ВИЯВЛЕННЯ ТА ЗАХИСТ ВІД ХМАРНИХ ЗАГРОЗ: МЕТОДИ ДЛЯ ДИНАМІЧНИХ ІНФРАСТРУКТУР

Ворошилов А.О., Заніздра П.Ю., Солоніченко О.О., Талипов І.В., Шевченко І.О.

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

E-mail: anton.voroshylov@nure.ua, pavlo.zanizdra@nure.ua, oleksii.solonichenko@nure.ua, ihor.talypov@nure.ua, illia.shevchenko1@nure.ua

Abstract

As cloud environments transition to dynamic API-oriented infrastructures, traditional perimeter-based security models are insufficient. This paper highlights the problems of shared responsibility and multi-user models and provides solutions for detecting threats using the latest methods. It provides scenarios of typical and malicious cloud security incidents based on breach investigations and threat analysis. Analysing these vectors, the paper provides recommendations for implementing a robust security system, emphasising the integration of behavioural analysis, artificial intelligence-based automation, and comprehensive visibility to protect modern cloud environments from complex threats.

Вступ

На відміну від традиційної периметральної безпеки, хмарне виявлення загроз працює з розподіленими робочими навантаженнями, безсерверними функціями, контейнерами та мультихмарними розгортаннями. Проблема виходить за межі видимості, тому що у хмарі можна контролювати лише код, ідентичності та конфігурації, периметри зникають, вектори загроз множаться у службах, про існування яких можна навіть не знати [1]. Ефективне виявлення загроз у хмарі вимагає поведінкового аналізу, машинного навчання та автоматизованих засобів реагування, які розуміють ефемерні ресурси, атаки на основі API та модель спільної відповідальності, що визначає межі безпеки хмари [2].

Основною метою роботи є визначення методів виявлення та захисту від загроз у хмарних середовищах, виявлення критичних точок відмови в традиційних підходах до безпеки при їх застосуванні в динамічних хмарних середовищах, а також надання ркомендацій для впровадження ефективних заходів безпеки на основі штучного інтелекту.

Традиційний захист периметра є недостатнім, оскільки змінилися основні принципи. Застарілі інструменти лише посилюють проблему. Якщо ввести події AWS CloudTrail у локальну систему SIEM можна побачити як зламаються парсери, панелі інструментів заповняться незнайомими полями, та інші компоненти системи захисту порушаться [3]. Таким чином виникла множина викликів щодо створення систем захисту інформації в хмарних середовищах, основні з яких наведено нижче [4].

Виклик телеметрії**:** телеметрія виглядає звичною, але контроль зник. Традиційні інструменти передбачають фіксовані периметри, повний доступ до гіпервізора та передбачувані мережні шляхи. Сучасні хмарні середовища усувають ці припущення завдяки багатокористувацькому доступу, постійній зміні IP-простору та моделям спільної відповідальності, які покладають конфігурацію та захист ідентичності безпосередньо на відділ захисту інформації.

Масштаб і складність: хмарні середовища можуть перевантажити традиційні підходи до моніторингу хмарної безпеки. Віртуальні машини з’являються і зникають за лічені хвилини, ідентичності поширюються по регіонах, а безсерверні функції виконуються мільйони разів щодня. Статичне виявлення на основі сигнатур не витримує такого обсягу і швидкості.

Розширення поверхні атаки: виникнення нових поверхонь атаки, кожна з яких працює інакше, ніж традиційні вразливості програмного забезпечення, включаючи:

– дані для навчання, які можуть бути зіпсовані зловмисниками;
– ваги моделей, які можуть викрасти інсайдери;
– кінцеві точки виведення, вразливі до швидкого введення;
– ненадійні рівні взаємодії людини та штучного інтелекту (ШІ), де надмірна залежність створює цикли автоматизації.

Хмарні рішення для захисту від просунутих загроз використовують поведінковий аналіз та машинне навчання для обробки мільярдів подій та виявлення найменших аномалій у реальному часі. Виявлення загроз на основі ШІ скорочує час перебування в гібридних та мультихмарних середовищах завдяки поведінковому аналізу невідомих загроз.

Хмара постійно піддається атакам, але легко недооцінити, як часто ці атаки досягають успіху в виробничих середовищах [5]. На основі розслідувань порушень було визначено шість критичних сценаріїв загроз, які наведено нижче.

1. Бічне переміщення: використання надпривілейованих облікових записів служб (ролі IAM, токени OAuth) для непомітного переміщення між проектами.

2. Атаки на ланцюжок постачання: отруєння образів контейнерів у публічних реєстрах для отримання доступу на рівні коду через конвеєри CI/CD.

3. Витік даних: використання неправильно налаштованого сховища (наприклад, відкритих S3-бакетів) для обходу традиційних правил DLP.

4. Використання API: компрометація неавтентифікованих API мікросервісів для перенаправлення східно-західного трафіку до внутрішніх баз даних.

5. Нативне програмне забезпечення-вимагач: націлювання на знімки, що управляються провайдером, для шифрування або видалення за допомогою скриптових інструментів CLI.

6. Атаки на федерацію ідентифікацій: використання фішингових токенів для розблокування міжхмарних ресурсів, пов’язаних через SAML/OIDC.

Ефективний захист хмарної безпеки вимагає постійного аудиту конфігурації, аналізу з урахуванням ідентифікаційних даних та автоматизованого обмеження, яке розуміє мінливу, орієнтовану на API природу сучасної інфраструктури.

Модель спільної відповідальності. Порушення починаються з неправильного розуміння моделі спільної відповідальності, невидимої межі, що розділяє те, що забезпечує безпеку постачальник, і те, що споживач повинен захищати [6]. Ця межа змінюється залежно від послуг, регіонів та окремих викликів API, створюючи плутанину, якою користуються зловмисники.

