СУЧАСНІ МЕТОДИ АНАЛІЗУ ВРАЗЛИВОСТЕЙ В ХМАРНИХ СЕРЕДОВИЩАХ

Фісенко Д. М.[1], Пантєлєєв В.О[1]., Білодід В.Г.[2]

[1]Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
[2] Харківський національний університет Повітряних Сил, Україна
Україна

E-mail: dmytro.fisenko@nure.ua
vadym.pantielieiev@nure.ua,
vibos111@gmail.com

Abstract

In light of the rapid advancement of information technologies, the assurance of information security has emerged as a pivotal concern. The prevalence of cloud environments as the predominant repository for data, including sensitive and confidential information belonging to companies, government agencies, and individuals, underscores the urgency of this issue. This research endeavors to examine contemporary methodologies for vulnerability assessment in cloud environments. To this end, an analytical approach was employed, encompassing a comprehensive literature review and an evaluation of existing techniques for vulnerability analysis in cloud environments.

В умовах стрімкого розвитку інфокомунікаційних технологій забезпечення інформаційної безпеки в хмарних середовищах є критично важливим через те, що хмарні середовища стають основним середовищем для зберігання, обробки та передачі даних, зокрема чутливих і конфіденційних даних, що належать компаніям, урядовим установам чи приватним особам.

Більшість хмарних платформ, зокрема AWS (Amazon Web Services) та Microsoft Azure, пропонують широкий набір інструментів для аналізу безпеки, однак сучасний підхід до оцінки вразливостей виходить за межі традиційного сканування на відомі вразливості. Сьогодні аналіз вразливостей охоплює автоматизацію процесів, аналіз конфігурацій, моніторинг у режимі реального часу, поведінковий аналіз тощо.

Одним із основних методів аналізу вразливостей є автоматизоване сканування на вразливості. Всі основні хмарні провайдери мають вбудовані інструменти, які дозволяють автоматично виявляти вразливості. Наприклад AWS має Amazon Inspector [1] — автоматизований і безперервний сервіс сканування вразливостей, який аналізує віртуальні сервери Elastic Compute Cloud (EC2), програмний код, що запускається в AWS Lambda та образи контейнерів в Amazon ECR. За допомогою цього сервісу можливо налаштувати постійну перевірку на наявність вразливостей програмного забезпечення та неавторизованого доступу до мережі.

Також пріоритетним аспектом є інструменти управління станом безпеки хмарного середовища. Вони зосереджуються на виявленні неправильно налаштованих ресурсів та порушень відповідності у хмарному середовищі. Прикладом є AWS Config [2], який дозволяє відстежувати зміни в ресурсах AWS і забезпечувати постійну оцінку відповідності найкращим практикам безпеки. Правила AWS Config можна налаштувати для забезпечення відповідності внутрішнім або зовнішнім політикам безпеки.

Такі напрямки як моніторинг мережевого трафіку, поведінки користувачів та аномалій забезпечують сучасний підхід до виявлення вразливостей або атак, що вже тривають. Прикладом такого сервісу в AWS є GuardDuty [3]. Цей сервіс допомагає виявляти загрози, за рахунок постійного сканування облікових записів та робочих навантажень на наявність зловмисної активності та надає докладні результати безпеки для видимості та виправлення. GuardDuty використовує канали аналізу загроз, такі як списки шкідливих IP-адрес і доменів, хеші файлів та моделі машинного навчання (ML), щоб ідентифікувати підозрілу та потенційно зловмисну активність у середовищі AWS.

Аудит безпеки та перевірка на відповідність галузевим стандартам також є важливою складовою забезпечення безпеки в хмарних середовищах. Відповідності стандартам, таким як PCI DSS, HIPAA та GDPR, допомагає виявляти вразливості, пов'язані з неправильними конфігураціями або прогалинами в заходах безпеки. Прикладом є AWS Security Hub [4]. Цей сервіс інтегрує кілька інструментів безпеки AWS для надання повного огляду стану безпеки в AWS акаунтах та проводить перевірку відповідно до різних стандартів, включаючи CIS AWS Foundations Benchmark, GDPR тощо.

Управління доступом в хмарних середовищах є значною складовою інформаційної безпеки. Моніторинг політик управління ідентифікацією та доступом допомагає виявляти та запобігати несанкціонованому доступу до систем та даних. Прикладом є IAM Access Analyzer [5] – сервіс, який забезпечує перевірку ролей та політик на наявність ризикованих дозволів або непередбаченого зовнішнього доступу. Може знаходити ресурси, доступні ззовні акаунта або які мають надто широкі права доступу.

При дослідженні хмарного середовища Microsoft Azure стало відомо, що воно також має вбудовані сервіси для автоматизованого сканування на вразливості. Такий сервіс як Microsoft Defender for Cloud забезпечує оцінку вразливостей, за результатами якої можливо дізнатися чи виявлені вразливості в програмному забезпеченні, що працює на віртуальній машині або в її операційній системі. Крім того, цей сервіс поєднує в собі такі можливості як централізоване управління політиками, яке забезпечує відповідність безпековим стандартам при конфігурації ресурсів, автоматичне виявлення конфіденційних даних в хмарних сховищах, та встановлення неавторизованих та потенційно шкідливих спроб отримати доступ до облікових записів [6].

