Секция «Информационное обеспечение деятельности федеральных органов исполнительной власти»

К вопросу о безопасности бизнес-систем и баз данных

Научный руководитель – Пономарева Ольга Алексеевна

Степаненко Дмитрий Владимирович
Студент (магистр)
Уральский федеральный университет имени первого Президента России Б.Н.Ельцина,
Институт радиоэлектроники и информационных технологий–РтФ, Екатеринбург, Россия
E-mail: dmitry.stepanenko@urfu.me

Известно, что бизнес-система представляет собой категорию процессной модели организации, выраженную с помощью системного подхода в рамках процессного управления [1]. В свою очередь, система управления базами данных (СУБД) - это комплекс программно-языковых средств, позволяющих создать базы данных (БД) и управлять данными. Иными словами, СУБД - это набор программ, позволяющий организовывать, контролировать и администрировать базы данных [10]. Все далее сказанное применимо как к СУБД, так и к бизнес-системам.

Данные - это ценный объект (информационный актив) организации, с которым необходимо надежно обращаться и управлять им, как и с любым экономическим ресурсом. Таким образом, некоторая часть или все коммерческие данные могут иметь тактическое значение для организаций и, следовательно, должны быть защищены и конфиденциальны.

Безопасность БД относится к набору инструментов, элементов управления и мер, предназначенных для установления и сохранения конфиденциальности, целостности и доступности БД, как эталонной модели (триады) информационной безопасности (ИБ) [9]. Но в контексте данной статьи хочется уделить основное внимание конфиденциальности, поскольку именно этот элемент подвергается риску в большинстве случаев утечки и компрометации данных.

Безопасность БД должна учитывать и защищать следующее:

- сами данные в БД;
- СУБД;
- любые связные приложения и программы;
- физические и виртуальные сервера БД;
- вычислительная и сетевая инфраструктура, используемая для доступа к БД.

Безопасность БД - сложная задача, включающая все аспекты технологий и методов обеспечения ИБ. При этом страдает один из принципов обеспечения ИБ - доступность [9]:

- чем доступнее и удобнее БД, тем более она уязвима для угроз безопасности информации (УБИ);
- чем более неуязвима БД для УБИ, тем труднее получить к ней доступ и использовать ее.

Применение надлежащих методов обеспечения безопасности БД жизненно важно для любой организации по целому ряду причин. Это включает:

1. Обеспечение непрерывности бизнеса.
2. Минимизация финансового ущерба.
3. Утрата интеллектуальной собственности.
4. Ущерб репутации бренда.
5. Наказания и штрафы. Организации должны соблюдать большое количество правил, таких как ФЗ «О персональных данных», Общие положения о защите данных (GDPR), Стандарт безопасности данных индустрии платежных карт (PCI DSS) и подобные [6],

[5], [11]. Если утечка данных происходит из-за того, что организация не соблюдает эти правила, штрафы и санкции могут быть очень серьезными. Но, вспоминая суммы штрафов в районе 60000 рублей за недавние утечки на миллионы строк из БД крупных российский компаний, усматриваются низкая эффективность принятых регуляторами мер и правовой нигилизм субъектов экономических отношений [7], [4].

Переходя к УБИ в БД, стоит отметить, что многие уязвимости в программном обеспечении (ПО), неправильные настройки, шаблоны неправильного или небрежного использования могут привести к взлому. Перечислим ряд наиболее известных причин и типов киберугроз безопасности БД:

1. **Внутренние угрозы**. Это УБИ из одного из следующих трех источников, каждый из которых имеет привилегированные средства доступа к БД [3, с. 498]:

- инсайдер со злым умыслом;
- небрежный сотрудник, который подвергает БД атаке неосторожными действиями;
- посторонний, который получает учетные данные с помощью социальной инженерии или других методов.

Особое внимание - внутренние пользователи (особенно ключевые сотрудники), которые часто не признаются актуальными нарушителями.

Таким образом, внутренняя угроза является одной из наиболее типичных причин нарушения безопасности БД и часто возникает из-за того, что многим сотрудникам предоставлен доступ привилегированного пользователя.

2. **Человеческий фактор**. Слабые пароли, совместное использование паролей, случайное стирание или повреждение данных и другие нежелательные действия пользователей по-прежнему являются причиной почти половины зарегистрированных проблем с БД [3, с. 498].

3. **Эксплуатация уязвимостей ПО**. Разработчики регулярно выпускают исправления безопасности, однако, если ими пренебрегать или устанавливать их недостаточно быстро, БД может подвергнуться атаке [2].

4. **Атаки с инъекциями SQL/NoSQL**. Один из распространённых способов взлома сайтов и программ, работающих с БД, основанный на внедрении в запрос произвольного SQL-кода/NoSQL-кода [12, с. 218]. Любая система БД уязвима для этих атак, если разработчики не придерживаются методов безопасного программирования [3, с. 499].

5. **Атаки на переполнение буфера**. Злоумышленники могут использовать избыточные данные, хранящиеся в соседних адресах памяти, в качестве отправной точки для запуска атак [3, с. 499].

6. **Атаки типа «отказ в обслуживании» (DoS/DDoS)**. При распределенной атаке типа «отказ в обслуживании» (DDoS) поддельный трафик генерируется большим количеством компьютеров, участвующих в ботнете, контролируемом злоумышленником [13]. Это создает очень большие объемы трафика, которые трудно остановить без хорошо масштабируемой защитной архитектуры [3, с. 500].

