Технологическая концепция

McAfee
An Intel Company

ЗАЩИТА БАЗ ДАННЫХ

Повышение эффективности защиты от атак и угроз утечки данных

ЭТАЛОННАЯ АРХИТЕКТУРА SECURITY CONNECTED

УРОВЕНЬ 1 2 **3** 4 5

Security Connected

Разработанный компанией McAfee подход Security Connected позволяет интегрировать друг с другом большое количество разных продуктов, услуг и партнерских отношений, создавая возможность централизованно, эффективно и надежно снижать уровень риска. Основанный на мерах безопасности, проверенных на практике на протяжении более двадцати лет, подход Security Connected позволяет организациям любого размера, в любом регионе мира и в любой отрасли повысить свой уровень безопасности, оптимизировать систему защиты, снижая расходы на нее, и выполнить стратегическую интеграцию системы безопасности и бизнес-процессов организации. В эталонной архитектуре McAfee Security Connected предлагаются конкретные шаги от идей до их воплощения. С их помощью концепцию Security Connected можно адаптировать к конкретным рискам, инфраструктуре и коммерческим целям вашей организации. Компания McAfee непрерывно ведет поиск новых путей защиты своих клиентов.

Повышение эффективности защиты от атак и угроз утечки данных

Ситуация

В 2010 году число утечек данных достигло рекордно высокого уровня, причем в 47 процентах атак злоумышленникам потребовалось лишь пара часов, а то и минут, чтобы проникнуть в систему и получить доступ к данным. В 44 процентах случаев для этого потребовалось несколько дней, согласно данным опубликованного в 2011 году совместного отчета компании Verizon и Секретной службы США о расследовании утечек данных. Итак, преступники проникают в систему — причем быстро. А ответные действия часто оказывается запоздалыми. Время между взломом обороны и его обнаружением порой измерялось неделями (в 38 процентах случаев), а то и месяцами (в 36 процентах случаев).[1] Согласитесь, что у преступников остается масса времени, чтобы похитить желаемое и скрыться незамеченными.

Злоумышленники оперируют минутами и днями, в то время как для реакции на их действия часто требуются недели и даже месяцы. Как получается, что преступникам удается так быстро работать? Благодаря новым тактикам. Самые распространенные тактические приемы — действия хакеров (50 процентов случаев) и вредоносные программы (49 процентов). Кроме того, авторы отчета делают вывод о том, что злоумышленники выбирают «удобные» цели — небольшие организации с недостаточно защищенными системами, — а не пытаются «сорвать куш» на серверах, где число записей в базе данных исчисляется миллионами.

Порой невольными пособниками злоумышленников становятся сами сотрудники компании. Используя приемы социальной инженерии и похищенные учетные данные, преступники без труда находят способ выдать себя за сотрудников компании с разрешенным доступом к информации. Имея представление о ценности баз данных и, учитывая кризисное состояние современной экономики, они весьма успешно используют подкуп сотрудников. Согласно тому же отчету, подстрекательство и подкуп были самыми распространенными методами социальной инженерии в прошлом году. Таким образом, нельзя полностью доверить безопасность своей базы данных средствам защиты периметра и нельзя полностью полагаться на добросовестность всех своих сотрудников.

Описание проблемы

Базы данных не только содержат критически важную информацию, но и зачастую подключены ко многим системам, обеспечивающим основные функции бизнеса. Любые перебои в работе, случайное разглашение конфиденциальных данных или потеря данных в базе могут нарушить ход работы всей компании и сказаться на ее репутации. Кроме того, поскольку в базе данных содержится конфиденциальная информация и данные, регулируемые нормативными актами, нарушение безопасности базы данных обычно приводит к нарушению нормативно-правового соответствия. Это влечет за собой огромные затраты на ликвидацию последствий, потерю доверия клиентов и, возможно, катастрофическое снижение рыночной капитализации предприятия.

