УДК 004.056

Обзор подходов защиты информации баз данных в современных системах управления базами данных

Назарко А. В.[*1], Чернышова А.В.[*2]

[*1] магистрант, Донецкий национальный технический университет,
nazar2539@gmail.ru, SPIN-код: 4689-0042

[*2] старший преподаватель, Донецкий национальный технический университет,
chernyshova.alla@rambler.ru, OrcID: 0000-0003-2546-2167, SPIN-код: 3318-2066

Назарко А.В., Чернышова А.В. Обзор подходов защиты информации баз данных в современных СУБД. *В данной статье рассматривается классификация уровней безопасности баз данных. Опираясь на классификацию, производится анализ подходов защиты информации баз данных в современных СУБД. Рассмотрены средства защиты информации баз данных на уровне системы управления базами данных. Определены достоинства и недостатки существующих решений по защите информации баз данных на уровне системы управления базами данных.*

Ключевые слова: *защита информации, базы данных, СУБД, подходы к безопасности, средства защиты, управление доступом.*

Введение

Для установления доступа к информации базы данных и работы с ней применяется система управления базами данных (СУБД). СУБД — это комплекс языковых и программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями. СУБД делятся по моделям данных, рассмотрим СУБД с реляционной моделью данных. СУБД предоставляют такие функции как: сортировка, связь баз данных, регистрация событий, отчетность внесенных изменений и т.д.

Значимость и ценность информации, внесенной в базу данных, требует обеспечения защиты этой информации с помощью средств СУБД [1].

Анализ подходов защиты информации баз данных в современных СУБД

При проектировании средств защиты информации в СУБД нужно рассмотреть потенциальные угрозы. Основной угрозой является риск взлома и утраты конфиденциальной информации, хранящейся в базе данных. При анализе безопасности необходимо учитывать, что даже самый незначительный недочет в системе защиты может повлечь за собой появление более серьезных угроз. Неучтенные или должным образом не функционирующие стандартные методы обеспечения безопасности информации с большой вероятностью являются причиной взлома базы данных или утечки информации из неё. Рассмотрим некоторые подходы защиты баз данных.

Система защиты информации базы данных в СУБД должна быть многоуровневой, количество уровней защиты снижает риск взлома базы данных. Нижние уровни включают такие подходы как: защита паролем, шифрование данных, разграничение прав доступа, регистрация выполняемых операций, резервное копирование. Это основные подходы, без которых полноценная защита недостижима.

Исходя из «Критериев определения безопасности компьютерных систем» разграничивают четыре класса безопасности (Security Classes):

- класс D– обеспечивает минимальную защиту (Minimal Protection), это системы, у которых безопасность не подходит по требованиям к другим классам;
- класс C – обеспечивает избирательную защиту (Discretionary Protection);
- класс B – обеспечивает обязательную защиту (Mandatory Protection);
- класс A– обеспечивает проверенную защиту (Verified Protection) [2].

Избирательное управление доступом (класс C) делится на 2 подкласса – C2 и C1 - менее безопасный, чем C2. Подкласс C1 подразумевает разделение данных и пользователя, как взаимный доступ к данным, так и раздельный. Подкласс C2 дополнительно предусматривает вход в систему, аудит и изоляцию ресурсов. Класс C поддерживается многими СУБД и базируется на идентификации пользователей, объектах баз данных

(таблицах, представлениях, доменах, определенных пользователем наборе символов, хранимых процедурах и т.д.) и привилегиях – наборе действий над тем или иным объектом.

Подлинность пользователя подтверждается его идентификацией или распознаванием пользователя по его идентификатору – логину и паролю. Подтверждается достоверность идентификатора – аутентификация. После чего пользователь авторизуется и ему доступны только данные, исходя из разграничения прав доступа.

Для надежности парольной защиты необходимо соблюдать следующие указания:

- пароль должен состоять из комбинации букв, цифр или специальных знаков;
- длина пароля не менее шести символов;
- пароли должны часто изменяться и храниться в тайне.

