Безопасность баз данных: проблемы и методы обеспечения

С.Л. ДОБРУШСКИЙ, менеджер по разработке продукта "Гарда БД" компании "МФИ Софт"

От уровня защиты баз данных (БД) зависит не только сохранность информации, но и непрерывность всего бизнеса в целом. Любые перебои в работе или компрометация коммерческих данных могут нарушить устоявшиеся бизнес-процессы и парализовать деятельность компании. Кроме этого, информация об утечке персональных данных клиентов или любая другая, защищаемая нормативными актами, обычно влечет за собой не только ухудшение репутации, но и отзыв лицензий или штрафы регуляторов.

Распространенные проблемы безопасности баз данных

Очень часто защите баз данных в компаниях не уделяют должного внимания. Среди самых распространенных причин, почему организации не хотят заниматься этим направлением, можно выделить следующие:

на предприятии установлена DLP-система, контролирующая деятельность сотрудников на рабочих местах. В данном случае, зачастую, руководство не видит смысла в защите еще и баз данных. Такой подход в корне неверен, так как DLP-системы не могут осуществлять контроль обращений к базам данных, если сотрудник не копировал таблицы с данными полностью. Кроме того, остается открытым вопрос контроля веб-приложений БД и внешних обращений к ним;

служба безопасности в принципе понимает целесообразность защиты БД, но в силу недостаточной информированности иногда не считает это направление задачей первостепенной важности. Такая позиция характерна для предприятий нефинансового сектора, пользующихся услугами системных администраторов по аутсорсингу;

подключение внутреннего логирования на серверах БД дает службе безопасности надежду на простое выявление нарушителей. Многие считают, что в этом случае достаточно поднять архивы логов и таким образом вычислить виновного. Однако такой подход позволяет выявить лишь небольшую долю возможных нарушений.

Подобные позиции объединяет недостаточное понимание серьезности проблемы защиты БД и кажущаяся сложность инфраструктуры последних. Безусловно, базы данных, их структура, синтаксис запросов к ним — вещи совсем не тривиальные, и, как правило, они находятся не в прямой компетенции службы безопасности. В обязанности сотрудников этого подразделения входит настройка гораздо более простых (типовых) политик безопасности, в частности, таких как "запрет использования USB-носителей" или "ограничение доступа на различные сайты в рабочее время". При этом существуют специализированные продукты, позволяющие решать многие задачи быстрее, а также автоматизировать ряд процессов. Организовать действительно качественную защиту баз данных без таких продуктов практически невозможно, так как сотруднику службы безопасности для этого необходимо обладать большим количеством непрофильных знаний. Без должной компетенции слишком много задач придется перекладывать на IT-отдел, что в лучшем случае будет доставлять ряд неудобств, а в худшем (и часто встречающемся на практике) — окажется просто невозможным.

Рассмотрим типовую задачу по защите баз данных, характерную для предприятия практически из любой отрасли.

Построение системы защиты баз данных без специализированных средств

Как правило, процесс осуществления мероприятий по защите БД начинается с составления перечня баз, которые действительно нуждаются в контроле, т. е. с необходимости определения, где именно содержится по-настоящему ценная для компании информация. И здесь сразу же следует объяснить, почему возникает необходимость выделения избранных баз данных и отсутствует смысл в контроле сразу всех. Практика внедрений систем защиты показывает, что только 20 — 30 % БД в компаниях содержат критичную информацию, на обеспечение конфиденциальности которой действительно стоит тратить ресурсы. Остальные выполняют лишь вспомогательные функции: в одних хранится внутренняя информация, другие используются для тестовых целей, отладки и т. д.

После того, как перечень контролируемых баз данных составлен, необходимо определить, какие данные являются наиболее ценными. Если перенести эту задачу на язык работы с БД, нужно выделить ряд таблиц, полей, вызываемых процедур, синонимов и представлений. В случае, когда у компании нет практики вести полноценную документацию с описанием классов охраняемой информации и мест их хранения, то сотрудник службы безопасности будет вынужден практически вручную перебирать тысячи таблиц и просматривать информацию в них, что сопряжено со значительными время- и трудозатратами. К тому же сама структура БД может меняться: в ней могут появляться новые таблицы или удаляться старые. При этом администраторы баз данных вполне способны создавать разные временные единицы: сино-