



Код безопасности
ГК «Информзащита»

TrustAccess – эффективная сертифицированная
защита серверов баз данных

Введение

Количество публикаций о случаях потери или кражи баз данных, содержащих персональные данные или иные данные ограниченного доступа, продолжает неуклонно расти. Согласно отчету по исследованию утечек информации за 2010 год, опубликованному командой Verizon Risk Team, 98% атак приходится на серверы¹. Сервер баз данных (сервер БД) является наиболее интересным для злоумышленников, поскольку именно на нем сосредоточены большие объемы важной информации (конфиденциальная информация, персональные данные и т.д.). Такой интерес обусловлен как все возрастающими объемами баз данных, клиентских приложений, СУБД, так и возросшей ролью информационных систем для бизнеса.

98% атак приходится на серверы

Несомненно, причина большинства утечек конфиденциальной информации кроется в действиях организованной преступности, однако и роль внутренних нарушителей (инсайдеров) в возникновении утечек также весьма значительна. По обнародованным компанией InfoWatch в первом полугодии 2010 года данным, в большинстве случаев «злоумышленником», виновным в утечке, является именно внутренний

нарушитель. Как правило, утечка конфиденциальной информации допускается сотрудниками организации, как в результате злоупотреблений, так и по причине халатности и ошибок.

В отчете Verizon Risk Team отмечается, что злоупотребление сотрудников полномочиями является одним из основных каналов утечки данных. При этом неавторизованный доступ при обращениях клиентских приложений к серверу БД составляет одну из основных уязвимостей сервера БД. Для защиты данных на серверах, в том числе от угрозы неавторизованного доступа, требуется построение комплексной системы защиты, включающей как технические средства, так и организационные меры. Достижение необходимого уровня защищенности невозможно без ряда простейших превентивных мер, таких как контроль неиспользуемых учетных записей, особенно уровня администратора, контроль привилегий пользователей. Однако все эти меры не обеспечат полноценной защиты баз данных, если не будет создан доверенный канал при обращениях приложений к серверу БД.

Распределенный межсетевой экран TrustAccess с функцией аутентификации сетевых соединений, разработанный компанией «Код Безопасности», позволит решить проблему неавторизованного доступа к серверу БД, а также создать защищенный канал при обращениях клиентских приложений к нему.

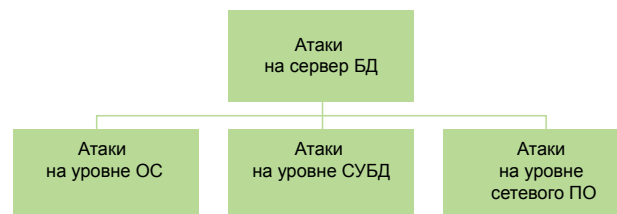
Защита сервера БД – на что следует обратить внимание?

Обзор основных угроз

Как правило, любые попытки взлома защиты компьютерных систем можно разделить на три группы:

- атаки на уровне систем управления базами данных (СУБД).
- атаки на уровне операционной системы (ОС);
- атаки на уровне сетевого программного обеспечения.

В большинстве случаев злоумышленники даже не пытаются атаковать СУБД, поскольку преодолеть защиту на уровнях операционной системы или сети гораздо проще. Тем не менее, в отдельных случаях преодоление защиты, реализуемой СУБД, вполне возможно. Например, успешная атака на СУБД возможна, если используется версия СУБД, защита



которой недостаточно надежна или же в случае допущения администратором БД грубых ошибок при определении политики безопасности. Следует отметить, что для реализации атаки на СУБД злоумышленник должен как минимум являться зарегистрированным пользователем СУБД.

1 2010 Data Breach Investigations Report (Verizon Risk Team)

Обычно для реализации атак на уровне операционной системы используются уязвимости конкретной операционной системы. К основным атакам, которым может быть подвергнута практически любая операционная система, можно отнести:

- кражу паролей пользователей;
- сборку «мусора»;
- сканирование жестких дисков компьютера с целью отыскать файлы, при описании прав доступа к которым администратор совершил ошибку и т.д.

Сетевое программное обеспечение является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен.

Наиболее актуальны для сервера БД атаки на уровне сети

Соответственно, любой, кто может иметь доступ к этому каналу, может перехватывать сообщения и отправлять свои собственные. На уровне сетевого ПО, как правило, используются такие атаки как:

- прослушивание сегмента локальной сети;
- перехват сообщений на маршрутизаторе;
- создание ложного маршрутизатора;
- навязывание сообщений;
- отказ в обслуживании и др.

На что же именно следует обратить особое внимание при обеспечении защиты сервера БД? Какие именно угрозы наиболее актуальны?

