Лекция 5. Защита баз данных / защита данных.

Обычно в процессе обсуждения защиты баз данных на первый план невольно выходит риск их взлома и утраты конфиденциальной информации. Представляется колоссальных масштабов трагедия: поврежденная деловая репутация, необратимые финансовые потери и долгий реабилитационный период. Далее выстраивается цепочка возможных мер, своевременное принятие которых позволило бы предотвратить случившееся, начинается тщательный анализ неучтенных уязвимостей во избежание будущих ошибок [1].

Серьезность последствий требует принятия действенных мер их предотвращения. В целом, все правильно. Однако анализ ситуации следует начать с принятия во внимания того факта, что даже самая незначительная брешь в системе защиты способна спровоцировать появление другой, более серьезной. Иначе говоря, причиной утечки или взлома могут стать неучтенные или должным образом нефункционирующие стандартные методы обеспечения безопасности информации. Речь пойдет именно о них, базовых, а вернее было бы даже сказать, основополагающих, способах защиты баз данных.

Средства защиты в различных СУБД несколько отличаются, однако общая суть в такой защите заключается в том, что система защиты информации в БД должна быть многоуровневой, и чем больше в ней уровней, тем сложнее будет ее преодолеть злоумышленнику. Нижние уровни образуют стандартные способы защиты, такие как защита паролем, шифрование данных, разграничение прав доступа к объектам БД, контрольный след выполняемых операций, резервное копирование – это своего рода база, то, без чего невозможно представить себе полноценную защиту.

Перечисленные способы являются частью более общей классификации уровней безопасности. Согласно «Критериям определения безопасности компьютерных систем» определяются четыре класса безопасности (Security Classes): D, C, B и A. Класс D обеспечивает минимальную защиту (Minimal Protection). Сюда относятся системы, безопасность которых не удовлетворяет требованиям более высоких классов. Класс C обеспечивает избирательную (Discretionary Protection), класс B – обязательную (Mandatory Protection), а класс A – проверенную защиту (Verified Protection).

Избирательное управление доступом

Избирательная защита класса C делится на 2 подкласса – C1 и C2, где подкласс C1 является менее безопасным, чем подкласс C2. Избирательное управление доступом осуществляется по усмотрению владельца данных.

Требованием класса C1 является разделение данных и пользователя, помимо взаимного доступа к данным возможно их раздельное использование пользователями.

Класс C2 дополнительно предусматривает учет на основе входа в систему, аудита и изоляции ресурсов. Избирательное управление доступом 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 идентификаией или распознаванием пользователя по его идентификатору – логину и паролю. Аутентификация, подтверждение достоверности идентификатора реализуется, например, секретным выражением. Далее требуется авторизация пользователя.

Согласно разграничению прав доступа пользователю предоставляются только те данные, на которые он имеет право.

Пароли с их главным достоинством – простотой и привычностью – при правильном использовании могут обеспечить приемлемый для многих компаний уровень безопасности. Надежность парольной защиты основывается на следующих требованиях:

– пароль должен представлять собой комбинацию букв, цифр или специальных знаков;

– длина пароля должна быть 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. В большинство СУБД встроен набор базовых средств по управлению правами доступа. Пользователи и группы наделяются правами доступа к определенным объектам базы данных. Помимо предоставления доступа многие СУБД указывают разрешенный тип доступа, начиная от только чтения, заканчивая реорганизацией всей базы данных.

Существует возможность управления правами на действия с определенным объектом в зависимости от его типа. Например, можно отдельно управлять правами на чтение, добавление, удаление и изменение записей в таблицах. Некоторые СУБД предусматривают управление доступом на уровне столбца таблицы или представления.