Так само як і AWS, Azure пропонує сервіс Microsoft Sentinel [7], який призначений для надання повного огляду безпеки організації, забезпечуючи можливість виявляти, запобігати та реагувати на загрози в реальному часі як у хмарних, так і в локальних та гібридних середовищах. Однією з головних особливостей даного сервісу є можливість інтеграції з різними джерелами для збору даних з пристроїв, користувачів, додатків та інфраструктури. Основними перевагами використання Microsoft Sentinel є:

- централізоване управління та моніторинг безпеки всієї організації;
- зниження часу на виявлення та реагування завдяки автоматизації та інтелектуальній аналітиці;
- відсутність необхідності в локальній інфраструктурі;
- автоматизація рутинних завдань, яка дозволяє зосередитися на критичних інцидентах.

Невід'ємною частиною аналізу вразливостей в хмарних середовищах є постійний збір та моніторинг логів та метрик. Це дає змогу забезпечити видимість загальносистемної продуктивності, вчасно реагувати на зміни та отримувати єдине уявлення про працездатність середовища. Зазвичай отримані дані використовуються для наступних цілей:

- візуалізація ключових показників безпеки в реальному часі;
- створення звітів, які дозволяють аналізувати історичні дані та виявляти тенденції або патерни загроз;
- створення оповіщень на основі певних умов або порогових значень, що дозволяє швидко реагувати на інциденти безпеки;
- інтеграція з іншими інструментами безпеки для розширеного аналізу та реагування;
- збір та зберігання логів для виконання вимоги регуляторних стандартів та проходження аудитів безпеки.

Для збору та аналізу логів та метрик AWS пропонує використовувати сервіс Amazon CloudWatch [8]. Даний сервіс надає можливість візуалізувати дані про продуктивність, створювати сповіщення та досліджувати метрики, для покращення продуктивності в ресурсах AWS.

В свою чергу Azure пропонує сервіс Azure Monitor [9], який є комплексним рішенням для збору, аналізу та реагування на дані моніторингу з хмарного та локального середовищ. Сервіс надає можливості для проактивного виявлення загроз, швидкого реагування на інциденти та підтримки відповідності стандартам безпеки.

Моніторинг мережі є суттєвим для забезпечення інформаційної безпеки з кількох причин. Він дозволяє виявляти, аналізувати та реагувати на потенційні загрози, відстежувати підозрілі трафікові патерни у мережевому середовищі, виявляти потенційні ризики безпеки, витоки даних або несанкціонований доступ.

Одним із способів моніторингу мережевого трафіку в середовищі AWS є AWS Traffic Mirroring [10]. Даний підхід, який є частиною сервісу Amazon VPC, забезпечує можливість захоплювати та відтворювати мережевий трафік з мережевих інтерфейсів екземплярів Amazon EC2 у віртуальній приватній хмарі. Цей підхід використовується для наступних цілей:

- глибока перевірка пакетів, яка дозволяє детально аналізувати мережеві пакети з точки зору безпеки або для пошуку несправностей;
- виявлення та запобігання вторгненням – полегшує виявлення зловмисних дій, надсилаючи захоплений трафік до пристроїв безпеки;
- моніторинг мережі – допомагає діагностувати проблеми мережі, надаючи доступ до фактичного мережевого трафіку;
- відповідність стандартам та аудит – допомагає відповідати нормативним вимогам шляхом моніторингу та реєстрації мережевих з'єднань.

Альтернативою AWS Traffic Mirroring в середовищі Azure є Azure Network Watcher [11]. Цей сервіс дещо відрізняється за принципом роботи, але пропонує схожі інструменти. Один з них це Topology, який забезпечує візуалізацію всієї мережі для розуміння конфігурації мережі та надає інтерактивний інтерфейс для перегляду ресурсів та їхніх з'єднань у середовищі. Наступний сервіс це Connection monitor – він забезпечує наскрізний моніторинг з'єднань для Azure і гібридних кінцевих точок. Це допомагає зрозуміти продуктивність мережі між різними кінцевими точками у мережевій інфраструктурі.

Пенетраційне тестування в хмарних середовищах є необхідною складовою інформаційної безпеки і сприяє виявленню та усуненню вразливостей в хмарних середовищах. Воно дозволяє зрозуміти, наскільки добре захищене середовище та чи є в ньому потенційні точки входу для зловмисників.

