УДК 004.75

Найпоширеніші проблеми кібербезпеки в хмарних середовищах

Максим Боровський
Андрій Аносов[0000-0002-2973-6033]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. Хмарні обчислення пропонують масштабованість, економічну ефективність та оптимізацію ресурсів, а також можливість вирішувати всі типи проблем, але це також створює нові проблеми безпеки. Огляд обговорює основні загрози безпеці та їх застосування до хмарних та інших систем у цій статті, зосереджуючись на інфраструктурі, даних, прикладному та управлінському рівнях.
Ключові слова: хмарні обчислення, кібербезпека, помилки конфігурації, AWS.

Common Cybersecurity Problems in Cloud Environments

Maksym Borovskyi
Andrii Anosov[0000-0002-2973-6033]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. Cloud computing offers scalability, cost efficiency, and resource optimization, as well as the ability to address a wide range of computational challenges. However, it also introduces new security issues. This review discusses the main cybersecurity threats and their relevance to cloud and other distributed systems, focusing on the infrastructure, data, application, and management layers.
Keywords: cloud computing, cybersecurity, misconfigurations, AWS.

Вступ

За останні кілька років організації масово мігрують свої робочі навантаження до хмарних інфраструктур (IaaS, PaaS, SaaS). Хоча хмарна модель дозволяє динамічне розподілення ресурсів та управління масштабованістю, з'являються нові вектори атак, які суттєво відрізняються від старих систем на фізичних серверах. Хмарні середовища, незважаючи на численні переваги, піддають нас конфігураційним помилкам, ризикам багатокористувацької архітектури, недолікам управління доступом та витокам даних. Згідно з опитуванням Cloud Security Alliance (2024), понад 77% установ відчувають себе непідготовленими до ефективного реагування на загрози безпеці в хмарі [1].

Метою цієї роботи є організація та аналіз основних проблем кібербезпеки хмарного середовища для систематичного та всебічного аналізу, їх класифікація, аналіз контрзаходів та побудова повної інтегрованої моделі безпеки для забезпечення багаторівневого захисту хмарної інфраструктури.

Методи

Систематичний огляд був проведений на літературі між 2015-2025 роками. IEEE Xplore, ACM DL, ScienceDirect, arXiv, Google Scholar були використаними базами даних.

Залежність від опублікованих матеріалів - потенційне пропущення неопублікованих даних. Опитування мають статистичні помилки. Воно не спирається на експериментальні перевірки; воно аналітичне за своєю природою.

Результати

Класифікація основних проблем безпеки:

1. Помилки конфігурації

У хмарі однією з найпоширеніших проблем безпеки є помилки в конфігурації. Порушення даних у публічних хмарах більш ніж на 82% пов'язані з неправильними налаштуваннями в службах зберігання або мережевих налаштуваннях [2].

Типові ризики:

- відкриті S3 бакети в AWS з публічним доступом «Everyone»;
- погана політика в Security Groups (0.0.0.0/0 для SSH або RDP);
- відсутність шифрування TLS на з'єднаннях між пристроями;
- неконтрольований доступ до кластерів Kubernetes або реєстрів Docker;
- недотримання політик IAM з мінімальним доступом.

Причинами є людський фактор, складність інтерфейсів управління, кількість регіонів і ресурсів, обмежений контроль шаблонів IaC (Terraform, CloudFormation), що викликає систематичні помилки.

В наслідок маємо те, що приватні данні чи інтерфейси стають публічними, хоча не планувались такими і відкривають новий вектор атак для потенційних зловмисників. Оскільки помилки цього типу дуже поширені і досить схожі між собою зловмисники використовують автоматизовані сканери для пошуку і подальшого аналізу.

Методи виявлення та запобігання:

- (OPA, HashiCorp Sentinel) застосування політик як коду;
- встановлення періодичного сканування конфігурацій (AWS Config, Prisma Cloud, Checkov);
- шифрування даних у стані спокою (AES-256) та під час передачі (TLS 1.3);
- забезпечення політики хмарних середовищ для автоматичного блокування відкритих портів або бакетів.

