УДК 004.738.5

В. І. Кубіря
А. В. Грицак

ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ КІБЕРЗАХИСТУ ХМАРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ШЛЯХОМ ЗАБЕЗПЕЧЕННЯ НЕЗМІННОСТІ ЖУРНАЛІВ ПОДІЙ У ХМАРНИХ СЕРЕДОВИЩАХ

Вінницький національний технічний університет

Анотація

У дослідженні розглянуто проблему компрометації журналів подій у хмарних середовищах як одного з критичних факторів зниження ефективності систем кіберзахисту. Проаналізовано сучасні сценарії атак, що передбачають модифікацію або підробку логів, зокрема вразливості в інструментах централізованого логування. Обґрунтовано необхідність забезпечення цілісності та достовірності журналів подій. Запропоновано підходи до підвищення захищеності логування на основі використання можливостей хмарних платформ, зокрема незмінного зберігання даних, розподілених архітектур та ізоляції середовищ.

Ключові слова: хмарні обчислення, журнали подій, цілісність даних, кіберзахист, інформаційна безпека.

Abstract

The thesis considers the problem of event log compromise in cloud environments as one of the critical factors reducing the effectiveness of cybersecurity systems. Modern attack scenarios involving log modification or forgery are analyzed, including vulnerabilities in centralized logging tools. The necessity of ensuring the integrity and reliability of event logs is substantiated. Approaches to enhancing logging security based on cloud platform capabilities are proposed, including immutable data storage, distributed architectures, and environment isolation.

Keywords: cloud computing, event logs, data integrity, cybersecurity, log tampering, information security.

Вступ

Одна з потенційних загроз, пов'язаних із порушеннями безпеки в хмарі, полягає в можливості маніпулювання журналами подій, які надають докази для моніторингу, виявлення атак та проведення розслідувань інцидентів. Цей тип загрози становить особливо серйозний ризик для систем, які обробляють критичну або конфіденційну інформацію; порушення цілісності журналів подій значно ускладнить виявлення будь-якої несанкціонованої діяльності; і, отже, значно обмежить здатність реагувати на інциденти.

Тим часом, платформи, що працюють у хмарах, дозволяють користувачам зберігати дані у незмінному вигляді; це досягається завдяки реалізації концепції одноразового запису, багаторазового читання, яка додатково захищає журнали подій від несанкціонованих змін або видалення. Метою цього дослідження є обґрунтування методів, які допоможуть підтримувати архівування та достовірність файлів журналів у хмарних умовах для підвищення ефективності механізмів кіберзахисту від сучасних кібератак.

Результати дослідження

Аналіз нещодавніх інцидентів у хмарній безпеці показує, що модифікація журналів подій є ефективним методом приховування кібератак. У 2025 році у Fluent Bit було виявлено серйозні вразливості. Fluent Bit – це інструмент збору та пересилання журналів, який використовується контейнерами та хмарними середовищами. Деякі критичні вразливості дозволяли зловмисникам повністю перезаписувати файли журналів. Крім того, деякі вразливості дозволяли зловмисникам вставляти фальшиві записи журналу в файли журналів та обходити перевірки автентифікації під час передачі телеметрії [1]. Зловмисник, який має можливість створювати та змінювати файли журналів, може приховувати власну діяльність.

Зламана система ведення журналу призведе до браку довіри не лише всередині системи ведення журналу, але й у процесі виявлення інцидентів. Це означає, що коли організація отримує доступ до своїх журналів, вона робить це з можливістю того, що ці журнали могли бути підроблені після факту. Це

включає будь-які розслідування, що тривають, та використання цих журналів як доказів для підтвердження або спростування того, що сталося під час події безпеки. Використання централізованої агрегації та зберігання журналів у хмарних середовищах робить цей ризик ще серйознішим, оскільки один вузол збору або архівування журналів може вплинути на значну частину середовища, якщо зловмисник зможе успішно отримати доступ.

Для того щоб усунути ризик приховування доказів доступу, слід використовувати механізм накопичення копій журналів доступу, які не можна буде змінити після їх накопичення хмарою. Цей механізм дозволить вільно записувати журнали, але запобігатиме їх редагуванню, перезапису або видаленню після запису протягом певного періоду зберігання. Один із способів зробити це – використовувати рішення для зберігання, яке працює в режимі одноразового запису та багаторазового читання (захист WORM). За допомогою цього типу сховища, після створення об'єкта його не можна змінити або видалити, доки не закінчиться заданий час зберігання [2], тому можна безпечно зберігати будь-який журнал подій, який був створений, доки не закінчиться встановлений період зберігання, що забезпечує більшу достовірність та цілісність журналів доступу, навіть якщо хмара частково порушена. Це особливо важливо під час реконструкції часової шкали злому. Можна відстежувати початок вторгнення, переглянувши вузол або обліковий запис, до якого було здійснено доступ першим, які команди або служби використовувалися, які ресурси були вражені та в який момент було надано додатковий доступ, переглядаючи незмінні журнали.

