УДК 004.056.5

АНАЛИЗ И КОНТРОЛЬ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ БЕЗОПАСНОСТИ

© 2024 И. Ю. Верещагин

Финансовый университет при Правительстве Российской Федерации,
г. Москва, Россия

Статья представляет собой аналитический обзор, посвященный методам и технологиям, которые используются и практикуются при анализе и контроле уязвимостей в информационных системах. Примером этого может служить сбор информации о системе или какой-либо базе данных, сканирование системы на уязвимость различных видов атак, а также любой из этапов кибератаки. Предложены решения выявленных проблем: примеры контроля и методы защиты уязвимостей, такие как регулярное обновление программного обеспечения, поэтапное проведение анализа уязвимостей, и также разработка новых стратегий безопасности базы данных.

Ключевые слова: информационная безопасность, уязвимости, контроль устройств, угрозы, база данных.

Обеспечение безопасности баз данных (БД) является одной из сложных задач для компаний. Чем сложнее базы данных на предприятии, тем более сложные меры безопасности необходимо применять. Подключение к базам данных по сети и Интернету может еще больше усложнить ситуацию. Кроме того, каждый дополнительный внутренний пользователь, который будет добавлен в базу пользователей, может создать дополнительные серьезные проблемы с безопасностью. В данной статье дается анализ наиболее распространенных угроз и уязвимости для баз данных организаций, также впоследствии даются рекомендации по основным средствам защиты для устранения этих угроз и уязвимостей.

Вообще понятие уязвимости относится к слабости или сбою в системе или механизме защиты, которые делают информацию уязвимой для атак или повреждения. Концепция угрозы объекту, физическому или иному юридическому лицу представляет собой риск потери актива. Предположение, лежащее в основе этого исследования, заключается в том, что, поняв слабые места и угрозы, с которыми он сталкивается, администратор базы данных может приступить к разработке плана обеспечения безопасности для лучшей защиты своих баз данных и данных, которые содержатся в них.

По мере того как организации все шире внедряют системы баз данных в качестве ключевой технологии управления данными для повседневных операций и принятия решений, безопасность данных, управляемых этими системами, приобретает одно из важнейших значений. Повреждение и неправильное использование данных затрагивают не только отдельного пользователя или приложение, но и могут иметь катастрофические последствия для всей организации в целом.

На сегодняшний день популярность информационных систем и различных веб-приложений сильно выросла, и тем самым повысился риск «вторжений» в различные базы данных и доступа к ним. Следует понимать, что данные должны быть защищены не только от внешних атак, но и от внутренних угроз, поэтому информационная безопасность сегодня стала важна как никогда.

Информационная безопасность базы данных напрямую зависит от различных видов контроля устройств, связанных с ней, будь то обычные данные, приложения, сервера или сетевые соединения, которые непосредственно связаны с БД [3].

При формировании информационной безопасности используются следующие виды контроля (рис. 1).

Рисунок 1 – Виды контроля

Системы управления базами данных все чаще используются для хранения информации обо всех аспектах деятельности предприятия. Данные, хранящиеся в СУБД, часто имеют очень важное значение для деловых интересов организации и рассматриваются как корпоративный актив. В дополнение к защите внутренней ценности данных корпорации должны рассмотреть способы обеспечения конфиденциальности и контроля доступа к данным, которые по разным причинам не должны раскрываться определенным группам пользователей [1].

По мнению Рамакришнана и Герке, при разработке защищенного приложения для баз данных необходимо учитывать три основные задачи. Когда речь заходит о защите базы данных, необходимо позаботиться о многих вещах. В данной статье подробно рассматриваются основные концепции безопасности баз данных, включая конфиденциальность и доступность [2].

Конфиденциальность (секретность) – это ситуация, когда информация не должна разглашаться неавторизованным пользователям. В концепции безопасности баз данных конфиденциальность всегда стоит на первом месте. Конфиденциальность может быть обеспечена путем шифрования данных, хранящихся в базе данных.

Шифрование – это способ преобразования данных таким образом, чтобы они не могли быть прочитаны кем-либо, кроме авторизованных сторон.

Другими словами, шифрование означает, что конфиденциальные данные становятся нечитаемыми для неавторизованных пользователей. Шифрование может выполняться на двух различных уровнях: для передачи данных и для хранения данных.