Чтобы защитить конфиденциальные данные от внешних и внутренних угроз, необходим визуальный контроль активности базы данных в режиме реального времени. Для обеспечения такой защиты многие компании в настоящее время используют средства журналирования и аудита, встроенные в СУБД, но и эти средства не могут адекватно противостоять современным тактическим приемам хакеров и злоумышленников, промышляющих приемами социальной инженерии. Для того чтобы надежно защитить базу данных от вредоносного кода и утечки данных, необходимо обратить внимание на следующие аспекты:

- **Мониторинг активности и изменений**. Все базы данных реагируют на команды. Если команда соответствует роли пользователя, пославшего запрос на получение данных из БД, то команда будет выполнена. Поскольку атаки и инструменты злоумышленников постоянно усложняются, преступники могут оставаться невидимыми для стандартных средств обнаружения и способны повышать свои права в системе. Неэффективные средства контроля доступа облегчают задачу злоумышленников. Обычно уровень доступа, предоставляемый пользователям, существенно шире набора прав, необходимых им в системе в соответствии с их ролью. Неиспользуемые учетные записи и слабый контроль за созданием новых учетных записей создают новые лазейки для преступников. Обычно они сначала производят атаку с подбором ненадежных паролей и паролей по умолчанию, а затем повышают свои права в системе. Доказано, что мониторинг сетевой активности неэффективен против подобных угроз, так как при локальном доступе есть возможность обойти сетевые системы мониторинга.

- **Средства аудита**. 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. Кроме того, встроенные средства журналирования и аудита способны снизить производительность базы данных. Они предназначены для мониторинга, а не для обеспечения безопасности, поэтому администраторы могут отключать эти функции вовсе, лишив их всякой ценности, которую могут представлять встроенные инструменты.
- **Предотвращение простоев, вызванных установкой исправлений**. Желание обеспечить прибыль, высокую доступность и бесперебойную работу нередко берет верх над соображениями безопасности. В ряде организаций установка пакетов исправлений выполняется реже одного раза в год. Каждый год появляются сотни новых угроз, однако, учитывая исключительную важность баз данных, их остановка едва ли может рассматриваться как возможное решение проблемы. Организациям хочется иметь постоянную защиту, не прибегая к установке пакетов исправлений СУБД.
- **Совместимость с «облачными» системами**. Учитывая, что организации начинают применять «облачные» решения, базы данных должны быть адаптированы для доступа и мониторинга не только через локальную сеть, но и используя «облачные» службы.
- **Подтверждение соответствия отраслевым, государственным и внутренним стандартам**. В зависимости от функции вашей базы данных вы должны соблюдать требования нормативно-правовых актов, отчитываться о соответствии им и поддерживать соответствующие политики. В число таких нормативных актов входят стандарт PCI DSS, закон Сарбейнса-Оксли, Закон о передаче и защите данных учреждений здравоохранения (HIPAA), положение о стандарте аудита (SAS-70), закон Грэмма-Лича-Блайли (GLBA) и Акт о праве на семейное образование и неприкосновенность частной жизни (FERPA). Если ваша компания ведет деловую активность в других странах, то следует принимать во внимание, что другие государства предъявляют аналогичные требования к защите конфиденциальности и обеспечению финансового контроля. Помимо названных, ваша организация может разработать собственные методы и стандарты работы. Руководство вашей компании хочет получать информацию о состоянии соответствия нормативно-правовым требованиям на панели мониторинга.

Факторы, влияющие на принятие решений

Ответы на следующие вопросы могут быть важны при построении архитектуры:

- Какие нормативно-правовые требования должна соблюдать ваша организация?
- Как измеряется степень нормативно-правового соответствия базы данных и как формируются отчеты об этом?
- Работают ли ваши базы данных в 64-разрядных операционных системах? Если да, то в каких именно?
- Известен ли вам уровень защищенности ваших баз данных?
- Как часто устанавливаются обновления для ваших СУБД?

Описание решения

Работа любой организации базируется на использовании базы данных. Если мы не полагаемся на то, что производители операционных систем могут обеспечить защиту своих ОС, то почему мы соглашаемся доверить защиту своих самых ценных информационных активов инструментам, выпускаемым производителями СУБД? Зная, что каждая база данных имеет весьма специфические проблемы, мы при этом возлагаем обязанности по применению политик безопасности и обеспечению нормативно-правового соответствия на администраторов баз данных. Заголовки различных изданий пестрят сообщениями о взломанных базах данных, и поэтому мы должны применить новый подход, способный обеспечить защиту всего комплекса баз данных от вредоносного кода — и как это не печально — от действий собственных сотрудников, пользующихся доверием компании.

Для противодействия этим угрозам решение должно отвечать следующим требованиям.

- **Мониторинг активности и изменений**. Решение должно обеспечивать мониторинг всей активности базы данных с точки, находящейся за пределами базы данных. Если такой мониторинг будет выполняться изнутри базы данных, у администраторов всегда будет возможность его отключить — случайно или умышленно. Решение должно уметь прекращать сеанс работы, идущий вразрез с политикой безопасности, направлять оповещения на консоль централизованного управления, а также помещать в карантин пользователей, действия которых являются злоумышленными или нарушают нормативно-правовые требования. Решение должно уметь обнаруживать способы обхода системы безопасности и не допускать их применения.
- **Средства аудита**. Средства аудита тоже не эффективны, если администратор может их отключить. Решение должно иметь функции защищенного аудита и журналирования, внешние по отношению к базе данных, что гарантирует фиксацию записей и их доступность для анализа. При компьютерно-технической экспертизе после инцидента безопасности такой журнал регистрации событий поможет оценить объем похищенных данных и лучше разобраться в характере вредоносной деятельности. Решение должно быть способно формировать журнал регистрации событий и отчеты в соответствии с требованиям SOX, PCI и других актов, регламентирующих процедуру аудита.
- **Предотвращение простоев, вызванных установкой исправлений**. Решение должно обнаруживать атаки с использованием известных уязвимостей, а также определять вероятные пути распространения угроз. При обнаружении атак следует сформировать оповещение либо автоматически прервать сеанс работы. Вы ожидаете, пока производитель СУБД выпустит пакет исправлений? Вы пропустили очередную установку пакетов исправлений? Вы хотите избежать спада производительности? Тем временем ваши базы данных остаются уязвимыми ко многим угрозам. Технология виртуальных исправлений способна обеспечить защиту от последних уязвимостей и уязвимостей «нулевого дня». Использование этой технологии позволяет избежать простоев баз данных и защитить конфиденциальные данные до наступления удобного момента для установки исправлений.

- **Совместимость с «облачными» системами**. Анализ сетевого трафика для выявления нарушений политик является либо невозможным, либо неэффективным в высокодинамичных и распределенных структурах, используемых для виртуализации центров обработки данных и «облачных» вычислений. Необходимо сконфигурировать решение таким образом, чтобы оно могло автоматически защищать каждую новую базу данных, запрашивать политику безопасности на основе хранимых данных и затем направлять оповещения на сервер управления. Даже в случае обрыва сетевого соединения данные находятся под защитой благодаря применяемым локально политикам безопасности.
- **Соответствие отраслевым, государственным и внутренним стандартам**. Внесение изменений в действующие стандарты и нормативные акты должно сопровождаться внесением соответствующих изменений в отчетность организаций. Решение должно обеспечивать соответствие нормативно-правовым требованиям и предоставлять шаблоны отчетов, которые должны обновляться согласно новым директивам в области средств управления и пресечения нарушений. Решение должно обнаруживать угрозы по мере их возникновения и создавать отчеты об их нейтрализации, снижая тем самым уровень риска и степень юридической ответственности. Комплект шаблонов должен включать отчеты о соответствии с требованиями стандарта PCI DSS, закона Сарбейнса-Оксли, Закона о передаче и защите данных учреждений здравоохранения (HIPAA), положения о стандарте аудита (SAS-70), которые можно просматривать из централизованно управляемой платформы.

Технологии, использованные в решении McAfee

McAfee предлагает два продукта, специально разработанных для обеспечения защиты баз данных, — McAfee® Vulnerability Manager for Databases и McAfee Database Activity Monitoring. Благодаря централизованному управлению с помощью McAfee ePolicy Orchestrator® (McAfee ePO™) эти два решения объединены в комплексную платформу для управления системой безопасности и соответствия нормативно-правовым требованиям всей инфраструктуры вашей компании.

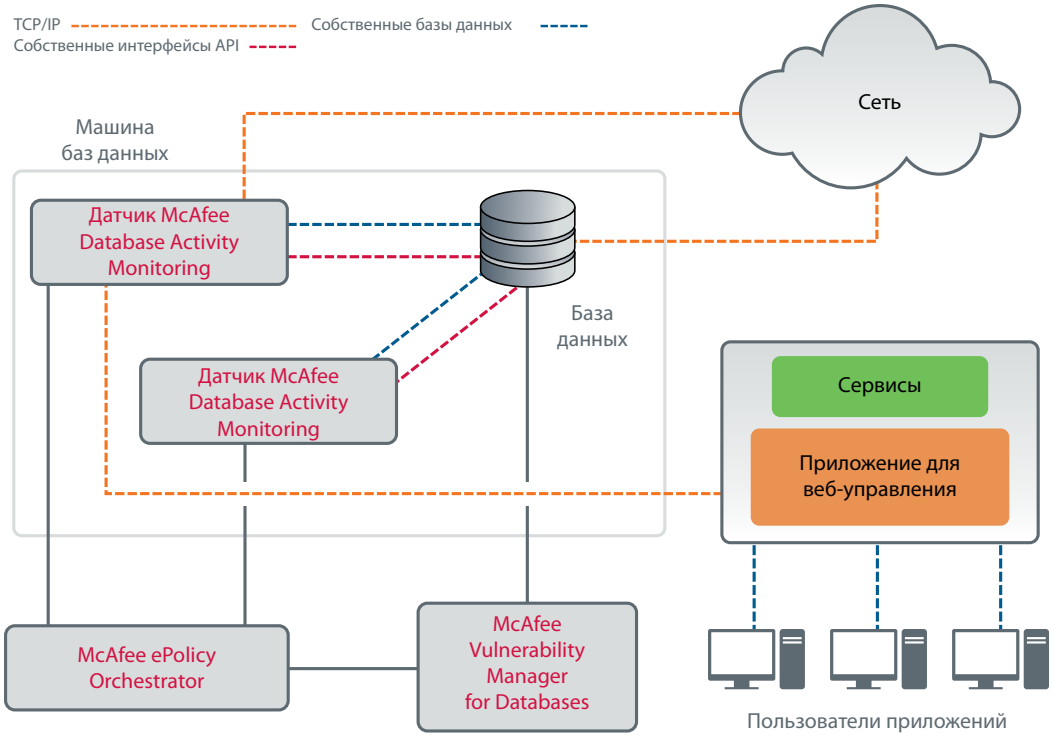
Программный продукт McAfee Vulnerability Manager for Databases проводит свыше 3 000 проверок на наличие уязвимостей в базах данных всех распространенных типов, включая Microsoft SQL Server, IBM DB2 и MySQL. За счет улучшенного визуального контроля уязвимостей баз данных и составления экспертных рекомендаций по исправлению Vulnerability Manager for Databases снижает вероятность возникновения опасных брешей и экономит деньги, позволяя лучше подготовиться к аудитам для оценки соответствия нормативно-правовым требованиям. Vulnerability Manager for Databases помогает уменьшить количество возможных направлений атак, выявляя типичные уязвимости, которыми может воспользоваться злоумышленник, например ненадежные пароли, общие пароли и учетные записи по умолчанию. Помогая вам отследить подозрительные события и отреагировать на них, решение сообщит об используемой версии и уровне исправлений, измененных объектах и правах, а также об обнаруженных следах использования распространенных хакерских инструментов.

