису.

Наведені методи можуть використовуватись окремо, проте для забезпечення максимальної точності в оцінці безпеки поєднувати їх. Також варто зауважити що оцінка рівня захисту інфраструктури повинна проводитись регулярно, для виявлення потенційних загроз та їх усунення.

Список використаних джерел:

1. Reconshell. Cloud Security Handbook. 2022. URL: https://reconshell.com/wp-content/uploads/2022/07/Cloud-Security-Handbook.pdf

2. ISO/IEC 27001:2022 "Information technology — Security techniques — Information security management systems — Requirements", International Organization for Standardization, Geneva, Switzerland. URL: https://www.iso.org/standard/27001