Обязательное управление доступом

В случае обязательного управления объектам данных присваиваются определенные классификационные уровни, образующие строгий иерархический порядок (например, «секретно», «совершенно секретно», «для служебного пользования» и т.д.), а каждый пользователь имеет соответствующий уровень допуска. Данная, достаточно статичная и жесткая, структура базы данных свойственна, например, военным или правительственным организациям. Пользователь имеет доступ к объекту БД, только если его уровень допуска идентичен или больше уровня классификации объекта. Более того, чтобы модифицировать объект уровень допуска пользователя должен быть равен классификационному уровню объекта. Таким образом, любой информации, внесенной пользователем, автоматически присваивается уровень, идентичный уровню классификации данного пользователя. Такая процедура исключает запись секретных данных пользователем с высоким уровнем секретности в файл с меньшим классификационным уровнем, тем самым сохраняя систему секретности. Обязательная защита класса B делится на три подкласса – B1, B2 и B3, где подкласс B1 наименее безопасен, а B3 является наиболее безопасным подклассом.

В соответствии с требованиями класса B1, как было сказано выше, каждый объект данных содержит отметку о его уровне классификации, а также неформальное сообщение о действующей стратегии безопасности.

Согласно требованиям класса B2, дополнительно требуется формальное утверждение о действующей стратегии безопасности. Кроме того, необходимо обнаружить и решить вопрос с плохо защищенными каналами передачи информации.

Наконец, класс B3 помимо прочего требует поддержки аудита, восстановления данных и назначение администратора режима безопасности. Что же касается класса A, такая защита является наиболее безопасной и требует математического доказательства соответствия метода обеспечения безопасности заданной стратегии.

Шифрование данных

Незаконно проникнуть в базу данных можно не только воспользовавшись обычными средствами доступа в системе, но и, подключившись к коммуникационному каналу, фактически переместить часть базы данных. Использование криптографических средств сокрытия информации позволит предотвратить данную угрозу. Для этой цели используется шифрование данных, т.е. хранение и передача конфиденциальных данных в зашифрованном виде. Процесс шифрования заключается в преобразовании с помощью специального алгоритма исходных данных (открытого текста) в новое представление, скрывающее содержание исходной информации. Зашифрованный текст с секретным ключом шифрования хранится в базе данных и передается по коммуникационному каналу.

Существуют два режима работы с зашифрованными базами данных. Первый способ заключается в дешифровании необходимого файла или части файла на внешнем носителе. После выполнения необходимых действий с открытой информацией, она вновь зашифровывается на внешнем запоминающем устройстве. Независимое последовательное функционирование средств шифрования и СУБД является несомненным достоинством такого режима. Однако в результате сбоя или отказа часть базы данных может остаться записанной в незашифрованном виде.

Дешифрование может производиться также в оперативной памяти непосредственно перед выполнением необходимых действий с данными. Процедуры шифрования в данном случае встроены в СУБД. Необходимо отметить, что при этом, несмотря на достаточно высокий уровень защиты от несанкционированного доступа, снижается уровень производительности СУБД в связи с ее усложнением.

Контрольный след выполняемых операций и резервное копирование

Контрольный след позволяет регистрировать детальные сведения обо всех операциях пользователей с БД. Данная сохраненная информация играет весьма существенную роль в обнаружении несанкционированного вмешательства в базу данных, выявлении уязвимостей в системе защиты, а также устранении каких-либо внесенных искажений данных.

Как правило, запись контрольного следа содержит системный номер терминала, с которого поступил запрос, ID пользователя, выполнившего операцию, дату и время запуска операции, исходный текст запроса, базовые отношения, кортежи и атрибуты, вовлеченные в запрос, а также исходные и конечные значения.

Помимо всего вышеперечисленного можно также отметить резервное копирование, позволяющее восстанавливать данные на случай аппаратных или программных сбоев. Рекомендуется настроить регулярное резервное копирование базы данных и хранить файлы не только на жестком диске компьютера, но также дублировать их на ленту или жесткий диск другого компьютера в сети.