Передача данных (относится к данным, которые перемещаются по сети). Например, конфиденциальные данные, которые передаются по сетевым каналам или через Интернет. Хакер может получить доступ к этим конфиденциальным данным путем подслушивания. Когда это происходит, конфиденциальность данных нарушается. Шифрование передаваемых данных позволяет избежать таких угроз. Данные в состоянии покоя: хакер может взломать данные, хранящиеся в базе данных. Шифрование данных в состоянии покоя предотвращает такие утечки. Доступны различные алгоритмы шифрования, в том числе стандарты шифрования данных (DES), Triple DES, а также расширенные стандарты шифрования (AES).

Хранение данных (конфиденциальность). Только авторизованным пользователям должно быть разрешено изменять данные. Целостность можно обеспечить, установив контроль доступа пользователей (UAC), который определяет, каким пользователям должны быть предоставлены те или иные разрешения в базе данных. Например, данные, относящиеся к информации о сотрудниках, хранящиеся в БД. У всех сотрудников могут быть разрешения на просмотр записей и их изменение только в части касающейся их информации, в то время как сотрудник отдела кадров будет иметь расширенный доступ.

Доступность данных. Авторизованному пользователю не должно быть отказано в доступе. В БД не должно быть незапланированных простоев. Для обеспечения этого необходимо предпринять следующие шаги:

- ограничить количество одновременных сеансов, доступных каждому пользователю базы данных;
- периодически создавать резервные копии данных, чтобы обеспечить их вос-

становление в случае проблем с приложением;

- защитить от уязвимостей в системе безопасности;
- для обеспечения высокой доступности рекомендуется использовать кластеры БД.

Для достижения этих целей необходимо разработать четкую и последовательную политику безопасности, описывающую, какие меры безопасности необходимо применять. В частности, она должна определять, какая часть данных будет защищена и какие пользователи к какой части данных получат доступ.

Для обеспечения соблюдения политики необходимо использовать механизмы безопасности базовой СУБД. Такие механизмы являются ценным инструментом для обеспечения соблюдения политики безопасности. Они позволяют ограничить доступ к конфиденциальным данным, предоставляя доступ к ограниченной версии (определенной с помощью представления) этих данных, а не к самим данным – Oracle.

Угрозы и риски для БД постоянно возрастают, и, следовательно, необходимость в защите баз данных также растет. Например, достаточно большой объем данных хранится в базах организаций, но, к сожалению, мало внимания уделяется их защите. На рисунке 2 представлен анализ наиболее атакуемых отраслей российской экономики в 2023 г. [4].

Рисунок 2 – Наиболее атакуемые отрасли бизнеса в 2023 году

Комплексные атаки имеют сложную структуру, различные механизмы их осуществления и опираются на возможность использования различных направлений распространения информации. Использование методов социальной инженерии позволяет находить наиболее продуктивные способы организации атак. В киберпространстве, по прогнозам экспертов, могут развиваться все более опасные и сложные угрозы, что делает задачу их всестороннего анализа и использования результатов его решения эффективной для противодействия существующим и возможным будущим киберугрозам. Тем самым и определяется необходимость анализа и контроля уязвимостей в информационной системе [4].

В данной работе предлагается определить безопасность БД как некий бизнес-процесс, который будет контролировать, анализировать и регулировать целостность базы данных.

Несанкционированный вход или доступ к серверу базы данных означает потерю конфиденциальности; несанкционированное изменение доступных данных означает потерю целостности, а отсутствие доступа к службам базы данных означает потерю доступности. Потеря одного или нескольких из этих основных аспектов окажет

значительное влияние на безопасность базы данных.

Для иллюстрации этой концепции представим, что веб-сайт компании содержит информацию о том, «кто она такая», чем занимается и что должны сделать потенциальные клиенты, чтобы связаться с ней по своим вопросам. В данном случае доступность служб БД является более важной по сравнению с другими факторами, будь то конфиденциальность или же целостность системы БД, как говорилось ранее. Если, к примеру, возьмем компанию, которая занимается продажей товаров онлайн, то конфиденциальность будет стоять на первом месте, так как клиенты будут использовать свои кредитные карты.

При проверке безопасности базы данных необходимо учитывать еще один фактор, а именно «надежность». Возьмем, к примеру, веб-приложение, работающее как интерфейс для сервера баз данных. Если веб-приложение, которое продает товары онлайн, уязвимо для межсайтового скриптинга, вероятность того, что люди не будут доверять веб-сайту, возрастает. Когда клиенты теряют доверие к компании, это может привести к потерям в бизнесе.

Базы данных подвержены и другим уязвимостям, таким как:

- неправильное управление паролями;
- внедрение SQL-кода;
- утечка данных и неправильная обработка ошибок.

