Попадюк Володимир Володимирович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

ШИФРУВАННЯ В БАЗАХ ДАНИХ SQL SERVER

Закон вимагає зашифрувати конфіденційну інформацію на рівні бази даних та операційної системи. Як і інші поширені комерційні системи управління базами даних, SQL Server має безліч варіантів шифрування, зокрема на рівні комірки, бази даних та файлів та на рівні передачі через Windows. Ці параметри шифрування забезпечують інформаційну безпеку на рівні бази даних та операційної системи. Крім того, навіть якщо це впливає на інфраструктуру або базу даних SQL Server, вони зменшують можливість несанкціонованого розкриття конфіденційної інформації. Після опису моделі шифрування SQL Server ми представили функцію шифрування, реалізовану в SQL Server, та способи шифрування конфіденційної інформації, що зберігається в базі даних SQL Server.

З'являється все більше повідомлень про втрачений і несанкціонований доступ до конфіденційних даних, а це означає, що безпека баз даних є дуже важливою проблемою для багатьох компаній. Організації, що містять конфіденційну інформацію в базі даних, повинні дотримуватися численних законів, включаючи Gramma-Leach-Bleigh (GLBA), Директиву ЄС про захист даних (EUDPD), Закон про спадкування та підзвітність медичного страхування (HIPAA), стандарт безпеки даних платіжних карток (PCI DSS) та Закон Сарбейнса-Окслі (SOX). Ці закони вимагають шифрування конфіденційної інформації на рівні бази даних та операційної системи.

Крім того, навіть якщо це впливає на інфраструктуру або базу даних SQL Server, вони зменшують можливість несанкціонованого розкриття конфіденційної інформації. Після опису моделі шифрування SQL Server я представив функцію

шифрування, реалізовану в SQL Server, та способи шифрування конфіденційної інформації, що зберігається в базі даних SQL Server.

Модель шифрування SQL Server

Модель шифрування SQL Server в основному забезпечує функції управління ключами шифрування, які відповідають стандарту ANSI X9.17. Стандарт визначає кілька рівнів ключів шифрування, ці рівні використовуються для шифрування інших ключів, а ці ключі використовуються для шифрування фактичних даних.

Головний ключ служби (SMK) є ключем верхнього рівня та родоначальником усіх ключів у SQL Server. SMK – це асиметричний ключ, зашифрований за допомогою API захисту даних Windows (DPAPI). Після зашифрування об'єкта та прив'язки до облікового запису служби SQL Server SMK створюється автоматично. SMK використовується для шифрування головного ключа бази даних (DMK).

Другим рівнем ієрархії ключів шифрування є DMK. Він шифрує симетричні ключі, асиметричні ключі та сертифікати. У кожній базі даних є лише одна DMK.

Наступний рівень містить симетричні ключі, асиметричні ключі та сертифікати. Симетричний ключ є основним засобом шифрування в базі даних. Корпорація Microsoft рекомендує використовувати лише симетричні ключі для шифрування даних. Крім того, SQL Server 2008 та новіші версії мають сертифікати рівня сервера та ключі шифрування бази даних для прозорого шифрування даних.

Шифрування на рівні осередків

Починаючи з SQL Server 2005, можна шифрувати або розшифровувати дані на сервері. Можна зробити це різними способами. Наприклад, можна використовувати один із наведених нижче методів для шифрування даних у базі даних:

- ця ж прохідна фраза використовується для дешифрування даних. Якщо збережені процедури та функції не зашифровані, до фрази очищення можна отримати доступ через метадані.

• Сертифікат. Цей метод забезпечує надійний захист і високу швидкість. Сертифікати можуть бути пов'язані з користувачами; для підписання потрібно використовувати DMK.

• Симетричний ключ. Досить надійний, щоб задовольнити більшість вимог щодо захисту даних та забезпечити достатню продуктивність. Один ключ використовується для шифрування та дешифрування даних.

• Асиметричний ключ. Оскільки для шифрування та дешифрування даних використовуються різні ключі, забезпечується надійний захист. Однак це може негативно позначитися на роботі. Експерти Microsoft не рекомендують використовувати його для шифрування великих значень. Асиметричні ключі можна підписати за допомогою DMK або створити за допомогою паролів.