Под "базой данных" понимается объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Любая база данных включает три составные части:

a) содержимое, т.е. хранимое в памяти произведение или информацию;

b) программное обеспечение, необходимое для функционирования базы данных;

c) другие электронные вспомогательные материалы (тезаурус, указатели, систему запросов).

Таким образом, база данных состоит из содержания и процесса упорядочения этого содержания. Авторское право распространяется только на отбор и упорядочение информации, а также на вспомогательные материалы (необходимые для функционирования базы данных), не затрагивая содержимого базы данных.

Что такое авторское право.

Понятие автора является одним из ключевых в авторском праве. В Законе РФ «О правовой охране программ для ЭВМ и баз данных» в ст. 8 сказано: «Автором программы для ЭВМ или базы данных признается физическое лицо, в результате творческой деятельности которого они созданы».

Авторское право на программу для базы данных, как и на любые иные объекты авторского права, возникает в силу их создания.

Субъектом авторского права на программу для базы данных признается правообладатель, под которым понимается автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительными имущественными правами, полученными в силу закона или договора.

Авторское право распространяется на любые программы для базы данных, как выпущенные, так и не выпущенные в свет, представленные в объективной форме независимо от материального носителя.

Права в отношении программы для базы данных подразделяются на личные и имущественные права.

К личным правам отнесены:

1) право авторства - то есть право считаться автором программы для базы данных;

2) право на имя - то есть право определять форму указания имени автора в программе базы данных: под своим именем, под условным именем (псевдонимом) или анонимно;

3) право на неприкосновенность (целостность) - то есть право на защиту как самой программы для базы данных, так и ее названия от всякого рода искажений или иных посягательств, способных нанести ущерб чести и достоинству автора.

Они связаны непосредственно с авторством на программу для базы данных, являются неотчуждаемыми (то есть не могут быть переуступлены другому лицу) и не ограничены сроком.

Имущественные права на программы базы данных связаны с возможностями автора по их использованию, а именно: выпуск в свет (опубликование); воспроизведение (полное или частичное) в любой форме, любыми способами;

распространение; модификацию и иное использование. Они могут быть переуступлены другому лицу (отчуждены) и срок их действия ограничен.

Определение термина «выпуск в свет (опубликование)» необходимо для различения опубликованных и неопубликованных произведений, имеющих разный правовой режим. Выпуск в свет программы для базы данных представляет собой по сущности процесс последовательной реализации права на воспроизведение и права на распространение.

Воспроизведение базы данных - это изготовление одного или более экземпляров базы данных в любой материальной форме, а также их запись в память ЭВМ.

Распространение базы данных - это предоставление доступа к воспроизведенной в любой материальной форме программе для базы данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставление взаймы, включая импорт для любой из этих целей.

Модификация программы БД - любое ее изменение, за исключением тех какие относятся к адаптации, в том числе перевод базы данных с одного языка программирования на другой. Модификация баз данных в современных условиях быстрого развития вычислительной техники является необходимым условием поддержания их конкурентоспособности.

Личные права могут принадлежать только автору - физическому лицу, в результате творческой деятельности которого создана программа для базы данных. Все иные физические и юридические лица, в том числе наследники и другие правопреемники, могут обладать только имущественными правами на программу для базы данных.

В целях оповещения о своих имущественных правах правообладатель может, начиная с первого выпуска в свет программы для базы данных, использовать знак охраны авторского права, состоящий из трех элементов: буквы "С" в окружности или в круглых скобках, наименования (имени) правообладателя и года первого выпуска программы для базы данных в свет.

Цель защиты прав на программы для базы данных - обеспечение прав авторов и иных правообладателей, а также предотвращение несанкционированных действий в отношении программ для базы данных.

Можно выделить несколько основных видов нарушений авторского права, которые особенно распространены у нас.

Это изготовление и распространение некоторыми фирмами поддельных экземпляров программ без разрешения правообладателей, по внешнему виду весьма схожих с оригинальными, изготовленными фирмами-производителями.

