Возможности устройств Imperva SecureSphere по мониторингу и защите СУБД

Любая современная СУБД представляет собой потенциальный объект воздействия огромного числа угроз, к наиболее опасным из которых можно отнести следующие:

- злоупотребление чрезмерными привилегиями доступа (Excessive Privilege Abuse);
- злоупотребление легитимными привилегиями доступа (Legitimate Privilege Abuse)
- превышение привилегий доступа (Privilege Elevation);
- уязвимости программного обеспечения СУБД (Database Platform Vulnerabilities)
- атаки типа SQL Injection;
- слабый аудит (Weak Audit Trail);
- отказ в обслуживании (Denial of Service);
- уязвимости протоколов баз данных (Database Communication Protocol Vulnerabilities);
- слабые механизмы аутентификации (Weak Authentication).

Принятие эффективных мер, направленных на защиту СУБД от вышеперечисленных угроз, позволяет снизить информационные риски и реализовать на практике требования стандартов информационной безопасности.

Злоупотребление чрезмерными привилегиями доступа (Excessive Privilege Abuse)

Такая угроза возникает в том случае, если пользователям (или приложениям) предоставлены привилегия доступа к базам данных, превышающие их должностные обязанности. К примеру, администратор кампусной сети, в обязанности которого входит изменение контактной информации о студентах, может воспользоваться своими привилегиями доступа для изменения данных по успеваемости.

Превентивной мерой борьбы с данной угрозой является реализация контроля доступа на уровне запросов к базе данных. Данный механизм ограничивает привилегии доступа - позволяет пользователям осуществлять минимально необходимый набор SQL-запросов (SELECT, UPDATE и др.) и только к определенным данным (колонкам и столбцам таблиц баз данных). Совершенный механизм повсеместного контроля доступа позволит администратору кампусной сети обновить контактную информацию и оповестит службу безопасности при попытке внесения изменений данных по успеваемости. Контроль доступа на уровне запросов полезен не только для выявления злоупотреблений чрезмерными полномочиями, но и для блокирования других опасных угроз, описанных ниже.

Большинство СУБД имеют встроенные средства контроля запросов пользователей (триггеры, блокировки на уровне строк таблиц и др.), которые, в виду отсутствия автоматических механизмов выработки политики запросов, ограничены в применении. Процесс выработки политики запросов пользователей к определенным строкам, колонкам таблиц баз данных и операциям над ними отнимает достаточно много времени. Проблема усугубляется еще и тем, что роли пользователей меняются со временем и политики доступа должны отражать эти изменения. Для многих администраторов задача оперативного создания политик на уровне запросов к базам данных является практически невыполнимой. В результате в компании появляется политика, которая предоставляет чрезмерные полномочия для большого числа пользователей**.** Выход из такой ситуации - использование автоматизированных средств выработки политики доступа.

Выпускаемые компанией Imperva устройства серии SecureSphere Database Security Gateway обладают автоматическим механизмом выработки и применения политик контроля доступа на уровне запросов пользователей. Технология динамического профилирования основана на алгоритмах автоматического обучения, позволяющих создавать профили для каждого пользователя и приложения, осуществляющих запросы к базе данных.

Каждый создаваемый профиль содержит информацию о конкретных запросах и процедурах, которые когда-либо выполнялись пользователем. Устройства SecureSphere в режиме обучения непрерывно обновляют профили пользователей, исключая необходимость ручной настройки.

В том случае, если действия пользователя выходят за рамки его профиля, устройство SecureSphere фиксирует это во внутреннем журнале, выдает оповещение и опционально блокирует действия пользователя (в зависимости от степени их опасности). Система SecureSphere достаточно быстро выявит неавторизованные действия системного администратора кампусной сети, профиль которого включает набор запросов, отражающих модификацию контактной информации о студентах и чтение данных по их успеваемости. Все попытки системного администратора по внесению изменений данных по успеваемости вызовут сигнал оповещения.

Злоупотребление легитимными привилегиями доступа (Legitimate Privilege Abuse)

Существует риск злоупотребления пользователями легитимно предоставленных им привилегий доступа. Например, служащий медицинского центра с легитимными привилегиями доступа имеет возможность просмотра ограниченного числа записей баз данных пациентов посредством интерфейса Web-приложения. Структура интерфейса Web-приложения не позволяет осуществлять просмотр истории болезни пациентов, ограничивает возможность просмотра множества записей одновременно и копирование информации на электронные носители. Однако служащий может обойти эти ограничения путем подключения к базе данных с помощью альтернативного клиентского приложения, например MS-Excel. Используя MS-Excel, свои логин и пароль доступа, он может реализовать свои корыстные цели.