Щоб максимізувати свій захист, слід розглянути можливість впровадження моніторингу криптографічної цілісності для доповнення незмінності збережених даних шляхом виконання перевірок на основі хешування та створення хеш-ланцюжків, де кожен новий запис, що хешується, пов'язаний з попереднім записом. Це ускладнює видалення або зміну однієї події без її виявлення. Будь-які зміни в журналі порушують цілісність журналу та будуть виявлені під час процесу перевірки.

Окреме значення цей підхід має для відновлення хронології вторгнення. Незмінні логи дозволяють визначити, з якого саме вузла чи облікового запису почалося проникнення, які команди чи сервіси застосовувалися далі, які ресурси були зачеплені та на якому етапі відбулося поширення доступу. Водночас для посилення захисту варто доповнювати незмінне накопичення криптографічним контролем цілісності, зокрема хешуванням записів та формуванням хеш-ланцюжків, у яких кожний наступний запис пов'язується з попереднім. У такому разі непомітне видалення чи зміна окремої події стає значно складнішим, адже будь-яке втручання руйнує послідовність журналу та може бути виявлене під час перевірки.

Ще один спосіб захистити дані – перенести журнали подій (архів) до окремого облікового запису або місця у хмарній інфраструктурі, яке не підключено до жодного з щоденних бізнес-процесів. Така ізоляція допомагає гарантувати, що навіть якщо у виробничому середовищі відбудеться компрометація, це не вплине на систему ведення журналу, таким чином створюючи бар'єр між місцем зберігання журналів та місцем походження подій [3]. Зрештою, якщо розділити адміністративні обов'язки разом із правами доступу, зменшиться ймовірність одночасної компрометації як основної служби, так і архівних журналів.

Використання технологій на основі реєстру, таких як розподілені записи, а також журнали аудиту на основі блокчейну для збору даних журналу аудиту з журналів подій, є життєздатним підходом до вдосконалення цієї практики. Розподілені платформи на основі блокчейну використовуються для зберігання хешів хмарних журналів подій, щоб забезпечити проведення судово-медичних перевірок, які можуть визначити, чи були журнали змінені з моменту їх першого запису. Це особливо важливо для систем, яким потрібен спосіб підтвердження автентичності результатів аудиту та процесів внутрішнього контролю, а також результатів розслідувань, проведених щодо інцидентів [4].

Якщо цілісність журналів подій встановлена, журнали подій необхідно постійно аналізувати тією ж системою моніторингу безпеки. Для досягнення цієї мети доступні системи SIEM та SOAR, які надають засоби для збору достовірної інформації про будь-яку подію, що відбувається в різних елементах хмарної інфраструктури; виявлення будь-яких незвичайних зв'язків між елементами; та дозволяють швидко реагувати на потенційно серйозні ситуації. Завдяки такому підходу можна фіксувати не лише окремі факти доступу чи зміни налаштувань, а й послідовність дій, що може вказувати на спробу атаки.

Висновки

Зміна журналів подій у хмарному середовищі, мабуть, є найбільшою загрозою для хмарних сервісів, оскільки, окрім того, що атака виглядає непомітною, інші форми атаки також роблять систему нездатною записувати атаку в міру її виникнення та не можуть бути використані для визначення того, що сталося. Якщо зловмисники можуть змінювати журнали подій, ці журнали більше не виконують свою основну функцію: надання достовірної інформації, яку можна використовувати для пошуку, розслідування та реагування на атаку. Таким чином, стає очевидним, що захист журналів не слід розглядати як додатковий захід, а слід сприймати як один з фундаментальних заходів безпеки, які можна використовувати для захисту хмарної інфраструктури. Тристороннє рішення, яке включає незмінне зберігання журналів, розділення архівів журналів та подальше звуження прав доступу до журналів, значно мінімізує ймовірність імітації, знищення та модифікації без дозволу. Отже, підвищення надійності журналів подій є дуже важливою вимогою для підвищення рівня кіберзахисту хмарних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. New Fluent Bit Flaws Expose Cloud to RCE and Stealthy Infrastructure Intrusions. The Hacker News. URL: https://thehackernews.com/2025/11/new-fluent-bit-flaws-expose-cloud-to.html? (дата звернення: 13.03.2026).
2. Locking objects with Object Lock - Amazon Simple Storage Service. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html (дата звернення: 16.03.2026).
3. Security Log Archive account - AWS Prescriptive Guidance. URL: https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/log-archive.html (дата звернення: 20.03.2026).
4. Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. NIST Special Publication 1800-25. URL: https://www.nccoe.nist.gov/publication/1800-25 (дата звернення: 25.03.2026).

Кубіря Варвара Іванівна - студентка, 1КІТС-23б, Вінницький національний технічний університет, м. Вінниця, e-mail: 07-23-250.stud@vntu.vn.ua.

Науковий керівник: Грицак Анатолій Васильович – доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Kubiria Varvara Ivanivna - student, Vinnytsia National Technical University, Vinnytsia, , e-mail: 07-23-250.stud@vntu.vn.ua.

Scientific supervisor: Hrycak Anatoliy Vasyliovych – Docent of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia.