Защита баз данных в банке

Проблемы и решения

МФИСОФТ

Аналитический центр
ООО «МФИ Софт»
2013 год

Содержание

Защита баз данных в банке — проблемы и решения

Какие проблемы защиты баз данных чаще всего возникают в компаниях и как их решить без ущерба для бизнеса рассказывают аналитики «МФИ Софт» на примере крупного регионального банка.

От уровня защиты баз данных 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. Помимо этого, информация об утечке персональных данных клиентов или другой информации, защищаемой нормативными актами, обычно влечет за собой не только ухудшение репутации, но и отзыв лицензий или штрафы регуляторов.

В качестве системы контроля баз данных многие компании используют штатные возможности СУБД для протоколирования действий пользователей, но, как показывает практика, этого функционала недостаточно для противодействия современным приемам злоумышленников. Кроме того, дополнительная нагрузка на сервер снижает скорость обработки данных и увеличивает время бизнес-процессов.

Распространенные проблемы защиты баз данных

Журналирование и аудит штатными средствами

Встроенные в СУБД возможности журналирования и аудита не обеспечивают должный уровень визуального контроля. Большинство из них не способны фиксировать выполненные изменения, использованные для этого права, администраторские учетные записи или системные изменения. Они служат больше для мониторинга, чем для защиты, поэтому чаще всего администраторы их просто отключают, поскольку встроенные средства журналирования и аудита способны снизить производительность базы данных. Решение по защите баз данных должно иметь возможность многоуровневого администрирования и защищенного журналирования. Это реализуется лишь в том случае, когда решение подключено параллельно базе данных.

Интегрированный контроль всех баз данных

Ведение отдельных аналитических выкладок по каждой базе данных не дает полной картины действий пользователей. Методами социальной инженерии злоумышленники способны замаскировать нарушения под совершенно легитимные действия пользователей, отвечающие политикам каждой из баз данных. Визуализация и объединение статистик пользования всеми базами данных повышает шансы на оперативное выявление инцидентов. Особенно актуален такой подход к защите баз данных для компаний, использующих облачные базы данных (включая интернет-банкинг, личные кабинеты и т.п.).

Контроль прав доступа в ручном режиме

Многие компании не придают значения строгому разграничению прав доступа к базам данных. Обычно уровень доступа, предоставляемый пользователям,

существенно шире набора функций, соответствующих их роли в системе. Кроме этого, ИТ-специалисты не всегда вовремя удаляют неиспользуемые учетные записи, что обеспечивает широкие возможности для злоумышленников. С помощью известного набора хакерских технологий подбора злоумышленники могут получить доступ к любой учетной записи, в том числе – администратора, и не только взломать ее, но и поднять права доступа в системе. Стандартные системы мониторинга активности пользователей не реагируют на подобные инциденты, так как с точки зрения системы они являются вполне легитимными. Система защиты должна уметь выявлять сеансы работы, идущие вразрез с политикой безопасности, направлять оповещения на консоль централизованного управления, а также обнаруживать способы обхода системы безопасности.

Архивы: запись, поиск, обработка

Хранение больших архивов данных для многих компаний становится сложной задачей, поскольку требует большого количества ресурсов. Тем не менее, ведение архивов изменений в базах данных необходимо в целях безопасности и для проведения служебных расследований. По этим причинам в специализированных системах обычно предусматривается функция быстрого поиска по архивам, дающая возможность анализировать большие массивы данных. Решение должно обладать высокой скоростью обработки данных и функцией циклической перезаписи данных для обеспечения автономной работоспособности комплекса без влияния администраторов системы.

Базы данных, как и любые ИТ-системы, требуют специализированной защиты, и далеко не всегда лучшим решением являются штатные разработки производителей СУБД. Для производства самих СУБД и систем их защиты применяются совершенно разные технологии, требующие наличия у разработчиков различных компетенций. То же самое можно сказать и о любом другом ИТ-решении, требующем специальной системы защиты (производители ОС не выпускают антивирусы или межсетевые экраны). Для лучшей защиты баз данных существуют специализированные технологии.

Специализированная защита баз данных

Системы управления базами данных широко распространены в российских компаниях. Существуют как универсальные СУБД, так и специализированные решения, предназначенные для определенного вида бизнеса – и все они имеют свои особенности и специфические проблемы.

В России существует несколько компаний предлагающих специализированные системы защиты информации от неправомочного доступа в СУБД. Ниже перечислены основные возможности таких систем:

- Выявление аномальных ситуаций путем сравнения всех действий, выполняемых с базой данных, с установленным базовым состоянием. Например, атака типа SQL Injection обычно состоит из команд, направленных на получение доступа к базе данных. При этом используемые SQL-команды нетипичны для стандартных бизнес-приложений компании.
- Выявление исключительных ситуаций, основанное на задаваемых пороговых значениях (например, предельное число неудачных попыток подключений или SQL-ошибок). Наличие SQL-ошибок может свидетельствовать о том, что злоумышленник пытается подобрать имена ключевых таблиц, используя команды с различными аргументами.
- Отслеживание всех данных, выгружаемых из базы, и сравнение их с определенными шаблонами. Например, могут отслеживаться запросы номеров кредитных карт или выгрузка большого объема данных, которая может свидетельствовать о взломе системы.
- Обнаружение и классификация конфиденциальных данных – обнаружение и анализ конфиденциальных данных и отношений до их переноса в среды больших данных, с целью оптимизации политик безопасности.
- Контроль доступа к данным и их изменений – создание политик, регулирующих права пользователей и приложений на доступ к данным и их изменение в средах больших данных.
- Мониторинг и аудит работы с данными в режиме реального времени – знание того, кто, когда, как и где получал доступ к данным, и формирование отчетности для обеспечения соблюдения требований.

- Защита данных – преобразование данных путем маскировки и шифрования.
- Предотвращение утечки данных – ведение контрольного журнала доступа к данным и их использования для исключения потери данных.
- Управление уязвимостями – знание слабых мест и применение политик для их устранения.
- Управление соблюдением требований – создание системы для подготовки, распространения и утверждения отчетов о соблюдении требований в системах больших данных.

Практика защиты баз данных в банковской сфере

Дальневосточный филиал ОАО «МТС-Банк» является лидирующей финансовой организацией региона и постоянно работает над укреплением своих позиций, в частности, за счет повышения уровня безопасности банковской системы.

Для повышения защищенности баз данных в 2013 году был реализован проект внедрения комплексной системы аудита и защиты информации от неправомочного доступа в автоматизированной банковской системе.

Масштаб проекта:

- более 1 000 автоматизированных рабочих мест
- более 20 000 информационных объектов

Цели проекта

- Повышение уровня защищенности баз данных Банка от нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения данных;

- Минимизация операционных рисков в части неправомочных и противоправных действий работников при обращении к АБС банка
- Сохранение высокой скорости доступа и обработки информации в базах данных.

Использованное ПО, оборудование и вспомогательные системы

- АПК «Гарда БД» (МФИ Софт)
- РБО ЦФТ-Ритейл банк
- ИБСО (информационная банковская система объектно-ориентированная на базе Oracle)

Уникальность

Проект позволил настроить многоуровневый контроль баз данных, с градацией по пользователям, включая администраторов. В результате проекта снижены риски, связанные со случайными и умышленными ошибками сотрудников при работе с базами данных с минимальными затратами на проект. Экспертные оценки свидетельствуют, что внедрение таких комплексов ведет к снижению вероятности наступления угроз на 35%.

Во многом проект можно назвать уникальным благодаря скорости его реализации – полностью внедрить и ввести в эксплуатацию систему контроля 20 000 информационных объектов удалось за три дня.

Описание проекта

На момент реализации проекта (тогда еще в Далькомбанке), у банка уже был опыт использования систем аудита доступа к базам данных. Используемая АБС позволяла контролировать операции, производимые в системе. Но, учитывая территориальную удаленность операторов системы от ЦОД и большой объем производимых ими операций в течение одного операционного дня (от нескольких десятков до сотен тысяч), это создавало большую нагрузку на инфраструктуру СУБД. Поэтому использование возможностей контроля, «встроенных» в АБС, могло периодически создавать проблемы в ее эксплуатации. Кроме этого, возможность прямого доступа к такой информации администраторов СУБД создавала риск внесения несанкционированных изменений в журналы протоколируемых событий.

В итоге специалисты банка пришли к пониманию, что, внедрив комплексную систему мониторинга работы с базами данных, можно снизить описанные риски и реагировать на возможные инциденты в режиме реального времени.

В результате сравнительного анализа решений аналогичного класса была выбрана система «Гарда БД», разработанная российской компанией «МФИ Софт», как наиболее подходящая для решения описанных задач. По сравнению с другими решениями у «Гарды БД» был ряд преимуществ:

- отсутствие влияния на производительность системы управления базами данных;
- невозможность вмешательства в работу аудита со стороны администраторов базы данных;
- контроль всех обращений и операций с базой вплоть до полей данных, независимо от пользователя и приложения (авторизация, доступ к данным, изменение схемы данных, изменение данных, изменение прав доступа);
- низкоуровневый контроль удаленного вызова процедур к базе данных;
- предоставление дополнительной статистической информации по каждому событию (дата\время события, объем передаваемых данных, логин, IP-адрес и порт источника\приемника и т.д.);
- построение статистических отчетов, ведение журналов событий;
- независимость от топологии системы базы данных;
- контроль нескольких независимых баз данных с единого центра управления;
- высокие скорости обработки данных (1 Гбит\сек и выше);
- удобный интерфейс с механизмом уведомления пользователей системы в режиме реального времени
- комплексная техническая поддержка и приемлемая стоимость.

Внедрение и первоначальная настройка АПК «Гарда БД» в локальную сеть Банка были реализованы в максимально короткие сроки. Система «Гарда БД» была встроена в инфраструктуру банка без изменения топологии сети. После подготовительного этапа понадобилось еще два дня на установку системы и запуск опытной эксплуатации.

На данный момент в Банке функционирует комплексная система защиты, перехватывающая информацию в рамках заданных критериев анализа в

режиме 24/7 и анализирующая в автоматическом режиме полученные данные с уведомлением сотрудников отдела ИБ о выявлении статистических аномалий и инцидентов.

Результаты проекта

Обеспечение безопасности баз данных в финансовом предприятии имеет высокое значение для работы предприятия в целом за счет минимизации целого комплекса рисков, а также удовлетворения законодательных норм. Внедрение системы «Гарда БД» сделало комплекс защиты информации банка более гибким, на порядок увеличилась оперативность принятия решений при предотвращении инцидентов нарушения политик информационной безопасности. Специалисты по информационной безопасности получили расширенные аналитические возможности обработки данных аудита, что повысило прозрачность процессов использования баз данных, а также эффективность и безопасность всех бизнес-процессов в целом.

«Благодаря тому, что система «Гарда БД» достаточно гибкая, мы смогли на порядок увеличить оперативность принятия решений при предотвращении инцидентов в сфере информационной безопасности. Наше аналитическое подразделение высоко оценило открывающиеся возможности для работы служб внутреннего контроля и внутренней безопасности. За прошедшее с момента запуска системы время, используя полученную информацию, мы смогли выявить и снизить риски несанкционированного доступа к конфиденциальной информации. Таким образом, мы получили реальную отдачу от работы системы»

К. Щепилов

главный специалист отдела информационной безопасности
департамента информационного обеспечения
Дальневосточного филиала «МТС-Банка»

Система «Гарда БД»

Внедрение специализированной защиты баз данных «Гарда БД» повышает возможности для противостояния инсайдерам и внешним атакам на базы данных.

Система контролирует абсолютно все события, происходящие с базами данных вплоть до обращения к отдельным полям таблиц. «Гарда БД» проводит мониторинг обращений к базам данных в режиме реального времени. При обнаружении подозрительных операций с базами данных (нехарактерные действия, массовое изменение или удаление данных и т.п.) система оповещает администратора и протоколирует запрос.

Система «Гарда БД» обладает широкими возможностями гибкой настройки критериев анализа, включающими IP-адрес клиента, дату и время прохождения запроса к базе данных, регистрационное имя пользователя, SQL-команды, названия таблиц и полей и т.д. Решение способно детектировать, в том числе, и шифрованные соединения, осуществлять поиск и перехват инцидентов по ключевым словам в запросах и ответах. Функционал мониторинга действий пользователей, осуществляющих соединения с базами данных через web-интерфейс по протоколу http особенно востребован у компаний, обслуживающих клиентов через Интернет (пользователи интернет-банков, личных кабинетов и т.п.).

В системе «Гарда БД» реализованы различные виды визуализации графических отчетов и возможность формирования списка критериев по уже заданным в контролируемых базах данных параметрам, а также механизм циклической перезаписи данных, обеспечивающий автономную работоспособность комплекса без вмешательства администратора системы.

Решение «Гарда БД» устанавливается параллельным способом, не нарушая топологии сети и не оказывая влияния на производительность СУБД. Внедрение системы занимает всего три дня.

Решение соответствует требованиям законодательства и отраслевых стандартов (152-ФЗ, 161-ФЗ, 781-ФЗ, 382-П, PCI DSS, Basel II, SOX и пр.)

Защита баз данных в банке — Проблемы и решения.

МФИСОФТ

Аналитический центр
ООО «МФИ Софт»
2013 год.

www.mfisoft.ru