В системе могут поддерживаться группы пользователей, обладающих одним и тем же идентификатором группы, которым предоставляются одинаковые права доступа – это позволяет упростить процесс администрирования. Операции добавления отдельных пользователей в группу или удаления из нее могут выполняться независимо от операции задания привилегий для данной группы.

Разграничение прав доступа – достаточно гибкая и развитая система любой многопользовательской СУБД. Администратор баз данных предоставляет права доступа пользователям в соответствии с принципом минимальных полномочий, необходимых для выполнения прямых должностных обязанностей. Большинство СУБД предоставляет набор базовых средств по управлению правами доступа. Пользователи и группы наделяются правами доступа к определенным объектам базы данных. Также многие СУБД указывают разрешенный тип доступа, например, только чтение и т.д.

Можно управлять правами на действия с определенным объектом в зависимости от его типа, допустим, правами на чтение, добавление, удаление и изменение записей в таблицах. Некоторые СУБД включают управление доступом на уровне столбца таблицы или представления [3].

Обязательное управление доступом (класс B) – объектам данных присваиваются определенные классификационные уровни, образующие строгий иерархический порядок (например, «секретно», «совершенно секретно», «для служебного пользования» и т.д.), а пользователи имеют уровни допуска. Делится на три подкласса – B1 – наименее безопасный, B2 и B3 – наиболее безопасный.

Подкласс B1: каждый объект данных содержит отметку о его уровне классификации, а также неформальное сообщение о действующей стратегии безопасности. Подкласс B2: дополнительно требуется формальное утверждение о действующей стратегии безопасности. Подкласс B3: поддерживает аудит, восстановление данных и назначение администратора режима безопасности.

Такая жёсткая структура базы данных используется в военных, или правительственных организациям. Доступ к объекту БД осуществляется при идентичности уровня допуска. Для модификации объект уровень допуска пользователя должен быть равен классификационному уровню объекта благодаря этому, любой информации, внесенной пользователем, автоматически присваивается уровень, идентичный уровню классификации данного пользователя – это исключает запись секретных данных пользователем с высоким уровнем секретности в файл с меньшим классификационным уровнем.

Проверенное управление доступом (класс A) – самый безопасный подход и требует математического доказательства соответствия метода обеспечения безопасности заданной стратегии.

Шифрование данных. Для получения несанкционированного доступа к базе данных пользуются не только обычными средствами доступа в системе, а еще перемещая часть базы данных через подключение к каналу. Для предотвращения такой угрозы необходимо использовать криптографические средства сокрытия информации (хранение и передача конфиденциальных данных в зашифрованном виде).

Режимы работы с зашифрованными базами данных: дешифрование необходимого файла или части файла на внешнем носителе (при завершении работы с информацией, она вновь зашифровывается на внешнем запоминающем устройстве) или дешифрование в оперативной памяти - непосредственно перед выполнением необходимых действий с данными (процедуры шифрования встроены в СУБД).

Рисунок 1 – Основные компоненты безопасности баз данных

Регистрация выполняемых операций и резервное копирование. Ведение лога позволяет регистрировать детальные сведения обо всех операциях пользователей с БД, оно играет значимую роль при обнаружении несанкционированных действий с базой данных, выявлении уязвимостей в системе защиты, а также устранении каких-либо внесенных искажений данных. Помимо выше перечисленного можно также отметить бэкап, который позволяет восстанавливать данные на случай аппаратных или программных сбоев. Также рекомендуется настроить регулярный бэкап данных и репликацию на удаленный компьютер.

Безопасность баз данных должна строиться поэтапно, начиная с принятия базовых мер. Рассмотренные подходы защиты способны в определенной степени обеспечить конфиденциальность и целостность данных, однако их использование не гарантирует полной безопасности данных [4].

