УДК 004.65

Гайко Анастасия Вячеславовна, Горчанина Алеся Ивановна
Белорусский государственный экономический университет
nastya.gaiko03@gmail.com,alesyagorchanina 13@gmail.com

Проблемы и перспективы безопасности баз данных

Атаки на хранилища и БД являются одними из самых опасных для предприятий и организаций. Согласно статистике в последние годы количество утечек данных в мире неуклонно растет. Даже если предположить, что в ряде случаев утечка включала данные, к которым сотрудник имеет легальный доступ, каждый третий случай приходится на внешнюю атаку. Также нужно отметить, что на внешние атаки приходится 7 из 8 утечек объемом более 10 млн. записей.

Злоумышленников интересуют такие виды информации, как внутренняя операционная информация, персональные данные сотрудников, финансовая информация, информация о заказчиках/клиентах, интеллектуальная собственность, исследования рынка или анализ деятельности конкурентов, платежная информация. Эти сведения в итоге хранятся в корпоративных хранилищах и БД.

Все это приводит к необходимости обеспечения защиты не только коммуникаций, операционных систем и других элементов инфраструктуры, но и хранилищ данных как еще одного барьера на пути злоумышленника. Однако на сегодняшний день работы в области обеспечения безопасности БД направлены в основном на преодоление существующих и уже известных уязвимостей, реализацию основных моделей доступа и рассмотрение вопросов, специфичных для конкретной СУБД.

Целью данной работы является комплексное рассмотрение и систематизация вопросов безопасности различных БД в свете новых угроз, общих тенденций развития информационной безопасности и возрастающей роли и разнообразия хранилищ данных.

Исторически развитие систем безопасности БД происходило как реакция на действия злоумышленников в соответствии с этапами эволюции самих хранилищ (БД) и изменениями типа и вида возрастающих угроз. Эти изменения были обусловлены общим развитием БД от решений на мейнфреймах до облачных хранилищ.

В архитектурном плане можно выделить следующие подходы:

– Полный доступ всех пользователей к серверу БД;

– Разделение пользователей на доверенных и частично доверенных средствами СУБД (системы управления БД);

– Введение системы аудита (логов действий пользователей) средствами СУБД;

– Введение шифрования данных; вынос средств аутентификации за пределы СУБД в операционные системы и промежуточное ПО; отказ от полностью доверенного администратора данных.

Тем не менее, введение средств защиты как реакции на угрозы не обеспечивает защиту от новых способов атак и формирует разрозненное представление о самой проблеме обеспечения безопасности. С одной стороны, крупные компании могут выделить достаточное количество средств обеспечения безопасности для своих продуктов, с другой стороны, именно по этой причине имеется большое количество разнородных решений, отсутствует понимание комплексной безопасности данных (и ее компоненты разнятся от производителя к производителю), нет общего, единого подхода к безопасности хранилищ данных и, как следствие, возможности. Усложняются прогнозирование будущих атак и перспективная разработка защитных механизмов, для многих систем сохраняется актуальность уже давно известных атак, усложняется подготовка специалистов по безопасности [1].

Именно разработка программных средств перспективной защиты (на опережение злоумышленника), обеспечение возможности внедрения такой технологии являются наиболее актуальными на текущем этапе.

Список основных уязвимостей СУБД не претерпел существенных изменений за последние годы. Проанализировав средства обеспечения безопасности СУБД, архитектуру БД, известные уязвимости и инциденты безопасности, можно выделить следующие причины возникновения такой ситуации:

– проблемами безопасности серьезно занимаются только крупные производители;

– программисты баз данных, прикладные программисты и администраторы не уделяют должного внимания вопросам безопасности;

– разные масштабы и виды хранимых данных требуют разных подходов к безопасности;

– различные СУБД используют разные языковые конструкции для доступа к данным, организованным на основе одной и той же модели;

– появляются новые виды и модели хранения данных.

Применение различных средств обеспечения информационной безопасности является для организации компромиссом в финансовом плане: внедрение более защищенных продуктов и подбор более квалифицированного персонала требуют больших затрат. Компоненты безопасности зачастую могут негативно влиять на производительность СУБД.

Эти проблемы усугубляются с появлением и широким распространением нереляционных СУБД, оперирующих другой моделью данных, однако построенных по тем же принципам, что и реляционные [2].

Обеспечение безопасности хранимой информации, в частности, невозможно без обеспечения безопасного управления данными. Исходя из этого, все уязвимости и вопросы безопасности СУБД можно разделить на две категории: зависящие от данных и не зависящие от данных.

Уязвимости, независящие от данных, являются характерными и для всех прочих видов ПО. Их причиной, например, может стать несвоевременное обновление ПО, наличие неиспользуемых функций или недостаточная квалификация администраторов ПО.

Большинство аспектов безопасности СУБД является именно зависящими от данных. В то же время многие уязвимости являются косвенно зависимыми от данных. Например, большинство СУБД поддерживают запросы к данным с использованием некоторого языка запросов, содержащего наборы доступных пользователю функций (которые, в свою очередь, тоже можно считать операторами запросного языка) или произвольные функции на языке программирования.

Архитектура применяемых языков, по крайней мере, то, что касается специализированных языков и наборов функций, напрямую связана с моделью данных, применяемой для хранения информации. Таким образом, модель определяет особенности языка, и наличие в нем тех или иных уязвимостей. Причем такие уязвимости, например, как инъекция, выполняются по-разному (sql-инъекция, java-инъекция) в зависимости от синтаксиса языка.

На основании разделения уязвимостей можно выделить зависящие и независящие от данных меры обеспечения безопасности хранилищ информации.