Хакеры пытаются атаковать базы данных, которые плохо настроены. Используют их слабые места для «взлома» БД компании.

Далее представлен анализ угроз, а также контроль устройств, который можно осуществить.

Когда к данным обращается много людей, вероятность их кражи возрастает. В прошлом атаки на БД были распространены, но их было меньше, поскольку хакеры взламывали сеть в основном для того, чтобы доказать, что данную БД можно взломать, а не для продажи конфиденциальной информации.

Другая причина атак на базы данных – получение денег за продажу конфиденциальной информации, которая включает персональные данные, номера кредитных карт, номера социального страхования и т.п.

Рассмотрим основания возможного недобросовестного поведения.

1. Чрезмерный доступ.

Данное основание имеет место, если у пользователей появляется доступ к БД с функциями, превышающими их должностные обязанности (таким видом доступа можно начать злоупотреблять). Например, администратор в школе, работа которого заключается в изменении контактной информации о школьнике, может воспользоваться БД и исправить какие-либо характеристики спортивных достижений или оценок учащегося. Это может случиться из-за того, что у администраторов БД нет времени обновлять механизмы детального контроля БД относительно доступа каждого пользователя. И в результате всем пользователям предоставляется доступ с «расширенными функциями» по умолчанию, которые намного превышают их функциональный доступ.

Решением данной проблемы может быть контроль дополнительного доступа на уровне запросов. Данное управление относится к механизму, который закрывает доступ к БД при использовании минимальных операций SQL (SELECT, UPDATE). Степень контроля доступа должна распространяться на определенные строки и столбцы. Такой вид контроля помог бы администратору школы (как представлено выше в примере) обновлять информацию, но выдавать ошибку или предупреждение, если он попытается изменить данные.

2. Законное злоупотребление доступом.

Пользователи могут использовать информацию БД для несанкционированных целей. Например, рассмотрим сотрудника адвокатуры или суда, у которого есть доступ к просмотру записей о разных клиентах с помощью отдельного веб-приложения. Структура такого приложения дает возможность просматривать только дело одного клиента. Но все же данный сотрудник может обойти все ограничения путем подключения к БД с помощью альтернативного клиента, например MS-Excel. При работе в MS-Excel можно, используя свои закон-

ные учетные данные, получить и сохранить все данные клиента.

Решением описанной проблемы является контроль доступа к БД, который будет применяться не только относительно конкретных запросов, как было в пункте 1, но и к контексту, который его окружает. Ограничение на время суток, месторасположение и т.п.

3. Повышение прав доступа.

Такое действие может произойти, если хакеры, используя уязвимость программного обеспечения БД, меняют права доступа обычного пользователя на права администратора. Ошибки могут быть обнаружены в различных процедурах, бизнес-процессах, в протоколах и инструкциях SQL.

Контрольные IP-адреса и контроль доступа на уровне запросов могут быть предотвращены с помощью комбинации традиционных систем предотвращения вторжений (IPS) и контроля доступа на уровне запросов (см. п. 1. «Чрезмерный доступ»). IPS проверяет трафик базы данных, чтобы выявить закономерности, соответствующие известным уязвимостям. Например, если известно, что данная функция уязвима, то IPS может либо заблокировать весь доступ к уязвимой процедуре, либо (если это возможно) заблокировать только те процедуры, которые используют встроенные атаки. К сожалению, при использовании только IPS иногда сложно точно определить, на какие запросы к БД направлены атаки. Многие уязвимые функции базы данных обычно используются в законных целях, поэтому блокировать все случаи использования таких функций нецелесообразно. IP-адреса должны четко отделять «законные» функции от функций, связанных со встроенными атаками. Здесь необходимо сказать о том, что бесконечные вариации атак во многих случаях делают это невозможным. Если это происходит, то системы IPS используются только в режиме оповещения (без блокировки), поскольку возможны ложные срабатывания. Для повышения точности IPS можно комбинировать с альтернативными индикаторами атак, например, такими, как управление доступом по запросу. При этом IP-адреса могут использоваться для проверки: обращается ли запрос к базе данных к уязвимой функции, в то время как система управления доступом к запросам определяет, соответствует ли запрос обычному поведению пользователя. Если запрос указывает на доступ к уязвимой функции и необычное поведение, то почти наверняка происходит атака.

4. Уязвимости протокола взаимодействия с БД.