Для предотвращения злоупотреблений легитимными полномочиями служат механизмы контроля доступа к базам данных уровне запросов (рассмотрены выше) и на уровне контекста. Идентификация подозрительных действий легитимных пользователей может

быть осуществлена с помощью правил (политик), контролирующих тип используемых клиентских приложений, время суток, местоположение и другие параметры.

В дополнение к информации о конкретных запросах и процедурах, технология динамического профилирования позволяет создавать контекстную модель нормального взаимодействия пользователя с базой данных.

Специфическая контекстная информация, сохраняемая в профиле, включает время суток, ip-адрес источника, объем полученных пользователем данных, тип клиентского приложения и другие параметры.

Любые подключения к базе данных, контекст которых не согласован с информацией, хранимой в пользовательском профиле, активируют сигнал тревоги. Злоумышленник может быть легко обнаружен системой SecureSphere благодаря нестандартному использованию клиента MX-Excel и значительному объему информации, который был им получен в рамках одной сессии. Кроме того, девиации в структуре нестандартных запросов с помощью клиента MX-Excel могут так же активизировать сигнал оповещения (см. раздел “Злоупотребление чрезмерными привилегиями доступа”)

Превышение привилегий доступа (Privilege Elevation)

Злоумышленники могут использовать уязвимости в СУБД в целях получения административных привилегий доступа к ним. Например, программист банка, получивший незаконным способом административные привилегии, может деактивировать механизмы аудита, создать фальшивые учетные записи, осуществлять перевод денежных средств и др.

Инциденты, связанные с превышениями привилегий доступа, могут быть предотвращены путем комбинированного использования традиционных систем предотвращения вторжений (IPS) и специализированных средств, обеспечивающих контроль доступа к базе данных на уровне запросов (см. выше). Системы IPS инспектируют трафик баз данных, используя сигнатурный метод обнаружения. Например, если определенная функция СУБД имеет уязвимость, то система IPS может, либо полностью заблокировать все запросы к ней, либо (если это возможно) – только вредоносные.

Обнаружение вредоносных запросов к базам данных является, как правило, трудновыполнимой задачей с помощью традиционных IPS. В связи с тем, что многие функции СУБД, имеющие уязвимости, широко используются для легитимных целей, их полное блокирование нежелательно. Богатые возможности языка SQL позволяют формировать огромное количество вариаций запросов, что еще больше затрудняет задачу традиционным системам IPS, которые по этой причине зачастую применяются лишь в режиме оповещения, а не блокирования угрозы.

В том случае, если системы IPS используются совместно со средствами контроля доступа на уровне запросов, то задача первых – проверка попыток запроса к потенциально уязвимым функциям, а вторых – выявление фактов отклонений поведения пользователя от зафиксированного в его профиле. Если данная интегрированная система выявляет запрос на доступ к потенциально уязвимой функции и одновременно отклонения в поведении пользователя, то такое действие рассматривается как атака.

Системы SecureSphere обладают возможностями как традиционных IPS, так и средствами контроля доступа на уровне запросов – в частности функцией динамического профилирования, что позволяет им достаточно эффективно решать задачу предотвращения инцидентов, связанных с превышением привилегий доступа.

Функционал IPS устройств SecureSphere обеспечивает защиту от известных атак с помощью сигнатурного метода (сигнатуры, формат которых совместим с форматом сигнатур популярной системы Snort). Сигнатуры разрабатываются и автоматически обновляются на еженедельной основе специалистами центра ADC (Application Defense Center) компании. Подсистема IPS устройств SecureSphere однозначно блокирует запросы, идентифицируемые ею как вредоносные без необходимости какого-либо подтверждения. Все запросы, идентифицируемые как подозрительные, коррелируются устройством SecureSphere с информацией, которая хранится в профиле.

