

ЗАГРОЗИ РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Кирина Д. В.

Національний аерокосмічний університет ім. М. Є. Жуковського
«ХАІ»

Науковий керівник Цуранов М. В.

Актуальність. За останні кілька років концепція хмарних обчислень і віртуалізації закріпилась та стала популярною у сфері інформаційних технологій. Мільйони користувачів та різноманітних організацій по всьому світу користуються хмарними технологіями для зберігання, обробки, використання чималої кількості даних. Оскільки, хмарні технології напряму пов'язані з Інтернетом, то для роботи з даними використовуються розподілені бази даних (РБД). Однією із важливих перевагою таких БД перед іншими є те, що РБД автоматично масштабують пропускну здатність для відповідей поточного робочого навантаження і здатні багатократно розбивати дані по мірі розширення таблиць, що значно підвищує доступність даних [1]. Найбільш популярними прикладами РБД можна вважати Torrent, Amazon DynamoDB, Azure Cosmos DB.

Метою даної роботи є аналіз вразливостей розподіленої бази даних.

Основні положення. Серед багатьох визначень РБД найбільш влучним є: розподілена база даних складається з двох чи більше частин, розташованих на різних серверах. Така база даних може зберігатися на кількох комп'ютерах [2].

РБД насправді є віртуальною базою даних, компоненти якої фізично зберігаються в декількох різних реальних базах даних на декількох різних вузлах (по суті, будучи логічним об'єднанням цих реальних баз даних). Фундаментальний принцип РБД ґрунтується на тому, що користувачі розподіленої системи повинні мати можливість діяти так, ніби система не є розподіленою [3]. Всі проблеми розподілених систем відносяться до проблем реалізації, а не до проблем рівня користувача.

Розподілена система має декілька точок входу, через які здійснюється доступ до даних. Чим більше в системі таких входів, тим гостріша проблема безпеки. При обробці інформації порушення її цілісності може виникнути внаслідок технічних несправностей, алгоритмічних та програмних помилок, помилок та деструктивних дій обслуговуючого персоналу, зовнішнього втручання, дії руйнівних та шкідливих програм (вірусів, експлойтів, черв'яків, логічних бомб) [4].

Аналізуючи функціональність РБД, було виявлено найчастіші загрози. Більшість загроз пов'язані з некоректною установкою та налаштуванням СУРБД адміністратором БД. СУРБД складається з єдиної логічної БД, розділеної на кілька фрагментів [5]. Прикладами найбільш розвинутих СУРБД є система R*, SDD-1, Distributed Ingres, BigTable.

Найпоширеніші з них: загрози перехоплення інформації у незахищених каналах зв'язку та мережах загального доступу; загрози впливу ШПЗ; загрози в системах автентифікації та авторизації; атака 51%; віддалені атаки на інфраструктуру (під інфраструктурою мережі слід розуміти сформовану систему організації відносин між об'єктами мережі та сервісні служби, що використовуються в мережі) і протоколи мережі (2PC, протокол двухфазної фіксації транзакцій, Frame Relay); атака на один із вузлів мережі (атака Eclipse).

Висновки. Оскільки, РБД не може існувати без мережі, тому атаки на мережу мають ключове значення. Також, при аналізі загроз РБД та причин їх виникнення було виявлено те, що більшість з них, пов'язані з організацією, установкою та налаштуванням СУРБД адміністратором баз даних. Тому система безпеки має одне із найважливіших значень в проектування та налаштуванні РБД.

Список літератури

1. Amazon RDS. *Amazon*. URL –<https://aws.amazon.com/ru/rds/> (дата звернення: 18.10.2021);
2. Что такое база даних? *Oracle*. URL – <https://www.oracle.com/ru/database/what-is-database/> (дата звернення: 22.11.2021);
3. Investigation of information security issues for graph databases suitable for big data processing while detecting money laundering and terrorism financing cases. *Безопасность информационных технологий*. URL - <https://bit.mephi.ru/index.php/bit/article/view/1306> (дата звернення: 17.11.2021);
4. Певнев В. Я. Методы обеспечения целостности информации в инфокоммуникационных системах/ В.Я. Певнев // Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг. – 2015. - № 51. – С. 74-77;
5. Системы управления базами данных – коротко о главном. *OSP*. URL: https://www.osp.ru/dbms/1995/03/13031428#part_1 (дата звернення: 20.11.2021).

Відомості про авторів

Кирина Діана Віталіївна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-030-56-18, d.kyryna@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки. m.tsuranov@csn.khai.edu