Изготовление контрафактных экземпляров путем записи на магнитные или оптические диски и их последующая реализация по более низким ценам; изготовление экземпляров, число которых превышает уровень, разрешенный правообладателем, для последующего распространения.

Широко распространено изготовление контрафактных экземпляров для баз данных конечным пользователем. Приобретение контрафактного экземпляра у законного пользователя, часто безвозмездно; установка законно приобретенной программы на большее число ЭВМ, чем это разрешено правообладателем.

С появлением телекоммуникационных средств практикуется несанкционированное распространение программ для баз данных по сетям ЭВМ, не исключая и международных каналов связи, по существенно сниженным ценам.

Все эти незаконные действия наносят значительный материальный ущерб фирмам-разработчикам баз данных. Поэтому потребовалось выработать соответствующие меры борьбы против нарушителей авторского права и для защиты прав законных правообладателей программ для баз данных.

Применяемые в настоящее время средства защиты можно условно разделить на следующие категории: а) программно-технические, б) правовые, в) экономические и г) комплексные, являющиеся сочетанием первых трех.

Программно-технические средства защиты предусматривают создание с помощью различных технических средств искусственных преград, которые в той или иной мере затрудняют воспроизведение и распространение программ. Например, жесткая привязка программы к конкретной ЭВМ; индивидуальное присвоение каждому законному пользователю специальных кодов и т.п. Существенный недостаток этого способа, весьма ограничивающий его применение - высокая вероятность применения специальных средств противодействия, постоянно совершенствуемых одновременно с совершенствованием программно-технических средств защиты.

Правовой способ защиты основывается на распространении норм авторского права на программы для базы данных. Это позволяет применять к правонарушителям установленные законодательством гражданско-правовые и уголовно-правовые санкции и реализовать нарушенные права правообладателей в принудительном порядке с помощью правоохранительных органов. При этом за защитой своего права авторы и правообладатели могут обращаться в суд, арбитражный или третейский суд. Суд или арбитражный суд могут вынести решение о конфискации контрафактных экземпляров программ для баз данных, а также материалов и оборудования, используемых для их воспроизведения, и об уничтожении, либо о передаче их в доход бюджета России, либо истцу по его просьбе в счет возмещения убытков.

В России существенную поддержку правообладателю в деле защиты его прав при возникновении разрешаемых судебными органами конфликтных ситуаций, связанных с нарушением авторских прав, дает официальная регистрация программ для баз данных в Российском агентстве по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем (РосАПО). При возникновении спора суд по заявлению соответствующий стороны может запросить в РосАПО депонированные материалы, рассматриваемые судом в качестве вещественных доказательств.

Экономический способ защиты прав на программы для базы данных заключается в создании условий, которые делают нарушение прав экономически невыгодным. Это достигается благодаря установлению различных льгот законным пользователям, обеспечению их бесплатной консультационной и технической поддержкой, сопровождению, обучению и предоставлению оперативной информации по новым версиям программ и баз данных. Эти версии реализуются со значительной скидкой для добросовестных пользователей [2].

Таким образом, защита баз данных должна осуществляться поэтапно, начиная с принятия базовых мер. Описанные выше методы способны в определенной степени обеспечить конфиденциальность и целостность данных, однако их использование не гарантирует полной безопасности данных. Для повышения уровня сохранности информации в базе данных рекомендуется использование комплексных мер, включая

интеграцию СУБД со специальными программными продуктами для защиты информации.

Список используемой литературы:

1. С чего начинается защита базы данных? URL: https://www.dataarmor.ru/%D1%81-%D1%87%D0%B5%D0%B3%D0%BE-%D0%BD%D0%B0%D1%87%D0%B8%D0%BD%D0%B0%D0%B5%D1%82%D1%81%D1%8F-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%B1%D0%B0%D0%B7%D1%8B-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85/

2. Правовая защита баз данных. URL: https://studwood.ru/553372/pravo/pravovaya_zaschita_baz_dannyh.