Если, например, программист банка пытается использовать уязвимость переполнения буфера СУБД для того, чтобы встроить вредоносный код и в результате этого действия получить административные привилегии, то устройство SecureSphere будет идентифицировать два события. Первое – любой запрос, который пытается получить доступ к функции с известными уязвимостями, генерирует сигнал тревоги. Второе – необычный запрос генерирует сигнал тревоги в результате отклонения от профиля. Корреляция двух событий, связанных с одним и тем же запросом от данного пользователя, позволяет однозначно идентифицировать атаку и применить соответствующие меры (оповещение или блокирование).

Уязвимости в программном обеспечении

Уязвимости в операционных системах (Windows, Unix и др.), под управлением которых функционируют базы данных, и в дополнительных установленных сетевых сервисах могут привести к возможности неавторизованного доступа, к потерям данных или к отказам в обслуживании.

Периодичность установки обновлений программного обеспечения (патчей) зависит как от оперативности производителя, так и расторопности системного администратора. В интервалах между обновлениями задача защиты возлагается на системы IPS, которые очень часто не в состоянии обнаружить принципиально новые атаки.

Устройства SecureSphere обладают возможностями традиционных систем IPS для защиты от угроз на программное обеспечение баз данных – вредоносного кода (черви, трояны и др.). Центр ADS разрабатывает и предоставляет на основе подписки еженедельные обновления уязвимостей, некоторые из них даже не фиксируются самими производителями СУБД.

Атаки типа SQL Injection

Злоумышленник, совершая атаку SQL Injection, вставляет неавторизованные команды в строки запросов к серверу баз данных. Выполнение таких команд сервером приводит к тому, что злоумышленник получает неограниченный доступ к базе данных.

На сегодняшний день существуют, по крайней мере, три технологии для борьбы с атаками типа SQL Injection: сигнатурный метод систем IPS, контроль доступа на уровне запросов и корреляционный анализ. Системы IPS могут идентифицировать уязвимые процедуры и строки запросов с неавторизованными SQL командами. Однако в силу того, что существует огромное число вариаций таких запросов, системы IPS не могут гарантировать высокую эффективность обнаружения реальной атаки. Точность обнаружения атаки SQL Injection можно повысить путем корреляции информации, полученной от IPS и системы контроля доступа на уровне запросов.

Устройства SecureSphere обладают функциями динамического профилирования, механизмами сигнатурного и корреляционного анализа (Correlated Attack Validation) для высокоточной идентификации атак SQL Injection:

- Динамическое профилирование позволяет осуществить контроль к базам данных на уровне запросов путем создания профилей для каждого пользователя/приложения;
- IPS включает уникальные сигнатуры, разработанные специально для идентификации уязвимостей хранимых процедур и SQL запросов;
- С помощью технологии Correlated Attack Validation осуществляется корреляция данных, полученных с помощью различных механизмов устройств SecureSphere.

Рассмотрим пример атаки на хранимую процедуру:
exec ctxsys.driload.validate_stmt ('grant dba to scott') .

Злоумышленник (scott), запускающий данную атаку, пытается получить административные привилегии к СУБД с помощью команды grant. Устройство SecureSphere от условия: применяется ли данная хранимая процедура при обращениях пользователей к СУБД или нет.

В случае если данная хранимая процедура не применяется при обращениях пользователей к СУБД, то подсистема IPS устройств SecureSphere с высокой степенью точности идентифицирует и опционально блокирует атаку.

Если данная хранимая процедура применяется при обращениях пользователей к СУБД (например, она может быть частью программного приложения, внесение изменений в которое не представляется возможным), то устройство SecureSphere сперва оповестит администратора безопасности и затем опционально задействует механизм Correlated Attack Validation. Этот механизм позволяет сопоставить все события, вызванные данной сигнатурой, со списком пользователей или программных приложений, которые авторизованы для запуска данной процедуры. В случае любых попыток неавторизованного запуска данной процедуры, SecureSphere сгенерирует тревогу и опционально заблокирует запрос.

Слабый аудит

При развертывании СУБД следует учитывать возможность автоматической записи всех критических и/или подозрительных запросов к базам данных. Наличие эффективной политики аудита позволяет решить следующие задачи:

Реализация требований стандартов безопасности – наличие мощных механизмов аудита позволят компаниям выполнить требования международных стандартов безопасности SOX, HIPAA, PCI и др.

Сдерживание - наличие мощных механизмов аудита позволят удержать злоумышленников от совершения компьютерных преступлений.