Для проведения атак на сервер БД на уровне операционной системы или СУБД злоумышленнику необходимо получить локальный или сетевой доступ к нему. Серверы с конфиденциальной информацией, как правило, располагаются в серверных помещениях и физический доступ посторонних лиц к ним ограничен. С другой стороны, в отсутствие сетевой защиты внутри локальной сети организации доступ к серверу БД может получить любой внутренний пользователь сети. Кроме того, даже в случае использования межсетевых экранов на границе сети, не исключена возможность атаки на сервер БД со стороны внешних злоумышленников. Традиционно внутренний периметр сети предприятия считается доверенной зоной и дополнительных мер по его защите, как правило, не предпринимается. С развитием современных технологий создание доверенного периметра уже не столь эффективно – злоумышленник может получить доступ внутрь корпоративной сети, например, по Wi-Fi, минуя маршрутизатор с системой защиты.

Поэтому при организации защиты наибольшее внимание следует уделить именно сетевой защите сервера БД.

Оценка эффективности основных защитных механизмов

Проанализируем, насколько могут быть эффективны для сервера БД механизмы защиты, которые обычно используются для сетевых соединений.

Механизм	Описание	Оценка эффективности
Изоляция сети от внешнего мира	Полная или частичная изоляция сервера БД от локальной сети и сети Интернет. Данный механизм является наиболее эффективным, но его применение не всегда возможно	Очевидно, что полностью изолировать сервер БД от локальной сети невозможно, поскольку сервер БД должен обрабатывать сетевые обращения клиентов информационной системы. С другой стороны, доступ к серверу БД для пользователей Интернет естественно должен быть заблокирован
Максимальное ограничение размеров компьютерной сети	Выделение в отдельный сегмент сети сервера БД и всех пользователей, которым разрешен доступ к нему. Суть данного механизма очевидна – чем меньше сеть, тем проще ее защитить.	Выделить в отдельный сегмент сети всех пользователей одной ИС не всегда просто технологически. Например, одному и тому же серверу БД могут иметь доступ не все сотрудники одного и того же отдела. Кроме того, такая мера не решит полностью проблему сетевых атак со стороны потенциальных злоумышленников
Шифрование сетевых сообщений	Шифрование всех сетевых пакетов, которыми обменивается сервер БД с клиентами ИС	Шифрование сетевых сообщений позволяет полностью устранить угрозу перехвата пакетов. С другой стороны, шифрование трафика несколько снижает производительность сети, что может стать критичным в случае получения данных из БД. Кроме того, средства криптографической защиты, реализующие функции шифрования, весьма сложны во внедрении и недешевы.
Электронная цифровая подпись сетевых сообщений	Удостоверение субъекта доступа с помощью электронной цифровой подписи	Применение ЭЦП позволяет полностью устранить угрозу навязывания пакетов и большинство угроз, связанных с отказом в обслуживании. Однако, для того, чтобы эта мера защиты принесла реальную пользу, необходимо, чтобы цифровая подпись пакета была обязательна и неподписанные пакеты игнорировались. В противном случае цифровая подпись защищает только от искажения легально отправленных пакетов, но не от навязывания пакетов. Обязательное применение цифровой подписи пакетов возможно только в том случае, когда программное обеспечение, необходимое для подписывания пакетов, установлено на каждом компьютере сети

Механизм	Описание	Оценка эффективности
Фильтрация сетевых соединений	Фильтрация передаваемых пакетов с помощью межсетевых экранов, с целью блокирования потенциально опасных пакетов, которые, возможно, были отправлены в ходе атаки сети злоумышленником	Применение межсетевых экранов является весьма эффективным механизмом защиты. Однако межсетевые экраны не всегда способны отличить потенциально опасный пакет от абсолютно безвредного. В результате при использовании межсетевых экранов случаются ситуации, когда межсетевой экран, с одной стороны, не защищает от некоторых атак, а, с другой стороны, препятствует нормальной работе сети

Применение межсетевых экранов – наиболее экономный и простой в реализации способ сетевой защиты сервера БД

Таким образом, организационные меры (изоляция сервера БД или ограничение размеров сети, к которой он подключен) при организации сетевой защиты сервера БД не всегда эффективны или вообще не применимы. Внедрение криптографических методов, таких как ЭЦП или шифрование, хотя и эффективно, но сопряжено со значительными техническими трудностями и финансовыми расходами. Применение межсетевого экрана – гораздо более экономный и простой способ.

Некоторые рекомендации

Если в организации принято решение защищать сервер БД с помощью межсетевого экрана – как выбрать наиболее оптимальный МЭ для защиты сервера БД?

Межсетевой экран, используемый для защиты сервера БД, должен обеспечивать его защиту от сетевых атак как извне, так и со стороны инсайдера.