В отличие от базового аудита или анализа журналов событий, которые всего лишь сообщают о событиях постфактум, McAfee Database Activity Monitoring позволяет осуществлять визуальный контроль и предотвращать вторжения в реальном времени с целью блокировки нарушения до нанесения ущерба. Более 380 предустановленных правил позволяют решить конкретные проблемы, учтенные в пакетах исправлений поставщиков баз данных, а также противодействовать распространенным сценариям атак. Пользовательская настройка встроенных шаблонов политик поддерживает правила надлежащего и соответствующего нормативно-правовым требованиями доступа к базам данных и процессам баз данных.

Оповещения, включающие всю информацию о нарушении политик, направляются непосредственно на панель мониторинга для решения выявленных проблем безопасности. Для обнаружения чрезвычайно опасных нарушений продукт может быть настроен на автоматическое прекращение подозрительных сеансов и помещение злоумышленников в карантин, что даст группе, осуществляющей защиту, время на расследование вторжения.

Атаки, направленные на ценные данные, хранящиеся в базах данных, могут исходить из сети, от локальных пользователей, зарегистрированных на самом сервере, и даже изнутри самой базы данных через хранимые процедуры или триггеры.

McAfee Database Activity Monitoring использует датчики, расположенные в оперативной памяти, для мониторинга активности и улавливания всех трех типов угроз с помощью единого комплексного и неинтрузивного решения. Виртуальные обновления для недавно обнаруженных уязвимостей предоставляются регулярно и могут быть реализованы без простоев базы данных, что обеспечивает защиту конфиденциальных данных до выпуска обновления поставщиком базы данных и установки обновления. Затем эта информация об активности и событиях может быть использована для подтверждения соответствия нормативно-правовым требованиям при проведении аудитов и для повышения общего уровня системы безопасности.



Специализированные средства защиты позволяют решению McAfee выполнять оценку уязвимостей баз данных и мониторинг злоумышленных и подозрительных действий.

McAfee Vulnerability Manager for Databases

Программный продукт McAfee Vulnerability Manager for Databases, предназначенный для ускорения начального сканирования и формирования стандартных отчетов о соответствии большинству нормативно-правовых требований, способен обнаруживать и сканировать многочисленные базы данных с единой консоли. Решение определяет местоположение и выявляет таблицы, содержащие конфиденциальную информацию, а также выполняет быстрое сканирование портов, предоставляя информацию о версии базы данных и состоянии исправлений. Помимо определения обычной надежности пароля (простых паролей, паролей по умолчанию или общих паролей) решение может выполнять проверку паролей, хэшированных с использованием таких алгоритмов, как, например, SHA-1, MD5 и DES. Решение также выявляет восприимчивость к типичным рискам баз данных, включая внедрение SQL-кода, переполнение буфера, вредоносный или незащищенный PL/SQL код, и представляет результаты в форме отчетов с заранее заданной конфигурацией для распространенных стандартов соответствия нормам.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring — нетребовательный к ресурсам датчик. Устанавливается на основном сервере базы данных как программный агент и отслеживает всю активность базы данных. Датчик — это самостоятельная программа, написанная на C++ и запускаемая хост-машине (компьютере сервера) базы данных. Датчик устанавливается с использованием стандартных для данной платформы средств (RPM, PKG, DEPOT, BFF или EXE) в отдельную учетную запись операционной системы. Он автоматически обнаруживает все экземпляры баз данных на хост-машине и способен выполнять одновременный мониторинг нескольких экземпляров, в том числе баз данных разных типов.

