ЗАКРИТИЙ ДОСТУП ДО СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ: МЕТОДИ ОБМЕЖЕННЯ ЗА ОБЛІКОВИМИ ЗАПИСАМИ ТА IP-АДРЕСАМИ

Яскевич Юрій Владиславович
аспірант групи ІБДдф-23-4.0д,
спеціальності 125 "Кібербезпека", Київського столичного університету імені Бориса Грінченка, науковий керівник – к.т.н., доц.Складаний П.М.

Забезпечення довіреного доступу до систем управління базами даних (СУБД) є фундаментальною задачею інформаційної безпеки. Несанкціонований доступ до критичних даних може призвести до фінансових та репутаційних втрат. Традиційні методи захисту, що базуються на автентифікації користувачів, є недостатніми без комплексного підходу, який включає мережеві обмеження [1]. Метою цього дослідження є систематизація практик, що поєднують фільтрацію за IP-адресами та прив'язку облікових записів до конкретних хостів, для створення надійної багаторівневої системи захисту.

Багаторівнева модель захисту та модель загроз

Розглядається клас загроз, пов'язаний із несанкціонованим віддаленим доступом, зокрема: підбір паролів (brute-force), компрометація облікових записів та їх неправомірне використання для просування всередині корпоративної мережі (lateral movement). Для протидії цим загрозам пропонується багаторівнева архітектура захисту, що реалізує принцип «глибокого захисту» (defense-in-depth).

Мережевий рівень (Firewall): Перший рубіж оборони. Його завдання – блокувати всі небажані з'єднання на порт СУБД на рівні мережевого периметра або хоста. Дозволи надаються лише для визначених IP-адрес або підмереж (наприклад, серверів додатків, VPN-шлюзів для адміністраторів).

Рівень сервісу (Слухач СУБД): Налаштування мережевого слухача (listener) СУБД для приймання з'єднань лише на конкретних мережевих інтерфейсах (наприклад, внутрішній IP-адресі 10.0.1.2), а не на всіх (0.0.0.0). Це унеможливлює доступ до СУБД ззовні, навіть якщо мережевий фільтр налаштовано неправильно.

Рівень СУБД (Автентифікація та авторизація): Внутрішні механізми контролю доступу самої СУБД. На цьому рівні конфігуруються правила, що дозволяють конкретному користувачеві підключатися лише з певного хоста. Це останній, але надзвичайно важливий бар'єр [2; 3].

Ефективність забезпечується лише при одночасному застосуванні всіх трьох рівнів. Компрометація одного з них не призводить до негайного несанкціонованого доступу.

Оцінка ефективності та операційні рекомендації

Запропонований підхід значно зменшує поверхню атаки, роблячи зовнішні сканування портів та атаки перебору паролів неефективними. Навіть у випадку компрометації облікових даних додатку, зловмисник не зможе підключитися до бази даних зі стороннього хоста. Однак існують і обмеження, як-от складність управління доступом для користувачів з динамічними IP-адресами, що вимагає

використання VPN або проміжних серверів (bastion hosts) [4; 5].

Ключові операційні рекомендації:

Політика «заборони за замовчуванням» (default deny): Дозволяти лише те, що є абсолютно необхідним.

Автоматизація: Використовувати системи управління конфігураціями (Ansible, Terraform) для розгортання та підтримки правил брандмауера та налаштувань СУБД. Це забезпечує відтворюваність та знижує ризик людської помилки [1; 6].

Моніторинг та аудит: Централізовано збирати журнали автентифікації та налаштовувати сповіщення про невдалі спроби входу. Регулярно проводити аудит облікових записів на наявність надлишкових привілеїв або занадто широких дозволів (наприклад, 'user'@'%' у MySQL).

Обмеження доступу до СУБД за обліковими записами та IP-адресами є ефективним методом захисту, що реалізує принципи найменших привілеїв та глибокої оборони. Його надійність залежить від системного застосування на всіх рівнях: від мережевого брандмауера до внутрішніх механізмів авторизації самої СУБД. Поєднання строгих правил фільтрації трафіку, коректного налаштування слухачів сервісу та гранулярних правил доступу на рівні користувачів створює стійку до атак інфраструктуру.

ДЖЕРЕЛА

1. OWASP Foundation. (2023). Database Security Cheat Sheet. [Електронний ресурс]: https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html

2. PostgreSQL 16 Documentation. (2024). Chapter 21. The pg_hba.conf File. [Електронний ресурс]: https://www.postgresql.org/docs/current/auth-pg-hba-conf.html

3. MySQL 8.0 Reference Manual. (2024). 6.2.4 Access Control, Stage 1: Connection Verification. [Електронний ресурс].: https://dev.mysql.com/doc/refman/8.0/en/connection-access.html

4. Center for Internet Security (CIS). (2023). CIS PostgreSQL 14 Benchmark v1.0.0. [Електронний ресурс]: https://www.cisecurity.org/benchmark/postgresql

5. Абрамов, В. О., Глушак, О. М., & Машкіна, І. В. (2025). Cisco Networking Academy як інструмент формування професійних компетентностей у студентів технічних спеціальностей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 29(1), 252-262.

6. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km