Відповідальність постачальника: Постачальники зміцнюють фізичні центри обробки даних, мережеву структуру та гіпервізори. Вони захищають інфраструктуру, на якій працюють робочі навантаження споживача, але не самі робочі навантаження, їх конфігурації або дані, які вони обробляють.

Відповідальність споживача: споживач налаштовує ідентичності, робочі навантаження та механізми захисту хмарної безпеки. Команди часто припускають, що оскільки Amazon, Microsoft або Google «володіють коробкою», вони також контролюють входи, виправляють гостьові операційні системи або шифрують сховища. Це не так. Це відповідальність споживача, і саме тут з'являються прогалини.

Сірі зони: відповідальність стає нечіткою на межі послуг. Керована контрольна площина Kubernetes є територією постачальника, але прив'язки ролей кластера та відкриті послуги належать споживачу. Вбудовані журнали існують за замовчуванням, але їх аналіз для отримання корисної інформації про загрози в хмарі – це робота споживача. Контроль зменшується, коли споживач переходить від IaaS до PaaS і SaaS, але відповідальність за дані та доступ ніколи не зменшується.

Інструменти безпеки, які передбачають повну відповідальність за стек, не враховують цих нюансів. Це створює сліпі зони, де надмірно привілейовані ідентичності, неправильно налаштовані контейнери та неконтрольовані API працюють непомітно [4]. Точне розуміння меж домену споживача та ретельний захист усього, що знаходиться в ньому, є єдиним шляхом до ефективного захисту.

Ідентифікація векторів загроз. На основі розслідувань порушень і розвідки було визначено критичні сценарії загроз:

– бічне переміщення: використання надпривілейованих облікових записів служб (ролі IAM, токени OAuth) для непомітного переміщення між проектами;
– атаки на ланцюжок постачання: отруєння образів контейнерів у публічних реєстрах для отримання доступу на рівні коду через конвеєри CI/CD;

– витік даних: використання неправильно налаштованого сховища (наприклад, відкритих S3-бакетів) для обходу традиційних правил DLP;

– використання API: компрометація неавтентифікованих API мікросервісів для переходу на східно-західний трафік до внутрішніх баз даних;

– нативне програмне забезпечення для вимагання викупу: націлювання на керовані провайдером знімки для шифрування або видалення за допомогою скриптових інструментів CLI;

– атаки на федерацію ідентифікацій: використання фішингових токенів для розблокування міжхмарних ресурсів, пов'язаних через SAML/OIDC.

Для вирішення проблем захисту було надано рекомендації, які наведено нижче.

– каталогізація активів: використання інструментів безперервного виявлення для інвентаризації всіх робочих навантажень, включаючи «тіньові» активи;

– блокування ідентичності: застосовування принципу мінімальних привілеїв, обов'язковість багатофакторної автентифікації та базових вимог на основі принципів нульової довіри;

– спостереження за всім: направлення необроблені події до SIEM і ввімкнення агентів моніторингу поведінки;

– уніфікація виявлень: інтеграція інформації про загрози з SOAR для централізованих операцій;

– захист за допомогою автоматизації: впровадити правила автоматизованого реагування для ізоляції робочих навантажень та скасування ключів.

Таким чином, ефективна безпека хмари вимагає фундаментального переходу від трактування хмари як аутсорсингового центру обробки даних до визнання її як окремого, орієнтованого на API операційного середовища. Модель спільної відповідальності вимагає від організацій суворого захисту ідентичностей, конфігурацій та даних, оскільки провайдери забезпечують безпеку лише базової фізичної інфраструктури.

Успіх у сучасній хмарній обороні залежить від постійного аудиту конфігурацій, аналізу з урахуванням ідентичності та автоматизованих можливостей локалізації. Дотримуючись структурованого шляху впровадження та уникаючи типових помилок, таких як покладання виключно на інструменти постачальника або ігнорування людського фактору, організації можуть створити адаптивну оборону, здатну протистояти складним, високошвидкісним загрозам сучасного цифрового середовища.

*Л*ітература

1. Nzeako G., Shittu R. A. Implementing zero trust security models in cloud computing environments / G. Nzeako, R. A. Shittu. *World Journal of Advanced Research and Reviews*. 2024. № 24(03). Pp. 1647-1660. DOI: 10.30574/wjarr.2024.24.3.3500.

2. Sreerangapuri A., Kombathula A. Zero Trust Security Model in Infrastructure Transition: Best Practices for Securing Cloud and Hybrid Environments /A. Sreerangapuri, A. Kombathula. *Neuroquantology*. 2022. №20(6). Pp. 101630-101636. DOI: 10.48047/nq.2022.20.6.NQ23044

3. Shah, M. Cloud Native Software Security Handbook: Unleash the Power of Cloud Native Tools for Robust Security in Modern Applications. Germany: Packt Publishing, 2023. 372 p.

4. Nomani, Q. Mastering Cloud Security Posture Management (CSPM): Secure Multi-cloud Infrastructure Across AWS, Azure, and Google Cloud Using Proven Techniques. Germany: Packt Publishing. 2024. 472 p.

5. Alghawli, A. S. A., Radivilova, T. Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation / A. S. A. Alghawli, T. Radivilova. *Alexandria Engineering Journal*. 2022. №107. Pp. 136-149. DOI:10.1016/j.aej.2024.07.036.

6. Mettu B.P.R. Beyond the Perimeter: A Comparative Analysis of Zero Trust Framework Implementations in Hybrid Enterprise Environments, *European Journal of Computer Science and Information Technology,* 2025. № 13(44). Pp.68-83. DOI: 10.37745/ejcsit.2013/vol13n446883