Пенетраційне тестування в хмарних системах мають свої особливості порівняно з традиційними мережами і вимагають спеціального підходу до тестування. Однією з таких особливостей є розподілені ресурси. Як відомо хмарна інфраструктура складається з віртуальних мереж, баз даних, обчислювальних ресурсів тощо, що можуть бути розміщені в різних регіонах. Відомо, що хмарні середовища мають модель спільної відповідальності [12], при якій хмарні провайдери відповідають за безпеку хмарної інфраструктури (безпека фізичних серверів, мереж, основних сервісів), а клієнт відповідає за безпеку своїх даних та додатків. Доцільним є зауважити, що на тестування можуть впливати обмеження з боку провайдера. Деякі дії під час тестування, наприклад, тестування DDoS або зміна налаштувань мережі, можуть бути заборонені провайдером, і їх необхідно узгоджувати.

Окремо слід відмітити, що аналіз вразливостей в приватних хмарних середовищах (on-premise) також є критично важливим для забезпечення безпеки інфраструктури та даних. Приватні хмарні середовища поєднують в собі переваги публічних хмарних середовищ та контроль, який надає власна інфраструктура. Однак це зазвичай накладає додаткову відповідальність за безпеку. Відомо, що в таких середовищах модель спільної відповідальності [13] побудована таким чином, що більша частина відповідальності за інформаційну безпеку покладається на замовника, а ніж на провайдера послуг. Наприклад, для забезпечення автоматизованого сканування на вразливості необхідно вдаватися до використання сторонніх сервісів, таких як OpenVAS, QualysGuard, Nessus тощо. З іншого боку, такі методи аналізу вразливостей, як пенетраційне тестування та DevSecOps підхід, будуть однаково корисні як для публічних, так і для приватних хмарних середовищ.

Провідну роль в забезпеченні інформаційної безпеки в хмарних середовищах відіграє DevSecOps підхід. Він базується на інтеграції інструментів безпеки в процес розробки та розгортання програмного забезпечення, який допомагає виявляти вразливості на ранніх етапах розробки. Впровадження DevSecOps підходу допомагає зменшити ризики безпеки завдяки наступним властивостям [14]:

- зменшення кількості вразливостей, зловмисного коду та інших проблем безпеки в програмному забезпеченні, що розробляється, без уповільнення виробництва та виробництва коду;
- зменшення потенційного впливу використання вразливостей протягом життєвого циклу програмного забезпечення за рахунок використання переваг сучасних та інноваційних технологій;

- усунення вразливостей і попередження їх повторної появи, наприклад, шляхом впровадження сучасних технологій тестування, вдосконалення практик розробки коду та роботи з хмарними сервісами;
- зменшення конфліктів між людьми, щоб розробники, фахівці з безпеки та оперативний персонал могли знайти спільну мову для підтримки швидкості та гнучкості, необхідних для підтримки місії організації.

Таким чином, за результатами дослідження визначено, що сучасний підхід до аналізу вразливостей, як в публічних так і в приватних хмарних середовищах, потребує комплексного підходу, який включає автоматизацію, безперервний моніторинг, пенетраційне тестування та інтеграцію з практиками DevSecOps. Інструменти, такі як Amazon Inspector, GuardDuty, AWS Config, IAM Access Analyzer та сторонні рішення (наприклад, OpenVAS, QualysGuard, Nessus), відіграють важливу роль у забезпеченні виявлення, пом'якшення та управління вразливостями в реальному часі в хмарних середовищах. Інтеграція аналізу вразливостей безпосередньо в процес розробки та розгортання програмного коду та інструменти моніторингу безпеки значно знижують ризики інформаційної безпеки в сучасних хмарних середовищах.

Література

1. Amazon Inspector Documentation. Режим доступу: https://docs.aws.amazon.com/inspector/
2. AWS Config Documentation. Режим доступу: https://docs.aws.amazon.com/config/
3. Amazon GuardDuty Documentation. Режим доступу: https://docs.aws.amazon.com/guardduty/
4. AWS Security Hub Documentation. Режим доступу: https://docs.aws.amazon.com/securityhub/
5. AWS Identity and Access Management Access Analyzer Documentation. Режим доступу: https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html
6. Microsoft Defender for Cloud documentation. Режим доступу: https://learn.microsoft.com/en-us/azure/defender-for-cloud/
7. Microsoft Sentinel documentation. Режим доступу: https://learn.microsoft.com/en-us/azure/sentinel/
8. AWS CloudWatch Documentation. Режим доступу: https://docs.aws.amazon.com/cloudwatch/
9. Azure Monitor documentation. Режим доступу: https://learn.microsoft.com/en-us/azure/azure-monitor/
10. What is Traffic Mirroring? Режим доступу: https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html
11. Network Watcher documentation. Режим доступу: https://learn.microsoft.com/en-us/azure/network-watcher/
12. Shared Responsibility Model. Режим доступу: https://aws.amazon.com/compliance/shared-responsibility-model/
13. Understanding the Shared Responsibilities Model in Cloud Services. Режим доступу: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/understanding-the-shared-responsibilities-model-in-cloud-services?utm_source=isaca_internal&utm_medium=share_link
14. Abed Saif Ahmed Alghawli, Tamara Radivilova, Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation, Alexandria Engineering Journal, Volume 107, 2024, Pages 136-149, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2024.07.036.