ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ХМАРНОМУ СЕРЕДОВИЩІ

Щерба М.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: maksym.shcherba@nure.ua

Abstract

The paper analyzes the existing types of clouds and cloud services. The main vulnerabilities of cloud systems are considered in detail. Attention is paid to ways to protect these systems from threats, as well as recommendations are put forward for setting up cloud services to create a safe and reliable cloud system. A structural diagram of the cloud infrastructure using the Amazon AWS platform has been developed. On the basis of the developed structural scheme, a cloud infrastructure was built using the Amazon AWS platform, taking into account the recommendations regarding the construction

В наш час, активного розвитку зазнали хмарні середовища. Там зберігається величезна кількість конфіденційної інформації. Згідно з публікацією Cybercrime Magazine [1] до 2025 року очікується, що сумарних об'єм даних в хмарі складатиме більше 100 зетабайтів. Головною задачею є забезпечення належного захисту цієї інформації. Таким чином, визначення способів захисту від загроз інформаційній безпеці у хмарному середовищі та налаштування хмарних послуг для безпечної та надійної системи є вкрай важливим.

Для вирішення поставленої задачі було проаналізовано основні вразливості хмарних систем. Та визначено основні загрози інформаційної безпеки.

Основних вразливостей хмарних систем

Хмарні обчислення разом з великими перевагами для користувачі, несуть з собою проблеми безпеки. Вони мають не лише ризики безпеки притаманні традиційним обчислювальним середовищам, а й нові проблеми безпеки. Ці проблеми виникають в основному через спільне користування інфраструктурою та ресурсами.

Загрози безпеки в системах хмарних обчислень можна розділити на три категорії: загрози інфраструктури, загрози інформації, загрози контролю доступу.

Рекомендації щодо налаштування хмарних послуг для створення безпечної та надійної хмарної системи

Постачальники хмарних послуг мають Well-Architected Framework. Це інструмент, який допомагає користувачу створити безпечну та надійну хмарну інфраструктуру. У ході роботи було розглянути Well-Architected Framework двох хмарних постачальників, а саме Amazon AWS та Microsoft Azure.

Amazon AWS Well-Architected framework включає в себе 6 принципів: Операційна досконаліть, безпека, надійність, ефективність продуктивності, оптимізація витрат, стійкість [2].

На сайті Center for Internet Security можна завантажити документацію, де будуть знаходитись деталізовані рекомендації, щодо налаштування параметрів безпеки для хмарних сервісів [3]. Що стосується рекомендації безпеки для Amazon AWS, то документ включає в себе налаштування без-

пеки для основних послуг таких, як AWS Identify and Access Management, AWS Config, AWS CloudTrail, AWS CloudWatch, AWS SNS, AWS Simple Storage Service, AWS EC2, RDS, AWS VPC.

Також для користувача, який користується хмарними послугами, необхідно притримуватись певних правил, які на мою думку є важливими та основними, для створення безпечної і надійної хмарної системи.

Найперше, що необхідно це обрати надійного постачальника послуг. Він має мати гарну репутацію в сфері безпеки. Необхідно детально ознайомитись з стандартами безпеки даного провайдера, переглянути сертифікації.

Наступним кроком буде встановлення прав доступу для співробітників. Кращим варіантом буде притримуватись правила найменших привілеїв, тобто кожен співробітник має мати права доступу, саме до того і лише до того з чим працює. Регулярно треба переглядати права доступу та за необхідністю їх скасовувати.

Для захисту облікових записів користувачів, необхідно використовувати політику паролів. Встановлювати складність паролів та регулярну їх заміну. Якщо є можливість, варто використовувати двофакторну автентифікацію.

Необхідно запровадити моніторинг та аудит безпеки. Це допоможе швидко зреагувати, якщо були помічені сліди порушення.

Також варто ознайомитись та використовувати інструменти безпеки, які надає постачальник послуг.

Данні у спокої та в транзиті мають бути обов'язково зашифроване міцними протоколами шифрування даних.

Для надійного зберігання даних варто робити резервні копії, для того щоб у разі необхідності була можливість їх швидко відновити.

Також ватро проводити бесіди з співробітниками стосовно інформаційної безпеки. Надавати їм базові знання, які допоможуть їм захистити дані.

Побудова хмарної інфраструктури з використанням платформи Amazon AWS на основі розробленої схеми

Проаналізувавши еталонні схеми базових інфраструктур, було розроблено структурну схему власної хмарної інфраструктури на платформі AWS. При побудові використовувались базові сервіси платформи AWS: Amazon VPC, Amazon EC2, Amazon RDS, Amazon CloudWatch, Amazon SNS.

На основі представленої схеми інфраструктури була побудована та налаштована хмарна інфраструктура на платформі AWS. Налаштування відбувалось виходячи з рекомендацій з офіційної документації AWS, що дозволило побудувати функціонуючу, безпечну та надійну хмарну інфраструктуру

Було розгорнуто віртуальну приватну хмару та дві підмережі, для яких було налаштовано групи безпек згідно офіційними документаціями Amazon AWS та рекомендацій Center for Internet Security.

Також був запущений і налаштований згідно з рекомендацій безпеки сервер програми Amazon EC2. за допомогою сервісу Amazon RDS була створена нова база даних. База даних була створена на основі MySQL 8.0.32.

Останнім етапом було налаштування додаткових сервісів Amazon CloudWatch та Amazon SNS, які допоможуть слідкувати за станом хмарної інфраструктури.

Література

1. The World Will Store 200 Zettabytes Of Data By 2025 : веб-сайт. URL: https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/ (дата звернення: 06.11.2023).

2. AWS Well-Architected : веб-сайт. URL: https://aws.amazon.com/architecture/well-architected (дата звернення: 06.11.2023).

3. CIS AWS Benchmark : веб-сайт. URL: https://www.cisecurity.org/benchmark/amazon_web_services (дата звернення: 06.11.2023).

4. Щерба М. О. Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі : кваліфікаційна робота : 125. Харків, 2023. 39 с.