2. Ризики спільної інфраструктури

Модель багатокористувацькості лежить в основі більшості пропозицій хмарних сервісів. Існують десятки або сотні різних клієнтів, які володіють віртуальними машинами, що розміщуються на одному фізичному хості, кожна з власним набором ресурсів і розміром системи. Це залишає можливість для порушення меж безпеки шляхом спільного використання ресурсів: CPU, пам'яті, кешів, мережевих адаптерів.

Типові ризики:

- атаки через побічні канали через кеш процесора (Spectre, Meltdown, L1TF);
- втеча з гіпервізора — зловживання вразливостями Xen, KVM, VMware ESXi;
- атаки через спільні області пам'яті або доступ DMA;
- вихід з контейнера — перехід з контейнера Docker на хост [3].

В наслідку маємо що зловмисник на тому ж хості може навіть спостерігати за поведінкою CPU або пам'яті, що може розкрити криптографічні ключі або шаблони доступу. Це підриває модель «ізоляції тенантів», яка передбачає довіру до провайдера. В найгіршому випадку отримуючи доступ до хоста зловмисник може отримати доступ до інших контейнерів, що відпрацьовують поруч з його ресурсами, також потенційно маючи доступ до оточення і змінних, котрі є на хості можна отримати подальший доступ до захищених мереж і баз даних [4].

Заходи, які захищають від такої атаки: оновлення гіпервізорів і мікрокоду процесора; технології конфіденційності (AMD SEV, Intel TDX) для розділення ресурсів та апаратна сегментація ВМ окремих клієнтів; контроль доступу до гіпервізора та журналювання кожної операції ВМ, сегментація віртуальних ресурсів і контроль доступів, не надавати зависоких доступів віртуальним контейнерам.

3. Збої систем управління ідентифікацією та доступом (IAM)

Механізми IAM є важливою частиною безпеки хмари. Але вони часто є джерелом порушень. Одне дослідження Cloud Security Alliance (2024) показало, що 58% організацій мають принаймні один інцидент, коли була зроблена неправильна конфігурація IAM.

Типові ризики:

- для забезпечення щоденних операцій використовуйте основний (або «root») обліковий запис;
- відсутність багатофакторної автентифікації (MFA);
- надмірні політики AdministratorAccess;
- передача облікових даних у Git репозиторії;
- неконтрольований доступ до токенів API та службових ролей.

Зловмисники можуть отримати доступ до відкритих репозиторіїв із закоміченими токенами AWS або GCP, розгортаючи власні ресурси (наприклад, для майнінгу криптовалют або витоку даних). Часто атака починається з фішингового електронного листа, що імітує повідомлення від CSP (Cloud Service Provider). Дуже частою є проблема, коли розробники додають AWS секрети в публічний репозиторій під час розробки, далі публічні сканери зловмисників знаходять код по знайомому шаблону і використовують його в своїх цілях

Наслідками може бути проникнення зловмисника в приватний контур інфраструктури з подальшим зломом/видаленням/майнінгом. В найгіршому випадку може бути доданий юзер з адміністративним доступом і його секрети закинуті в репозиторій, в такому випадку зловмисники будуть мати повний доступ до інфраструктури, баз даних і коду додатків.

Захиститись від цього можна за допомогою MFA доступу для всіх користувачів, принципом найменших привілеїв, регулярний аудит політик IAM, використання токенів замість звичайних юзерів [5]. На всіх сучасних популярних хмарах є можливість використовувати системні ролі для доступу між сервісами, так можна передати контроль на сторону хмари і контролювати чисто складову політики. Для захисту від потрапляння токенів в репозиторій варто використовувати автоматичні сканери коду, котрі можуть сповістити про компрометацію ключів у випадку випадкового потрапляння.

4. Витоки даних та порушення конфіденційності

Витоки даних залишаються великою проблемою для середньостатистичної організації, що базується на публічній хмарі. Невдача у захисті персональних або комерційно чутливих даних може спричинити не лише фінансові втрати, але й призвести

до юридичних проблем відповідно до GDPR або CCPA, включаючи юридичні наслідки, а також репутаційні і фінансові.