В протоколах взаимодействия с базами данных всех поставщиков баз данных выявляется все больше уязвимостей в системе безопасности. Любые действия, которые направлены на устранение этих уязвимостей, могут быть в диапазоне от несанкционированного доступа до повреждения данных. Например, червь SQL Slammer 2 воспользовался уязвимостью в протоколе Microsoft SQL Server для принудительного отказа в обслуживании. Что еще хуже, во встроенном журнале аудита не будет записей об этих факторах мошенничества, поскольку операции протокола не охватываются встроенными механизмами аудита базы данных. Атаки по протоколу управления базами данных могут быть предотвращены с помощью технологии, обычно называемой проверкой протокола. Технология проверки протокола, по сути, анализирует (дизассемблирует) трафик базы данных и сравнивает его с ожиданиями. В том случае, если текущий трафик не соответствует ожиданиям, могут быть приняты меры по предупреждению или блокировке.

5. Слабая аутентификация.

Слабые схемы аутентификации позволяют злоумышленникам выдавать себя за законных пользователей базы данных, похищая или иным образом получая учетные данные для входа. Злоумышленник может использовать любое количество стратегий для получения учетных данных.

6. Руткиты базы данных.

Руткит базы данных – это программа или процедура, скрытая внутри базы данных и предоставляющая привилегии администратора для получения доступа к данным в базе данных. Такие руткиты могут отключать оповещения, запускаемые системами предотвращения вторжений (IPS).

Установить руткит можно только после взлома базовой операционной системы. А чтобы этого избежать, необходимы периодические проверки. В противном случае присутствие руткита в базе данных может остаться незамеченным. В дополнение к этому администратор базы данных (DBA) также должен использовать пароль root для доступа к корневой базе данных, который должен храниться в секрете и предоставляться авторизованному пользователю только в целях технического обслуживания, когда в этом возникнет необходимость.

В заключение можно отметить, что угрозы, которые связаны с БД, разнообразны, поэтому для каждой БД средства контроля безопасности должны различаться. На сегодняшний день в открытом доступе можно приобрести как различные БД (PostrgesPro, Pangolin, Oracle, SQL, Access), так и различные типы решений к ним.

Для анализа угроз и уязвимости информационной безопасности (ИБ) баз данных необходимо оценить риски и снизить их путем соответствующих решений. При этом ИБ БД имеет ряд особенностей, которые необходимо серьезно учитывать. Один из вариантов обеспечения безопасности БД заключается в ее оптимальной защите. Обеспечение безопасности базы данных должно осуществляться как снаружи, так и изнутри, включая обеспечение безопасности, начиная с физического уровня и заканчивая уровнем данных (физический, сетевой, хост, приложения и данные).

СПИСОК ИСТОЧНИКОВ

1. Barabási A. L., Albert R., Jeong H. Mean-field theory for scale-free random networks // Statistical Mechanics and Its Applications. 1999. Vol. 272 (1-2). Pp. 173–187. Doi: 10.1016/s0378-4371(99)00291-5.
2. Watts D. J., Strogatz S. H. Collective dynamics of “small-world” networks // Nature. 1998. № 393 (6684). Pp. 440-442. Doi: 10.1038/30918.
3. Евин И. А. Введение в теорию сложных сетей // Компьютерные исследования и моделирование. 2010. Т. 2. № 2. С. 121-141.
4. Аналитика Angara Security: в 2023 году ритейл и e-commerce вошли в ТОП-3 самых атакуемых отраслей российской экономики. URL: https://www.novostiitkanala.ru/news/detail.php?ID=176179&ysclid=lxegh9pio9445158036
5. Галиндо Ф., Дмитриенко Н. В., Карузо А., Россодивита А., Тихомиров А. А., Труфанов А. И., Шубников Е. В. Моделирование сложных атак на комплексные сети // Безопасность информационных технологий. 2010. Т. 17. № 3. С. 115-121.

ANALYSIS AND CONTROL OVER VULNERABILITIES IN SECURITY INFORMATION SYSTEMS

© 2024 Ilia Y. Vereshchagin

Financial University under the Government of the Russian Federation, Moscow, Russia

The article is an analytical review that is devoted to the methods and technologies that are used and practiced in the analysis and control of vulnerabilities in information systems. An example of this would be collecting information about a system or some database, scanning a system for vulnerability to various types of attacks, or any of the stages of a cyber attack. This article also provides examples of control and methods for protecting vulnerabilities, such as regular software updates, step-by-step vulnerability analysis, and also the development of new database security strategies.

Keywords: information security, vulnerabilities, device control, threats, database.