Не зависящими от данных можно назвать следующие требования к безопасной системе БД:

- Функционирование в доверенной среде.

Под доверенной средой следует понимать инфраструктуру предприятия и ее защитные механизмы, обусловленные политиками безопасности. Таким образом, речь идет о функционировании СУБД в соответствии с правилами безопасности, применяемыми и ко всем прочим системам предприятия.

- Организация физической безопасности файлов данных.

Требования к физической безопасности файлов данных СУБД в целом не отличаются от требований, применяемых к любым другим файлам пользователей и приложений.

- Организация безопасной и актуальной настройки СУБД.

Данное требование включает в себя общие задачи обеспечения безопасности, такие как своевременная установка обновлений, отключение неиспользуемых функций или применение эффективной политики паролей.

Следующие требования можно назвать зависящими от данных:

- Безопасность пользовательского ПО.

Сюда можно отнести задачи построения безопасных интерфейсов и механизмов доступа к данным.

– Безопасная организация и работа с данными.

Вопрос организации данных и управления ими является ключевым в системах хранения информации. В эту область входят задачи организации данных с контролем целостности и другие, специфичные для СУБД проблемы безопасности. Фактически эта задача включает в себя основной объем зависящих от данных уязвимостей и защиты от них [3].

Для решения проблем обеспечения информационной безопасности СУБД необходимо перейти от метода закрытия уязвимостей к комплексному подходу обеспечения безопасности хранилищ информации. Основными этапами этого перехода, должны стать следующие положения.

– Разработка комплексных методик обеспечения безопасности хранилищ данных на предприятии.

Создание комплексных методик позволит применять их при разработке и внедрении хранилищ данных и пользовательского ПО. Следование комплексной методике позволит избежать многих ошибок управления СУБД и защититься от наиболее распространенных на сегодняшний день уязвимостей.

– Оценка и классификация угроз и уязвимостей СУБД.

Классификация угроз и уязвимостей СУБД позволит упорядочить их для последующего анализа и защиты, даст возможность специалистам по безопасности установить зависимость между уязвимостями и причинами их возникновения. В результате при введении конкретного механизма в СУБД, у администраторов и разработчиков появится возможность установить и спрогнозировать связанные с ним угрозы и заранее подготовить соответствующие средства обеспечения безопасности.

– Разработка стандартных механизмов обеспечения безопасности.

Стандартизация подходов и языков работы с данными позволит создать средства обеспечения безопасности, применимые к разным СУБД. В данный момент они могут быть лишь методическими или теоретическими, так как, к сожалению, появление готовых комплексных программных средств защиты во многом зависит от производителей и разработчиков СУБД и их желания создавать и следовать стандартам [4].

Таким образом, информационные активы составляют основу бизнеса любой организации, а базы данных являются доминирующим инструментом для хранения структурированной информации. Растущие масштабы утечки критически важных данных делают все более актуальной необходимость в защите баз данных. Система защиты БД играет важнейшую роль в автоматизации контроля над действиями пользователей, работающими с базами данных, защите от внешних и внутренних угроз и повышении надежности функционирования баз данных.

Источники литературы

1.Основные аспекты безопасности СУБД. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://tproger.ru/articles/db-security-basics/– Дата доступа: 16.12.2018.

2.Безопасность базы данных. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://revolution.allbest.ru/programming/00752628_0.html– Дата доступа: 16.12.2018.

3.Защита и безопасность баз данных. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://scienceforum.ru/2015/article/2015015774– Дата доступа: 16.12.2018.

4.Безопасность баз данных. [Электронный ресурс]. – Электронные данные. – Режим доступа: http://samzan.ru/48348 – Дата доступа: 16.12.2018.

Gaiko Anastasia, Gorchanina Alesya
Belarus state economic university

Problems and prospects of database security

Annotation. The article discusses the existing problems of database security, their causes and features of database protection.

Keywords. Database, DBMS, information security, data protection, data security.

УДК 334.72

Гиносян Кристине Айковна, Кеян Сусанна Эдуардовна
Российско-Армянский университет
kristine-gh@mail.ru, sus.keyan@gmail.com

Стартап экосистема Армении и роль акселераторов в ее развитии

Армения когда-то была центром инноваций в сфере информационных технологий для СССР. Бурная история душит экономику, но ситуация с Кавказской республикой начинает улучшаться. Высококвалифицированные инженерные кадры постсоветского пространства и диаспора в сочетании с новыми правительственными инициативами способствуют возобновлению роста в сфере информационных технологий Армении.

Армения становится все более гостеприимным местом для иностранных инвестиций, с хорошими показателями по международным рейтингам. Инвестиционный климат Армении создает несколько проблем и рисков из-за ее небольшого рынка, его относительной географической изоляции из-за закрытых границ с Турцией и Азербайджаном, ВНД на душу населения около 3800 долларов и через искусственные ограничения конкуренции из-за коррупционных влияний. Армения официально вошла в торговый блок Евразийского экономического союза, единого экономического рынка с населением около 180 миллионов человек. В ноябре 2017 года Армения подписала Соглашение о всеобъемлющем и расширенном партнерстве с ЕС, которое частично направлено на улучшение инвестиционного и делового климата в Армении.

Недавнее законодательство значительно упростило процесс создания, эксплуатации и развития технологического стартапа в Армении.

Создание и поддержка здоровых инновационных «экосистем», привлекающих к себе и удерживающих предпринимателей, является необходимым условием конкурентоспособности страны в условиях рыночной экономики двадцать первого века. В связи с этим