Механізми витоку:

- відкритий доступ до сховищ (S3, Azure Blob, GCS Buckets);
- помилки в політиках IAM;
- MITM атаки при мережевому доступі без TLS;
- слабкі місця API, які компрометують (наприклад, GraphQL з неавтентифікованою кінцевою точкою);
- незнищені знімки або резервні копії.

Найпростішим варіантом захисту є підхід «шифрувати все», на щастя хмарні провайдери нам пропонують достатньо легкі у інтеграції способи додати шифрування як в кінці, так і в транзиті для більшості готових хмарних сервісів. Для ротації старих резервних копій існують також механізми, котрі дозволяють просто поставити термін «життя» і надалі копія буде автоматично видалена через певний час.

5. Інсайдерські загрози

Інсайдери — співробітники або адміністратори компаній, що мають легальний доступ, але використовують його зловмисно або недбало. Це також можуть бути рядові співробітники, котрі отримали забагато доступу через відсутності політики least privilege access.

На відміну від зовнішніх атак, такі дії важко виявити через те що поведінка інсайдера виглядає нормальною, оскільки може розцінюватись як його звичайна робота [6].

Є 3 основні типи інсайдерів:

1. Інсайдер-Зловмисник – співробітник, котрий з корисною метою вирішив викрасти чи пошкодити дані, або шкодить системі надаючи доступ третім особам.
2. Недбалий інсайдер – співробітник, котрий створює проблему, або вразливість несвідомо через недостатню кваліфікацію, або через недбалість [7].
3. Компрометований інсайдер – співробітник, чиї дані викрадено, або його робочий комп’ютер скомпрометовано і зловмисник мають доступ від його іменіх [8].

Для захисту від інсайдерських атак можна використовувати AI/ML моделі, котрі будуть шукати аномалії в аудит логах системи і можуть попереджати про ранішні аномалії пов’язані з користувачем. Least privilege access для всіх співробітників і користувачів системи, це може допомогти звузити радіус атаки навіть у випадку компрометації [9–13].

Обговорення

Кожен варіант наведеного захисту також має свої недоліки, котрі починаються від дороговизни розробки, інтеграції і підтримки. Для найкращого покриття наявних загроз у випадку автоматичних сканерів варто дивитись на великих гравців на ринку кібербезпеки, оскільки збір і аналіз інформації про актуальні загрози потребує великих ресурсів на підтримання актуальності інформації. Навіть при умові якщо провайдер надає всі потрібні інструменти завжди існують певні обмеження на кількість логів чи подій, котрі будуть оброблені, залежно від заключеного контракту. Також треба враховувати що з нашої сторони теж треба виділяти час і ресурси для інтеграції стороннього сервісу в екосистему.

Будь який аналіз, логи, запис подій для будь-якої системи сповільнює її. Для розробки найкращим варіантом буде “shift left” стратегія, де задача автоматичних перевірок буде повідомити про потенційну загрозу якомога раніше в процесі розробки, а не на фінальному етапі. Також іде сповільнення в швидкості розробки і підвищується вартість

додавання нового функціоналу, оскільки командам розробки треба буде довше налаштовувати інфраструктуру для правильної і безпечної взаємодії.

Також коли в систему додано шифрування з'являється нова потреба в інструментах для дешифрування, оскільки в процесі роботи може виникнути потреба працювати з зашифрованими даними, чи потреба розгорнути зашифровану копію.

Висновки

Проведене дослідження дало змогу узагальнити найважливіші проблеми кібербезпеки, з якими стикаються організації під час експлуатації хмарних середовищ. Аналіз літератури, галузевих звітів і реальних інцидентів показав, що питання захисту даних у хмарі залишається одним із найскладніших у сучасній цифровій інфраструктурі. Незважаючи на технологічну зрілість великих постачальників хмарних сервісів, кількість інцидентів, пов'язаних із людськими помилками, конфігураційними прорахунками та неправильним управлінням доступом, продовжує зростати.

Характерною рисою більшості виявлених проблем є те, що вони виникають не через недоліки самої технології, а через її складність і недостатній рівень організаційного контролю. Помилки конфігурації, зокрема відкриті сховища або неправильно визначені правила доступу, стають одним із головних чинників витоків даних. Водночас архітектурна особливість багатокористувацьких середовищ створює потенційну небезпеку перетину ізоляційних меж між віртуальними ресурсами, що може призвести до порушення цілісності інформації.