Обнаружение нарушений и принятие мер к восстановлению данных – мощные механизмы аудита позволят выявить случаи проникновения злоумышленников и своевременно принять меры к восстановлению данных.

В настоящее время задачи аудита в основном возлагаются на встроенные в СУБД средства аудита, которые имеют следующие недостатки:

- они не могут идентифицировать пользователей, осуществляющих запросы к базам данных посредством WEB-приложений (SAP, Oracle E-Business Suit, PeopleSoft). В таких случаях пользовательская активность ассоциируется с учетной записью WEB-приложения, а не с именем конкретного пользователя;
- они сильно задействуют ресурсы центрального процессора, оперативной памяти и жесткого диска, что влечет к снижению производительности СУБД в целом;
- пользователи с административным доступом к базе данных (полученным легитимно или в результате вредоносных действий) обладают возможностью деактивировать встроенные механизмы аудита с целью скрыть вредоносные действия. Нарушается принцип разделения административных и аудиторских полномочий;
- они не осуществляют детальную запись событий, необходимую для идентификации атаки, анализа и восстановления последовательности событий. Например, не учитываются тип клиентского приложения, ip-адрес источника запросов, атрибуты запросов, неудачные попытки запросов.
- к сожалению, каждая СУБД имеет уникальный механизм аудита: например, форматы журналов событий для Oracle и MS-SQL отличаются друг от друга. Если в организации используются несколько типов СУБД, то процесс анализа журналов событий достаточно трудоемкий.

Большинство недостатков встроенных средств аудита устраняется с помощью использования специализированных сетевых устройств, обладающих следующими достоинствами:

- *Высокая производительность* – сетевые устройства могут работать на скорости подключения к сети и не влиять на производительность СУБД. Фактически, возлагая задачи проведения аудита на специализированные сетевые устройства, компании повышают производительность СУБД;
- *Разделение полномочий* - специализированные сетевые устройства могут выполнять свои функции независимо от администраторов баз данных, позволяя реализовать на практике принцип разделения административных и аудиторских полномочий;
- *Независимость от типа СУБД* – сетевые устройства поддерживают наиболее популярные модели СУБД и позволяют стандартизировать и централизовать процесс проведения аудита.

Все вышеперечисленные возможности специализированных сетевых устройств позволяют снизить стоимость СУБД и затраты на администрирование, обойти требование балансировки нагрузки, повысить уровень безопасности.

Устройства SecureSphere обладают рядом уникальных возможностей по проведению аудита, которые позволяют выделять их среди альтернативных решений:

- Технология *Universal User Tracking* позволяет осуществлять аудит действий конкретных пользователей, даже если они осуществляют доступ посредством программных web-приложений (Oracle, SAP, PeopleSoft или пользовательских). Устройство определяет сетевое имя (логин) пользователя, под которым он работает с web-приложением, отслеживает все пользовательские http/https- сессии и коррелирует собранную информацию с SQL-запросами самого приложения к базе данных;
- Технология *Granular Transaction Tracking* предназначена для обнаружения попыток кражи информации, в целях проведения расследований и восстановления данных. Журналы событий обладают высокой степенью детализации и включают такие параметры как имена клиентских приложений, строки запросов к СУБД, атрибуты ответов сервера СУБД, типы операционных систем источников запросов и др. ;
- Технология *Distributed Audit Architecture* предоставляет возможность построения распределенной системы детализированного аудита центров обработки данных (ЦОД);
- Технология *External Data Archival* дает возможность автоматизированного архивирования данных аудита на внешних хранилищах. Данные могут быть предварительно сжаты, зашифрованы и скреплены цифровой подписью;
- Встроенный *генератор отчетов* позволяет создавать графические отчеты различной формы с помощью имеющихся шаблонов, а так же пользовательские. Кроме того, анализ данных можно осуществлять с помощью любого ODBC совместимого программного приложения;
- Аудит локальной активности при помощи программного клиента *SecureSphere DBA Security Monitor* позволяет осуществлять мониторинг локальных запросов к СУБД.

Защита от DoS-атак

DoS-атаки нацелены на блокирование доступа пользователей к сетевым приложениям или данным. Злоумышленники, реализующие Dos-атаки, используют уязвимости СУБД с целью разрушение данных, перегрузки серверных ресурсов и др.