Обзор средств защиты на уровне СУБД

Представление – это поименованная динамически поддерживаемая сервером выборка из одной или нескольких таблиц. Это виртуальная таблица, у которой записи формируются при обращении к ней пользователя согласно ранее назначенному ей запросу. С помощью представлений формируется доступ не к целой таблице, а к определенным записям, необходимым для работы пользователю.

Предположим, что вас интересует составной список из погодных записей и координат городов. Для решения этой проблемы необходимо создать представление по данному запросу, фактически присвоить имя запросу, а затем обращаться к нему как к обычной таблице:

CREATE VIEW myview AS SELECT city, temp_lo, temp_hi, prcp, date, location FROM weather, cities WHERE city = name; SELECT * FROM myview;

Активное использование представлений — это ключевой аспект хорошего проектирования баз данных SQL. Представления позволяют скрыть внутреннее устройство ваших таблиц, которые могут меняться по мере развития приложения, за надёжными интерфейсами. Представления можно использовать практически везде, где можно использовать обычные таблицы. И довольно часто представления создаются на базе других представлений. Можно сделать вывод, что представление - это простейший метод защиты как конфиденциальности, так и целостности данных, позволяющий четко ограничить данные, доступные пользователю и контролировать тот набор данных, который пользователь имеет право модифицировать [5].

Триггер – это подпрограмма, автоматически срабатывающая в случае модификации данных в таблице. Триггеры также классифицируются в соответствии с тем, срабатывают ли они до, после или вместо операции. Они называются триггерами BEFORE, AFTER и INSTEAD OF, соответственно. Триггеры BEFORE уровня оператора срабатывают до того, как оператор начинает делать что-либо, тогда как триггеры AFTER уровня оператора срабатывают в самом конце работы оператора. С помощью триггеров можно проверить привилегии пользователя, то есть ответить на вопрос есть ли у пользователя право на модификацию конкретных данных (можно выполнить до модификации данных, при недостаточности прав пользователя на данную операцию будет отменена), протоколировать (например, в отдельной таблице аудита) все события, связанные с модификацией данных в защищаемой таблице – даёт возможность быстро найти пользователя выполнившего несанкционированную модификацию данных. Триггеры дают возможность эффективно контролировать целостность данных и протоколировать их модификацию [6].

Функции шифрования. Встроенные функции шифрования имеются не во всех СУБД, поэтому, универсальным данный метод назвать нельзя. В СУБД PostgreSQL возможно шифрование на разных уровнях и предоставлена гибкость в выборе средств защиты данных при утере сервера, некомпетентных администраторов или в незащищенных сетях. Шифрование может быть необходимо для обеспечения защиты конфиденциальных данных: финансовых переводов и т.д. Шифрование паролей пользователей - хранятся в виде хешей (password_encryption определяет алгоритм хеширования), администратор не имеет доступа к не хешированным паролям. Pgcrypto предоставляет возможность хранить выбранные поля базы в зашифрованном виде. Используется, когда ценная только часть данных базы. Для дешифровки, клиент передаёт ключ, сервер расшифровывает данные и передаёт их назад клиенту. Расшифрованные данные и ключ дешифрования находятся на сервере в процессе расшифровывания и передачи данных. Это создает уязвимость перехвата данных и ключей лицом с полным доступом.

Проверка подлинности сервера SSL. Клиент и сервер имеют возможность проверять подлинность друг друга с помощью SSL сертификатов. Для этого необходимо соответственно настроить их, что надежнее чем пароль. При такой защите фейковый компьютер не сможет выдавать себя за сервер с целью получения паролей пользователей базы данных. Атаки с посредником («man in the middle» незаметная передача всех запросов и данных между клиентом и подлинным сервером) тоже с большей вероятностью будут предотвращены [7].

Достоинства и недостатки существующих решений защиты данных на уровне СУБД

Решения защиты данных на уровне СУБД несложные в эксплуатации, но не смотря на простоту эффективно обеспечивают конфиденциальность и целостность данных.