Проблеми керування ідентичністю й правами користувачів залишаються критично важливими для будь-якої хмарної платформи. Надмірні дозволи, відсутність багатофакторної автентифікації чи нехтування ротацією ключів відкривають шлях до компрометації інфраструктури. Дослідження також засвідчило, що навіть у випадку коректної конфігурації ризик витоку даних не зникає повністю — він переноситься у площину людського фактору. Інсайдерські загрози, як свідомі, так і випадкові, є особливо небезпечними через складність їхнього виявлення та контрольованості.

Загалом можна стверджувати, що безпека хмарних середовищ формується не лише за рахунок технічних засобів, а передусім завдяки постійному управлінню ризиками та чітко визначеній відповідальності між клієнтом і провайдером. Модель спільної відповідальності, яку декларують більшість хмарних постачальників, потребує реального практичного впровадження, а не формального прийняття. Саме від цього залежить ефективність захисних механізмів і здатність організації запобігати інцидентам.

Перспективним напрямом подальших досліджень є створення систем автоматичного аналізу конфігурацій та поведінкових аномалій у хмарі, здатних виявляти ризики ще до того, як вони призводять до інцидентів. Особливу увагу також варто приділити питанням побудови довіри у середовищах з кількома користувачами, а також розробці підходів до виявлення інсайдерських дій без порушення конфіденційності працівників.

Таким чином, можна зробити висновок, що хмарна безпека сьогодні є не стільки технічною проблемою, скільки управлінською дисципліною, яка потребує постійного аналізу, навчання персоналу та вдосконалення процесів. Лише системний і безперервний підхід, який об'єднує технології, політики та людський чинник, може забезпечити належний рівень захисту даних у хмарних екосистемах.

Джерела

1. Cloud Security Alliance. (2023, August 14). Managing cloud misconfigurations risks. Retrieved from https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks

2. Alquwayzani, A., Aldossri, R., & Frikha, M. (2024). Prominent security vulnerabilities in cloud computing. International Journal of Advanced Computer Science and Applications, 15(2), 112–120. https://doi.org/10.14569/IJACSA.2024.0150281

3. SentinelOne. (2025, August 8). 17 security risks of cloud computing in 2025. SentinelOne Cybersecurity 101. Retrieved from https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/

4. Kazdagli, M., Tiwari, M., & Kumar, A. (2024). CloudLens: Modeling and detecting cloud security vulnerabilities. arXiv preprint arXiv:2402.10985. https://arxiv.org/abs/2402.10985

5. Wiz. (2025, August 12). Top 11 cloud security vulnerabilities and how to fix them. Wiz Academy. Retrieved from https://www.wiz.io/academy/common-cloud-vulnerabilities

6. Fortinet. (2025, January 15). Navigating today's cloud security challenges. Fortinet Blog. Retrieved from https://www.fortinet.com/blog/business-and-technology/navigating-todays-cloud-security-challenges

7. Inayat, U., Anwar, Z., & Malik, A. (2024). Systematic literature review on cloud computing security: Threats, mitigations, and trends. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4775074

8. CloudComputing-News. (2024, July 10). 10 real-life cloud security failures and what we can learn from them https://www.cloudcomputing-news.net/news/10-real-life-cloud-security-failures-and-what-we-can-learn-from-them

9. ISC2. (2021, October 26). Insider threats can turn your cloud security into a storm. Retrieved from https://www.isc2.org/Insights/2021/10/insider-threats-can-turn-your-cloud-security-into-a-storm

10. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

11. Складанний, П., Гулак, Г., & Корнієць, В. (2025). Коаліційний підхід до управління кібербезпекою інформаційних систем що застосовують хмарні технології. Кібербезпека: освіта, наука, техніка, 4(28), 8–25. https://doi.org/10.28925/2663-4023.2025.27.825

12. Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка, 4(28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857

13. Складанний, П., Костюк, Ю., Мазур, Н., & Пітайчук, М. (2025). Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології, 1(86), 61–74. https://doi.org/10.31673/2412-4338.2025.014649