СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ БАЗ ДАННЫХ

Шаргородская С.Б., Губенко Н.Е.
Донецкий национальный технический университет

В данном докладе будут рассмотрены различные виды и способы защиты баз данных на предприятиях малого и среднего бизнеса. Особое внимание будет уделено возможным атакам и способам борьбы с ними на базы данных написанные на языке Ms SQL. А так же некоторые рекомендации для администраторов баз данных касаемо диагностики атак вцелом.

В современных СУБД достаточно развиты средства дискреционной защиты. Дискреционное управление доступам (discretionary access control) — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Дискреционная защита является многоуровневой логической защитой. Логическая защита в СУБД представляет собой набор привилегий или ролей по отношению к защищаемому объекту. К логической защите можно отнести и владение таблицей (представлением). Владелец таблицы может изменять (расширять, отнимать, ограничивать доступ) набор привилегий (логическую защиту) . Данные о логической защите находятся в системных таблицах базы данных и отделены от защищаемых объектов (от таблиц или представлений) [1]. Однако дискреционная защита является довольно слабой, так как доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным. В случае реализации информационной системы с использованием реляционной СУБД объектом будет, например, именованное отношение (то есть таблица), а субъектом — зарегистрированный пользователь. В этом случае нельзя в полном объеме ограничить доступ только к части информации, хранящейся в таблице. Частично проблему ограничения доступа к информации решают представления и использование хранимых процедур, которые реализуют тот или иной набор бизнес-действий [1]. Средства мандатной защиты предоставляются специальными (trusted) версиями СУБД. Мандатное управление доступом (mandatory access control) — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Для чего же нужна мандатная защита? Средства произвольного управления доступом характерны для уровня безопасности. Их, в принципе, достаточно для подавляющего большинства коммерческих приложений. Тем не менее, они не решают одной весьма важной задачи — задачи слежения за передачей информации. [1]

Средства произвольного управления доступом не могут помешать авторизованному пользователю законным образом получить секретную информацию и затем сделать ее доступной для других, неавторизованных, пользователей. Нетрудно понять, почему это так. При произвольном управлении доступом привилегии существуют отдельно от данных (в случае реляционных СУБД — отдельно от строк реляционных таблиц), в результате чего данные оказываются «обезличенными» и ничто не мешает передать их кому угодно даже средствами самой СУБД; для этого нужно лишь получить доступ к таблице или представлению.

Физическая защита СУБД главным образом характеризует данные (их принадлежность, важность, представительность и пр.). Это основном метки безопасности, описывающие группу принадлежности и уровни конфиденциальности и ценности данных объекта (таблицы, столбца, строки или поля). Метки безопасности (физическая защита) неизменны на всем протяжении существования объекта защиты (они уничтожаются только вместе с ним) и территориально (на диске) располагаются вместе с защищаемыми данными, а не в системном каталоге, как это происходит при логической защите [1]. Помимо систематического применения арсенала средств, описанных выше, необходимо использовать административные и процедурные меры, в частности регулярное изменение паролей пользователей, предотвращение доступа к физическим носителям информации и диагностику . Ее следует проводить в несколько этапов. Первым этапом является классификация предполагаемых угроз. Второй этап -этап составления математических моделей

основных информационных потоков и возможных нарушений, моделирование типовых действий злоумышленников. Третий этап - этап выработки комплексных мер по пресечению и предупреждению возможных угроз с помощью правовых, организационно-административных и технических мер защиты [2]. На данный момент самыми распространенными базами данных на малых предприятиях являются базы данных, написанные с использованием языка MS SQL server. Существует ряд рекомендаций позволяющий предупредить или устранить возможные виды атак и угроз.

- Четко разграничить производственную и тестовую среду (среду разработки). Производственные сервера не должны содержать тестовых баз данных или инструментария разработчиков.

- Исключить возможность совмещения различных корпоративных сервисов на сервере с установленной СУБД MS SQL.

- Использовать сложные пароли для административных учетных записей как операционной системы, так и СУБД - не менее 15 символов, содержащих буквы в разных регистрах, цифры и специальные символами.

- Удалить из пользователей MS SQL группу "Администраторы" операционной системы и четко прописать, какие учетные записи операционной системы имеют доступ к базам данных. - Избегать предоставления доступа к расширенным хранимым процедурам для пользователей СУБД.

- Использовать привилегированные учетные записи СУБД только для выполнения административных задач.

- Запускать процесс MS SQL Server с правами учетной записи непривилегированного пользователя. Это серьезно усложнит проникновение в систему, так как потенциальный нарушитель в лучшем случае сможет выполнять команды только как пользователь с ограниченными привилегиями. - Протоколировать системные события MS SQL Server, что позволит упростить процесс слежения за действиями потенциального нарушителя.

- Регулярно устанавливать обновления операционной системы Windows и СУБД MS SQL. - Ограничить с помощью межсетевого экрана доступ к портам MS SQL для пользователей, не использующих этот сервис [3].

Итак, можно смело сделать вывод о том, что обеспечение безопасности баз данных - сегодня одна из самых актуальных тем. И это понятно. Главное в этой ситуации состоит в том, что уделяя огромное внимание защите баз данных снаружи, не следует забывать о защищать их изнутри. Для минимизации риска потерь необходима реализация комплекса нормативных, организационных и технических защитных мер.

Литература

1. Безопасность баз данных http://www.connect.ru/article.asp?id=6633
2. Безопасность СУБД http://www.citforum.ru/security/articles/db_security/
3. Скрытые возможности MS SQL http://www. citforum.ru/ security/articles/ sql_sec/