При работе датчик использует доступ только для чтения и прикладные программные интерфейсы (API) для прикрепления к области памяти кэша SQL, выделенной для экземпляра базы данных, после чего начинается мониторинг активности путем цикличного опроса области памяти. В каждом цикле опроса для каждого сеанса работы с базой датчик производит анализ текущих и предыдущих инструкций. На основании предварительно заданных политик, полученных с сервера, датчик определяет, какие инструкции следует заблокировать, а о каких сформировать оповещение. Инструкции, не соответствующие политикам, передаются на консоль управления в виде оповещений в режиме реального времени. Можно также настроить датчик на прекращение сеансов работы при определенных нарушениях и помещение пользователей в карантин. Датчик является неинтрузивным решением и использует небольшую долю ресурсов процессора (менее пяти процентов загрузки одного ядра даже на многопроцессорных конфигурациях). Функции предотвращения нарушений датчика используют собственные интерфейсы прикладного программирования (API) СУБД, что позволяет датчику прекращать сеансы при работе с базой данных без малейшего риска для целостности данных.

McAfee ePolicy Orchestrator (McAfee ePO)

Решение McAfee ePO предназначено для централизованного автоматического распространения программ и управления политиками. Решение McAfee Vulnerability Manager for Databases интегрировано с панелью мониторинга McAfee ePO, что обеспечивает централизованное формирование отчетов и сводную информацию для всех ваших баз данных. Кроме того, McAfee ePO подключается к решению McAfee Database Activity Monitoring, предоставляя оптимизированную отчетность и обзор системы в едином «окне».

Результаты внедрения решения

Внедрение специализированной защиты от атак на базы данных и утечки данных повышает возможности для обнаружения внешних атак и успешного противодействия им, а также снижает вероятность взлома и нарушения работы баз данных изнутри сети.

Выполняя мониторинг и создавая оповещения о подозрительных событиях, решения McAfee обеспечивают визуальный контроль и защиту от всех источников атак в режиме реального времени. Независимо от того, исходит ли угроза из сети, от локальных пользователей, зарегистрированных на самом сервере, или изнутри базы данных, McAfee помогает снизить уровень риска и уменьшить объем юридической ответственности благодаря пресечению атак до причинения ими ущерба. Технология виртуальных исправлений недавно обнаруженных уязвимостей баз данных обеспечивает моментальную защиту и может быть применена без простоев баз данных.

Предустановленные шаблоны и правила, автоматизированные и обновляемые проверки, а также интерфейсы в виде мастеров ускоряют развертывание и помогают построить эффективную архитектуру обеспечения безопасности, позволяющую легко выполнить аудит баз данных.

Дополнительные ресурсы

www.mcafee.com/ru/solutions/database-security/database-security.aspx
www.mcafee.com/ru/products/vulnerability-manager-databases.aspx
www.mcafee.com/ru/products/database-activity-monitoring.aspx
www.mcafee.com/ru/products/epolicy-orchestrator.aspx

Дополнительную информацию об эталонной архитектуре McAfee Security Connected можно получить, посетив страницу www.mcafee.com/ru/enterprise/reference-architecture/index.aspx.

Об авторе

Уй Хьюн (Uy Huynh) — старший директор отдела технического обеспечения сбыта компании McAfee. В его обязанности входит руководство отделом, задача которого состоит в разработке необходимых решений, проектов и рекомендаций в области обеспечения защиты, призванных помочь клиентам улучшить состояние безопасности и защитить их наиболее важные цифровые активы. Эксперт в области безопасности, он работал с крупными компаниями из списка Fortune 100, в том числе с HP, Oracle, ATT, McKesson, помогая им выбрать системы обеспечения безопасности, отвечающие их непростым требованиям.

До прихода в McAfee создал и возглавил подразделение технического обеспечения сбыта в компании Foundstone. На этой должности разработал рекомендации по управлению уязвимостями и рисками для крупных сетей и систем. Еще ранее работал старшим консультантом компании ISS, занимаясь внедрением защитных решений, политик и технологий в крупных организациях.

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

38600bp_protecting-databases-L3_1111