Защита данных на уровне СУБД:
актуальные проблемы и методы защиты

Иван ПАНЧЕНКО,
заместитель генерального директора, Postgres Professional

Сегодня уже никого не нужно убеждать в том, что данные – это «нефть» XXI века. Но достаточно ли они защищены? Даже гиганты вроде «Яндекса» не застрахованы от утечек данных: в январе 2023 г. злоумышленники выложили в открытый доступ код внутренних сервисов интернет-компании. Ущерб от подобных действий может быть миллионным. Благодаря таким «сливам» хакеры могут находить уязвимости, а конкуренты – копировать ноу-хау лидеров ИТ-рынка. Еще более частым случаем является утечка персональных данных пользователей.

Согласно исследованию Consoltech, до 94% компаний никогда не восстанавливаются после крупной потери данных и почти 70% предприятий малого бизнеса закрываются в течение года после инцидента. У крупных компаний больше возможностей нивелировать негативные последствия. Тем не менее и они сталкиваются с ужесточением ответственности за утечки персональных данных.

По данным Tadviser, максимальный штраф за утечку персональных данных для бизнеса в России составляет 500 тыс. руб. 26 декабря 2022 г. стало известно о решении Минцифры РФ установить для компаний штрафы за утечку персональных данных в диапазоне от 5 млн до 500 млн руб. – соответствующий законопроект находится на рассмотрении и, как ожидается, вступит в силу в сентябре 2023 г. Среди прочих мер в нем обсуждается и введение уголовной ответственности за незаконный сбор, хранение, использование и передачу баз данных – эта инициатива уже поддержана Правительством РФ.

В 2022 г. объем утечек информации в России, по данным Infowatch, вырос более чем в два раза – зарегистрировано 710 случаев, связанных с компрометацией данных. Компании могут существенно снизить риски за счет грамотной работы с системами управления базами данных (СУБД). Современные СУБД обладают встроенными возможностями защиты и восстановления данных. Их правильная конфигурация обеспечивает разграничение прав доступа, снижая вероятность возникновения утечки. В частности, СУБД можно настроить так, что доступ к чувствительным данным будет, например, у двух человек, а не у двадцати.

Роли и профили пользователей

В СУБД PostgreSQL и разработанной нами для высоконагруженных промышленных систем СУБД Postgres Pro есть развитая система ролевого управления доступом пользователей. Благодаря ей каждый пользователь получает доступ к строго определенной части данных и операций над ними. В качестве пользователя БД может выступать не только человек, но и приложение – в этом случае тоже есть возможность позаботиться о том, чтобы оно имело ровно тот доступ к данным, который ему необходим. Это забота архитекторов прикладных систем, их разработчиков и администраторов баз данных. Одна из типичных ошибок – предоставление пользователю избыточных полномочий. Например, если вы назначаете непроверенному стороннему приложению роль суперпользователя с доступом «на всё», то сильно рискуете: из-за ошибки или уязвимости в приложении можно лишиться всех данных. Для компаний с крупными мультитерабайтными системами важность минимизации доступа возрастает: цена ошибки слишком высока.

Еще одна проблема – ненадежные пароли, особенно у пользователей с большими привилегиями, их использование по-прежнему является ахиллесовой пятой. Поэтому, в частности, для СУБД Postgres Pro были разработаны дополнительные расширенные политики аутентификации пользователей. Они позволяют ограничивать

использование базы данных и устанавливать требования к паролям при назначении профилей ролям. Каждый профиль определяет набор параметров, ограничивающих использование базы данных, и его можно назначить конкретной роли и всем новым пользователям с такой ролью. Таким образом, в самой СУБД предусмотрена защита от предоставления чрезмерных прав пользователям. Конечно, этими возможностями нужно умело пользоваться и активно следить за новыми релизами СУБД.

