УДК 004.056.52

А. М. ГРИЦЕНКО, канд. техн. наук, доц.
Криворізький національний університет

ПІДВИЩЕННЯ БЕЗПЕКИ БАЗ ДАНИХ ШЛЯХОМ ЗАСТОСУВАННЯ ЗБЕРЕЖЕНИХ ПРОЦЕДУР

У сучасну цифрову епоху дані стали стратегічним ресурсом, який визначає конкурентоспроможність бізнесу, ефективність державних структур та якість надання послуг. Зі зростанням обсягів зібраної, обробленої й збереженої інформації, зростає і вразливість баз даних до внутрішніх та зовнішніх загроз.

Щодня у світі фіксуються тисячі спроб несанкціонованого доступу до інформаційних систем, серед яких переважають атаки на бази даних (БД). До того ж, законодавчі вимоги щодо захисту персональних та фінансових даних, зокрема: GDPR, PCI DSS та національні стандарти безпеки, накладають додаткову відповідальність на організації.

Системи керування базами даних (СКБД) є основним середовищем зберігання критичних даних. Відтак, безпека цих систем є питанням не лише надійної роботи інформаційних систем, а й юридичної відповідальності та репутації компаній.

Використання збережених процедур, тригерів та функцій що вбудовуються в БД підвищують систему захисту даних безпосередньо на рівні бази даних. Це особливо актуально в умовах: розподілених систем з численними точками доступу; великою кількістю користувачів; зберігання конфіденційної інформації (персональні дані, фінанси, медичні записи тощо).

Таким чином, впровадження процедур безпеки безпосередньо в БД на набуває особливої уваги, є необхідним і перспективним напрямом для фахівців з інформаційної безпеки, розробників та адміністраторів баз даних.

Процедури, що зберігаються, - це попередньо скомпільований набір SQL-команд, який зберігається у базі даних та виконується на сервері по запиту. Вони дозволяють автоматизувати та оптимізувати операції з інформацією, виконують складні завдання швидше та безпечніше. Додаткові переваги полягають у тому, що між клієнтом та сервером немає зайвої комунікації, клієнту не надаються відомості, дослідження яких може надати пряму чи опосередковану інформацію щодо структури організації бази даних, та підґрунтя для майбутній атак. Користувачі отримують доступ тільки до процедури, а не до SQL-таблиці, що знижує ризик несанкціонованих змін. З іншого боку, враховуючи, що процедури приховують внутрішню структуру даних, що дозволяє програмістам БД проводити зміни за потреб розширення, розподілення, модифікації без необхідності вносити зміни в програмні продукти клієнтів, що користуються даними. Клієнтські програмні продукти викликають процедури, а операції з даними залишаються лише на рівні бази даних, то відповідно для внесення змін до основної бази даних буде достатньо оновити лише процедури.

При необхідності застосування агрегатних функцій до складної колекції даних, то у випадку використання процедур на рівні БД по каналах зв’язку між клієнтом і сервером передається лише виклик процедури з параметрами (аргументами) та результат обробки функцією колекції даних. Робота з вибіркою та маніпулюванням даних відбувається на рівні БД та вся колекція даних не пересилається каналами зв’язку програмі-клієнту, чим забезпечується захист інформації від її витоку в каналах зв’язку та на рівні клієнтського програмного забезпечення.

Процедури стали важливим, а в деяких випадках невід’ємним елементом БД. Вони дозволяють спрощувати взаємодію клієнта та сервера, прискорювати обробку даних, централізувати логіку та головне, забезпечувати цілісність та безпеку інформації. Але слід зазначити, без достатніх знань та досвіду, дуже легко перетворити навіть маленьку базу на велике джерело проблем, які важко відстежувати.

Список літератури

1. Атака шляхом впровадження коду SQL. Microsoft.com. 02.01.2025. URL: https://learn.microsoft.com/ru-ru/sql/relational-databases/security/sql-injection?view=sql-server-ver16 (дата звернення: 10.03.2025).;

2. **Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mah-mood, S.** Cyber security threats and vulnerabilities: Asystematic mapping study. Arabian Journal for Science and Engineering, 45 (2020), 3171–3189 p.;

3. **Yang, P., Xiong, N., & Ren, J.** Data security and privacyprotection for cloud storage: A survey. IEEE Access, 8 (2022), 131723–131740 p.