Недостатком решений защиты данных встроенными средствами СУБД является то, что защиту с их помощью сложно обеспечить для уже существующей системы. На этапе проектирования защищенных БД предусматривается дополнительный уровень защиты в виде комплексного использования представлений, триггеров и встроенных криптографических функций СУБД.

Дешифрование зашифрованной информации базы данных на внешнем устройстве. Достоинство - независимое последовательное функционирование средств шифрования и СУБД. Недостаток - в результате сбоя или отказа часть базы данных может остаться записанной в незашифрованном виде.

Дешифрование зашифрованной информации базы данных в оперативной памяти. Достоинство - высокий уровень защиты от несанкционированного доступа. Недостаток - низкий уровень производительности СУБД в связи с ее усложнением.

Выводы

В рамках статьи кратко рассмотрены средства защиты современных СУБД. Приведено описание возможности их использования для защиты данных в базе данных на уровне СУБД. При рассмотрении существующих подходов, решений и средств для обеспечения безопасности баз данных были выявлены их достоинства и недостатки. В дальнейшем планируется рассмотреть более подробно уязвимости в клиент-серверных приложениях двухзвенной и трехзвенной архитектуры на конкретном примере базы данных, а также представить рекомендации по проектированию и созданию безопасных клиент-серверных приложений с использованием современных СУБД.

Литература

1. Основные аспекты безопасности СУБД: что следует знать [Электронный ресурс] /. – Режим доступа: https://tproger.ru/articles/ dbsecurity -basics. - Загл. с экрана.

2. Классы информационной безопасности в международных стандартах [Электронный ресурс] /. – Режим доступа: https://arinteg.ru/articles/klassy-informatsionnoy-bezopasnosti-v-mezhdunarodnykh-standartakh-30970.html. - Загл. с экрана.

3. Системы управления базами данных [Электронный ресурс] /. – Режим доступа: http://www.bseu.by/it/tohod/sdo4.htm. - Загл. с экрана.

4. С ЧЕГО НАЧИНАЕТСЯ ЗАЩИТА БАЗЫ ДАННЫХ? [Электронный ресурс] /. – Режим доступа: https://www.dataarmor.ru/c-чего-начинается-защита-базы-данных. - Загл. с экрана.

5. Методы защиты данных встроенными средствами СУБД [Электронный ресурс] /. – Режим доступа: http://www.panasenko.ru/ Articles/192/192.html. - Загл. с экрана.

6. Обзор механизма работы триггеров [Электронный ресурс] /. – Режим доступа: https://postgrespro.ru/media/docs/postgresql/12/ru/postgres-A4.pdf/. - Загл. с экрана.

7. Возможности шифрования [Электронный ресурс] /. – Режим доступа: https://postgrespro.ru/media/docs/postgresql/12/ru/postgres-A4.pdf. - Загл. с экрана.

Назарко А. В., Чернышова А.В. Обзор подходов защиты информации баз данных в современных СУБД. *В данной статье рассматривается классификация уровней безопасности баз данных. Опираясь на классификацию, производится анализ подходов защиты информации баз данных в современных СУБД. Рассмотрены средства защиты информации баз данных на уровне системы управления базами данных. Определены достоинства и недостатки существующих решений по защите информации баз данных на уровне системы управления базами данных.*

Ключевые слова: *защита информации, базы данных, СУБД, подходы к безопасности, средства защиты, управление доступом.*

Nazarko A.V., Chernyshova A.V. Review of approaches to protecting database information in modern DBMS. *This article discusses the classification of database security levels. Based on the classification, an analysis of approaches to protecting database information in modern DBMS is carried out. The means of protecting database information at the level of the database management system are considered. The advantages and disadvantages of existing solutions for the protection of database information at the level of the database management system are determined.*

Key words*: information protection, databases, DBMS, approaches to security, protection means, access control.*