7. **Вредоносное ПО.** Защита от вредоносных программ важна для любой конечной точки, но особенно для серверов БД из-за их высокой ценности и чувствительности [3, с. 500].

8. **Развивающаяся ИТ-среда** делает БД более восприимчивыми к угрозам. Тенденции, которые могут привести к новым типам атак на БД или могут потребовать новых защитных мер [3, с. 500]:

- растущие объемы данных;
- распределенная инфраструктура;
- ужесточающиеся нормативные требования;
- нехватка навыков в области обеспечения кибербезопасности.

Перейдем к рассмотрению методов обеспечения безопасности БД. Как было сказано ранее, для обеспечения хорошей безопасности нам нужно учесть множество нюансов.

Поскольку БД почти всегда доступны из сети, любая УБИ для любого компонента или части сетевой инфраструктуры также является угрозой для БД, и любая атака, затрагивающая устройство или рабочую станцию пользователя, может угрожать БД. Таким образом, безопасность БД должна выходить далеко за пределы одной только БД.

При оценке безопасности БД необходимо рассмотреть каждую из следующих областей [2]:

1. Физическая безопасность.
2. Административное и сетевое управление доступом.
3. Безопасность учетной записи/устройства конечного пользователя.
4. Шифрование.
5. Безопасность ПО БД, системного и прикладного ПО.
6. Безопасность приложения/веб-сервера.
7. Безопасность резервного копирования.
8. Аудит.

Соответственно, поиск следов компрометации инфраструктуры необходимо проводить комплексно, принимая во внимание максимально широкий круг источников обнаружения УБИ.

Кроме того, необходимо регулярно проводить оценку зрелости процессов ИБ организации, включая методы тестирования на проникновение - PenTest, для получения реального состояния уровня защищенности инфраструктуры. Это качественно упрощает расследование инцидентов и реагирование на них.

В заключении следует отметить, что подход к обеспечению безопасности бизнес-систем и СУБД с возможностью интеграции рассмотренных выше методик станет эффективнее не только в стадии эксплуатации, но и на этапе создания систем защиты информации и будет более практико-ориентированным. Это улучшит способность противостоять УБИ, активно обнаруживать поведение злоумышленников и поддерживать надежный, контекстуально двунаправленный обмен информацией.

Источники и литература

1) Бизнес-система (Глоссарий процессного управления) // Технологии BPM и ERP от ПитерСофт URL: https://piter-soft.ru/knowledge/glossary/process/bizines-sistema.html (дата обращения: 10.02.2023).

2) Защита баз данных // Научно-технический центр ЕВРААС URL: https://www.evraas.ru/solutions/db-protection/ (дата обращения: 12.02.2023).

3) Казарян К.К. БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022

4) Минцифры готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных // Минцифры России URL: https://digital.gov.ru/ru/events/41722/ (дата обращения: 10.03.2023).

5) Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR-TEXT.COM URL: https://gdpr-text.com/ru/ (дата обращения: 10.02.2023).

6) О персональных данных (с изменениями на 14 июля 2022 года) // Электронный фонд правовых и нормативно-технических документов URL: https://docs.cntd.ru/document/901990046?section=status (дата обращения: 10.03.2023).

7) Служба безопасности Яндекс Еды сообщила об утечке информации // Новости Яндекса URL: https://yandex.ru/company/services_news/2022/01-03-2022 (дата обращения: 12.02.2023).

8) Соколин Демьян Дмитриевич, Тимохович Александр Степанович Методы комплексного обеспечения безопасности SQL-сервера от атак типа SQL-инъекции // Academy. 2017. №3 (18). URL: https://cyberleninka.ru/article/n/metody-kompleksnogo-obespecheniya-bezopasnosti-sql-servera-ot-atak-tipa-sql-inektsii (дата обращения: 13.02.2023).

9) Чепурина Ю.А., Ольхов В.В. МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТ ИНФОРМАЦИИ В РЕЛЯЦИОННЫХ СУБД // Инновационная наука. 2021. №1. URL: https://cyberleninka.ru/article/n/metody-kriptograficheskoy-zaschit-informatsii-v-relyatsionnyh-subd (дата обращения: 12.03.2023).

10) Что такое СУБД // RU-CENTER (АО «Региональный Сетевой Информационный Центр») URL: https://www.nic.ru/help/chto-takoe-subd_8580.html (дата обращения: 10.02.2023).

11) Что такое PCI DSS и как происходит проверка на соответствие стандарту? // Хабр URL: https://habr.com/ru/company/payonline/blog/303330/ (дата обращения: 10.03.2023).

12) Юрченко, А. С. Отдельные аспекты безопасности информационных систем / А. С. Юрченко, Д. А. Яшаров, К. Н. Ефименко // Программная инженерия: методы и технологии разработки информационно-вычислительных систем (ПИИВС-2018) : сборник научных трудов II Международной научно-практической конференции (студенческая секция), В двух томах, Донецк, 14–15 ноября 2018 года. Том 2. – г. Донецк: Донецкий национальный технический университет, 2018. – С. 218-222. – EDN AJEVJE.

13) Botnet DDoS Attacks // Imperva URL: https://www.imperva.com/learn/ddos/botnet-ddos/ (дата обращения: 10.03.2023).