Возможности устройств SecureSphere по отражению DoS-атак включают:

- *Контроль соединений* служит для предотвращения серверных ресурсов от перегрузки путем ограничения скорости соединения каждого пользователей базы данных;
- *Сигнатурный анализ и анализ протоколов на аномалии* уменьшают шансы злоумышленников по использованию известные уязвимости СУБД для реализации DoS-атак;
- *Динамическое профилирование* позволяет в автоматическом режиме обнаружить неавторизованные запросы, которые могут вызвать отказы в обслуживании;

- *Контроль времени отклика* позволяет выявить задержки реакции СУБД на определенные запросы, которые могут быть ассоциированы с DoS-атаками.

Уязвимости протоколов СУБД

В настоящее время наблюдается рост уязвимостей в протоколах СУБД. Злоумышленники могут использовать эти уязвимости для неавторизованного доступа к данным, их разрушению и отказам в обслуживании.

Атаки на протоколы баз данных могут быть предотвращены с помощью технологии Protocol Validation . Суть данной технологии заключается в детальном анализе составляющих трафика и сравнении их с ожидаемыми значениями. В случае рассогласования подается сигнал оповещения.

В устройствах SecureSphere реализован эффективный механизм оценки протоколов путем сопоставления текущих значений параметров протоколов с их ожидаемыми значениями (сигнатурами). Сигнатуры протоколов для наиболее популярных баз данных Oracle, Microsoft и IBM разрабатываются и обновляются центром ADC.

Слабые механизмы аутентификации

Отсутствие сильных механизмов аутентификации дает возможность злоумышленникам получать идентификационные данные пользователей путем подбора логина/пароля (Brute Force атака), социальной инженерией или с помощью кражи.

К числу наиболее эффективных относятся двухфакторные методы аутентификации на базе токенов, сертификатов и биометрии. Однако присущие им высокая стоимость и сложность реализации вынуждают пользователей прибегать к более дешевым и, к сожалению, менее защищенным способам, одним из которых является парольная защита.

В целях достижения высокой масштабируемости и простоты использования механизмы строгой аутентификации следует интегрировать с инфраструктурой директорий.

Инфраструктура директорий позволяет использовать единые аутентификационные параметры (логин и пароль) для доступа к различным приложениям и базам данных, что еще больше повышает эффективность двухфакторных методов аутентификации в сравнении с парольной защитой.

Несмотря на высокую эффективность двухфакторных методов аутентификации, злоумышленники находят способы их взлома. Устройства SecureSphere успешно справляются с задачей обнаружения попыток неавторизованного доступа с помощью функции динамического профилирования, механизмов обнаружения неудачных попыток доступа (Failed Login Detection) и оценки эффективности механизмов аутентификации (Authentication Assessment).

С помощью функции динамического профилирования устройства SecureSphere отслеживают весь спектр пользовательских атрибутов, которые свидетельствуют о попытках неавторизованного доступа. К таким атрибутам относятся IP-адрес пользователя, имена пользовательского компьютера, тип операционной системы и наименование клиентского приложения. Например, злоумышленник, получивший

незаконным образом административные права, будет выявлен устройством SecureSphere по имени его хоста, типу операционной системы и IP-адресу, так как они не согласованы с профилем реального администратора.
В том случае, если злоумышленник завладеет компьютером реального администратора, то устройство SecureSphere способно выявить его с помощью следующих механизмов:

- *Обнаружение неавторизованных запросов (Unauthorized Query)* – как правило, активность злоумышленника идет вразрез с активностью пользователя. Злоумышленник может запрашивать данные из таблиц, к которым пользователь никогда не обращался, или выполнить операции (Update, Delete и др.), которые ни разу не запускались пользователем;
- *Отслеживание времени запросов* – злоумышленники, как правило, пытаются осуществить намеченные планы, завладев компьютерами пользователей, в нерабочие часы;
- Устройство SecureSphere подает сигнал оповещения, когда активность пользователей осуществляется за рамками их рабочего времени;
- Механизм Failed Login Detection устройств SecureSphere позволяет обнаруживать и опционально блокировать попытки ввода логина и пароля в целях предотвращения атак типа Brute Force;
- Устройства SecureSphere обладают встроенным механизмом оценивания политики парольной защиты: проверяется длина, наличие требуемых символов и интервалы смены пароля.