Работа с обновлениями

Для отслеживания новостей о свежих выпусках СУБД есть еще одна причина – устранение уязвимостей в новых версиях. Их обнаруживают даже в самых зрелых программных продуктах с высоким качеством кода. Своевременные обновления означают, в частности, и устранение известных уязвимостей – если у вас СУБД очень старой версии, этим могут воспользоваться. Информация о серьезных уязвимостях и затрагиваемых версиях продукта зачастую публична. С одной стороны, пользователи благодаря этому могут оценить масштаб вероятных проблем, с другой – у злоумышленников появляется практически готовый план действий. Вот почему обновлениями не следует пренебрегать и откладывать их бесконечно.

Если вы получили в обслуживание СУБД очень старой версии, но не решаетесь выполнить обновление самостоятельно, следует рассмотреть возможность привлечения экспертов. Это обойдется дешевле, чем штрафы за утечку персональных данных и устранение последствий атаки злоумышленников на вашу организацию.

Маскировка данных

Во многих проектах с активно ведущейся разработкой часто используется практика тестирования вновь разработанной функциональности на данных, приближенных к «боевым». То есть у сотрудников отдела разработки есть полная копия всей базы данных на конкретную дату. Насколько защищено окружение разработки? Насколько вы доверяете сотрудникам-разработчикам? Копия базы, пусть и не совсем актуальная, тоже должна быть защищена, и в этом может помочь маскировка (обфускация) данных. Как показывает внутренняя статистика Postgres Pro, спрос на нее огромный.

При маскировке имеющиеся подлинные данные заменяются похожими на них фиктивными, что вполне подходит для целей разработки, а настоящие персональные данные и конфиденциальные сведения при этом остаются недоступными для потенциальных злоумышленников. Маскировка может быть как статической (применяемой к конкретной копии базы данных), так и динамической (на лету). С распространением практики непрерывной интеграции (CI/CD) динамическая маскировка данных стала особенно востребованной. На уровне компании у нас было принято решение развивать расширение-анонимайзер, обеспечивающее оба типа маскировки данных.

> Риск того, что какие-то данные в базе будут повреждены или потеряны, сохраняется всегда.

Резервное копирование и восстановление

Риск того, что какие-то данные в базе будут повреждены или потеряны, сохраняется всегда. Практика снятия резервных копий (бэкапов) предусмотрена во всех СУБД, ориентированных на промышленную эксплуатацию. При работе с большими СУБД не всегда удобно делать их полные копии: иногда целесообразно снимать полную копию один раз в течение какого-то периода и часто копировать только накопившиеся с тех пор изменения. На этом основана практика разработанных нами инкрементальных бэкапов, которые создаются с помощью специальной утилиты pg_probackup. Таким образом обеспечивается страховка от риска повреждения и потери данных, при этом резервные копии не занимают много места (с ростом цен на серверное «железо» это крайне важно).

Недостаточно регулярно снимать копии с базы и надежно их хранить, восстановление базы из бэкапа нужно тщательно тестировать, на практике убеждаться, что вы знаете, что делать с этими копиями, если основная база данных выйдет из строя. Без налаженного процесса восстановления вы можете либо потерять данные навсегда, потому что копии базы по какой-то причине окажутся неактуальными, либо на их восстановление уйдет масса времени, что негативно скажется на работе пользователей. Компетенции администраторов баз данных (DBA) становятся все более редкими и дорогими, опытных специалистов на рынке сейчас мало, поэтому квалифицированная техподдержка для СУБД – хороший выход в такой ситуации: так вы точно получите рабочие копии, из которых вашу базу данных можно будет восстановить, и сможете работать дальше.

Внедрения кода и вредоносные запросы

С помощью «плохих» SQL-запросов может быть выполнен целый ряд вредоносных действий. Если запросы будут слишком «тяжелыми» и перегрузят СУБД, вплоть до отказа приложения,

оно станет недоступно пользователям. Если в теле запроса будет присутствовать вредоносный код для внедрения (SQL injection), а вы не приняли мер, то вашу базу данных смогут удалить или скопировать посторонние лица, получившие несанкционированный доступ. К счастью, сейчас существуют инструменты оценки уязвимостей и специально разработанные практики безопасного использования СУБД, которые помогают защититься от подобных проблем. Качественные средства мониторинга также позволяют обнаружить запросы, на исполнение которых уходит подозрительно много времени.