SQL Server має вбудовані функції для шифрування та дешифрування на рівні комірки. SQL Server має два системних подання, які можна використовувати для отримання метаданих про всі симетричні та асиметричні ключі, які існують в екземплярі SQL Server. Як випливає з назви, sys.symmetric_keys повертає метадані симетричного ключа, а sys.asymmetric_keys – метадані асиметричного ключа. Ще один корисний досвід – це sys.openkeys. Цей поданний каталог містить інформацію про ключі шифрування, відкриті в поточному сеансі.

Прозоре шифрування даних

SQL Server 2008 тепер може використовувати прозоре шифрування для шифрування всієї бази даних. Використовуючи це шифрування, стає можливим захистити базу даних, не змінюючи існуючу програму, структуру бази даних або процес. Це найкращий вибір для задоволення вимог нормативних актів та правил безпеки компанії, оскільки вся база даних зашифрована на жорсткому диску.

Прозоре шифрування даних шифрує базу даних у режимі реального часу, оскільки введення здійснюється у файлі бази даних SQL Server (*.mdf) та файлі журналу транзакцій (*.ldf). Під час резервного копіювання бази даних записи також

шифруються в режимі реального часу, а потім створюється знімок. Дані шифруються перед записом на диск і дешифруються перед вилученням. Цей процес є повністю прозорим для користувачів або програм, оскільки він працює на рівні обслуговування SQL Server.

За допомогою відповідного методу SQL Server використовує ключ шифрування бази даних для шифрування бази даних. Цей асиметричний ключ зберігається в записі завантаження бази даних, тому він завжди доступний під час відновлення.

Ключ шифрування бази даних шифрується за допомогою сертифіката сервера, а сертифікат сервера шифрується за допомогою основної бази даних бази даних DMK. DMK основної бази даних використовує шифрування SMK. SMK – це асиметричний ключ, зашифрований за допомогою Windows DPAPI. Під час першого зашифрування будь-якого об'єкта ключ SMK автоматично генерується та зв'язується з обліковим записом служби SQL Server.

Захист даних в SQL Server

Шифрування – це процес шифрування конфіденційних даних за допомогою ключа або пароля. Шифрування надійно захищає дані та зменшує можливість несанкціонованого розголошення конфіденційної інформації, оскільки без належного ключа або пароля дані будуть зайвими. SQL Server має безліч режимів шифрування, включаючи рівень комірки, рівень бази даних, файли на базі Windows та шифрування рівня передачі. Шифрування SQL Server не може вирішити проблеми інфраструктури та бази даних SQL Server, але навіть якщо інфраструктура SQL Server або конфіденційність бази даних порушена, це також може покращити безпеку даних на рівні бази даних та операційної системи.

Список використаних джерел:

1. Подборка материалов по SQL Injection [Электронный ресурс] – Режим доступа: http://injection.rulezz.ru/

2. Qiu M., Davis S. Database security mechanisms and implementation. IACIS, Issues in Inform. Syst. 2002 vol. 03 pp. 529–534.

3. Потапов А. Е., Манухина Д. В., Соломатина А. С., Бадмаев А. И., Яковлев А. В., Нилова А. С. Безопасность локальных баз данных на примере SQL Server Compact // Укр. Тамбов. ун-та. Серия: Естественные и технические науки. 2014. № 3. С. 915–917.

4. Бортовчук Ю. В., Крылова К. А., Ермолаева Л. В. Информационная безопасность в современных системах управления базами данных // 106 Современные проблемы экономического и социального развития. 2010. № 6. С. 224–225. 31 Горбачевская

5. Ткаченко Н. А. Реализация монитора безопасности СУБД MySQL в dbf / dam системах // ПДМ. Дополнение. 2014. № 7. С. 99–101.

6. Полтавцева М. А. Задача хранения прав доступа к данным в СУБД на примере Microsoft SQL Server // Актуальные направления фундаментальных и прикладных исследований: матер. V Междунар. научно-практич. конф. 2015 С. 118–120.

7. Кузнецов С. Д. Базы данных: учебник для студ. М.: Академия, 2012. 496 с. 42

8. Зегжда Д. П., Калинин М. О. Обеспечение доверенности информационной среды на основе расширения понятия «целостность» и управление безопасностью // Проблемы информ. безопасности. Компьютерные системы. 2009. № 4. С. 7–16.

Ключові слова: шифрування SQL Server, база данних, ключ шифрування, симетричний і асиметоричний ключі.

Ключевые слова: шифрование SQL Server, база данных, ключ шифрования, симметричный и асиметоричний ключи

Keyworbs: encryption SQL Server, database, encryption key, symmetrical and asymmetrical keys.

Науковий керівник: *к.т.н., доцент Соколов А. В.*