Для защиты современных веб-приложений существует множество сторонних инструментов, включая защитные экраны WAF (Web Application Firewalls). Кроме того, полезно повышать осведомленность разработчиков о внутреннем устройстве используемой СУБД – часто после такого обучения они принимают более рациональные решения при проектировании приложений и написании запросов, минимизируя риски отказа из-за перегруженности базы.

Физический сервер: ЦОД и облака

Немаловажную роль играет и физическое расположение сервера базы данных и уровень безопасности в конкретном центре обработки данных (ЦОД). Если по каким-то причинам пострадает физический сервер с данными, у вас должна быть их копия. Поставщики услуг облачной инфраструктуры имеют свои стандарты безопасности, которые далеко не всегда совпадают с потребностями их клиентов (провайдер исходит из того, что нужно большинству пользователей услуг, а у вас может быть нестандартный случай).

Ошибочно думать, что размещение в облаке гарантирует вашим данным стопроцентный уровень безопасности – риски сохраняются и в этом случае. Если вы сделали выбор в пользу облачной инфраструктуры и конкретного провайдера DBaaS (Database-as-a-Service), нужно получить полное представление о том, что можно менять и что нельзя. Работа по обеспечению безопасности должна вестись и с вашей стороны.

Безопасность или скорость?

Среди практиков, работающих с СУБД, распространено мнение, что нужен некий разумный компромисс между безопасностью СУБД и скоростью работы. На самом деле не все, что мы делаем ради безопасности данных, вынуждает СУБД работать медленнее: при рациональном подходе можно сохранить высокую производительность. Тем не менее попытки обеспечить максимальную безопасность без глубокого понимания внутреннего устройства СУБД действительно могут привести к избыточным мерам, замедляющим работу СУБД и приложения.

О возможных рисках

Уход западных вендоров значительно увеличил риски российских пользователей их решений. Во-первых, по истечении срока действия лицензии зарубежные компании не смогут гарантировать своевременного устранения некорректного поведения и уязвимостей в системах. Во-вторых, «ключи от кода» находятся в руках коммерческих компаний, подконтрольных недружественным России странам. Возможные решения проблемы вроде самоорганизации оставшихся сотрудников западных вендоров в сервисные компании или принудительное лицензирование такого ПО вызывают большие сомнения с точки зрения безопасности. В обозримом будущем, по мере того как сроки действия лицензий будут подходить к концу, ситуация может обостриться.

На этом фоне возрастет востребованность решений российских разработчиков, которые выполняют взятые обязательства и действуют в рамках российского юридического поля. Повысится и интерес к отечественным решениям, имеющим сертификацию ФСТЭК, которая служит дополнительной гарантией безопасности. Мы уже отмечаем увеличение количества пользователей сертифицированной версии СУБД Postgres Pro со встроенными дополнительными средствами защиты от несанкционированного доступа и ожидаем, что в будущем это продолжится – такие решения становятся отраслевым стандартом.

О силе сообщества

Среди других трендов – повышение спроса на ПО разработчиков на базе ОСПО. Любая СУБД без обновлений стремительно накапливает угрозы безопасности, поэтому так важен регулярный переход на более свежие версии и налаженный контакт с разработчиками решения. В идеальной ситуации компания ведет собственную разработку и передает накопленные знания о найденных проблемах в сообщество, в свою очередь, получая оттуда информацию об уязвимостях, обнаруженных другими его участниками. В итоге код проекта, созданного сильным сообществом, наиболее защищен, и на его базе целесообразно развивать коммерческие решения (этому требованию соответствует свободная СУБД PostgreSQL, ставшая основой для Postgres Pro). В такой открытой работе сообщества над безопасностью есть большой практический смысл: зачастую сами пользователи подсказывают, что еще можно сделать для совершенствования защиты.

Кадры решают всё

Разумеется, в рамках одного материала невозможно рассмотреть все приемы и решения для обеспечения безопасности СУБД. Основной риск – это всегда человеческий фактор. Поэтому качественная работа с кадрами, обучение сотрудников лучшим практикам работы с СУБД, грамотные корпоративные политики и постоянная разъяснительная работа о потенциальной опасности тех или иных действий помогут существенно снизить риски. ■