Фильтрация сетевых соединений не гарантирует того, что несанкционированный доступ исключен – злоумышленник может получить доступ, используя разрешенные протоколы и порты. Аутентификация сетевых соединений позволит гарантировать, что соединение осуществляется не только по разрешенным протоколу и порту, но и со стороны легитимного пользователя.

При обеспечении защиты сервера БД не менее важна задача выполнения требований нормативно-правовой базы в области ИБ, в частности, ФЗ №152. Мало обеспечить эффективную защиту сервера БД, необходимо гарантировать легитимность этой защиты. Сертификация продукта в органах ФСТЭК является легитимным и наиболее безопасным способом выполнения требований Закона.

При настройке межсетевого экрана, в первую очередь, следует задать правила фильтрации оптимальным образом, заблокировав все порты, кроме используемых клиентскими приложениями при обращениях к серверу БД.

В таблице приведены рабочие порты, обычно используемые некоторыми СУБД:

Протокол	Номер порта	Назначение
TCP,UDP	118, 156	Сервисы SQL
TCP,UDP	1433	СУБД Microsoft SQL Server – Server
TCP,UDP	1434	СУБД Microsoft SQL Server – Monitor
TCP	1521	Oracle database default listener (неофициально)
TCP	1526	Oracle database common alternative for listener (неофициально)
TCP	2030	Oracle Services for Microsoft Transaction Server (неофициально)
TCP	2483	Oracle database listening for unsecure client connections to the listener
TCP	2484	Oracle database listening for SSL client connections to the listener
TCP,UDP	3306-3309	Система управления базами данных MySQL
TCP,UDP	3306	Система управления базами данных MS SQL (неофициально)
TCP	3872	Oracle Management Remote Agent (неофициально)
TCP,UDP	5432	PostgreSQL
TCP,UDP	5984	Сервер БД CouchDB

Защита сервера БД с помощью TrustAccess

Распределенный межсетевой экран высокого класса защиты TrustAccess с функцией аутентификации сетевых соединений является оптимальным средством для сертифицированной защиты сервера БД. TrustAccess обеспечит разграничение доступа к серверу БД и создание доверенного канала при обращениях клиентских приложений к серверу БД. Использование TrustAccess позволит обеспечить организации эффективную защиту сервера БД от большинства известных сетевых атак:

Сетевая атака	Защищает?
Man in the Middle	✓
Подмена защищаемого объекта	✓
Replay-атака	✓
IP-спуфинг	✓
Перехват сетевых пакетов	✓
Прослушивание сети	✓ ²
Подмена сетевых пакетов	✓
Отказ в обслуживании	✓

TrustAccess – это не только эффективное решение для защиты сервера БД от большинства сетевых атак, но и наиболее простой способ выполнения требований законодательства в области защиты персональных данных при обработке таковых на сервере БД. Продукт сертифицирован во ФСТЭК по уровню МЭ 2 и НДВ 4³, что позволяет использовать его для защиты информационных систем персональных данных до класса К1 включительно, а также для защиты автоматизированных систем до класса 1Г включительно. Следует отметить, что продукт позволит выполнить требования к системе защиты персональных данных (на основании приказа ФСТЭК 58) не только к подсистеме межсетевого экранирования, но и к подсистемам управления доступом, а также регистрации и учета.

Следует также отметить, что продукт прост во внедрении: не требует реконфигурации сети или приобретения дополнительного оборудования. Его компоненты могут функционировать на сервере под управлением практически любой операционной системы семейства Windows.

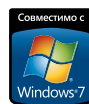
TrustAccess – оптимальное решение для эффективной сертифицированной защиты сервера БД

- Защита от большинства известных сетевых атак.
- Аутентификация сетевых соединений и разграничение доступа.
- Правила фильтрации с широким диапазоном настроек.
- Защита сетевого взаимодействия.
- Легитимность защиты подтверждена сертификатами ФСТЭК.
- Эффективность на современных конфигурациях информационных систем (терминальные соединения, виртуальные машины).
- Простота внедрения.

Важным преимуществом TrustAccess является наличие статусов совместимости Microsoft Works with Windows Server 2008 R2 и Microsoft Works with Windows 7. Драйверы TrustAccess протестированы в соответствии с методикой Microsoft и подписаны сертификатом WHQL (Windows Hardware Quality Lab).

Защитные механизмы TrustAccess эффективны в современных конфигурациях информационных систем (например, когда обращение к серверу БД осуществляется посредством сервера терминалов или сервер БД работает на виртуальной машине).

Следует отметить, что TrustAccess имеет статус VMware Ready и внесен в каталог партнерских продуктов VMware.



2 Обеспечивается без использования криптографических методов

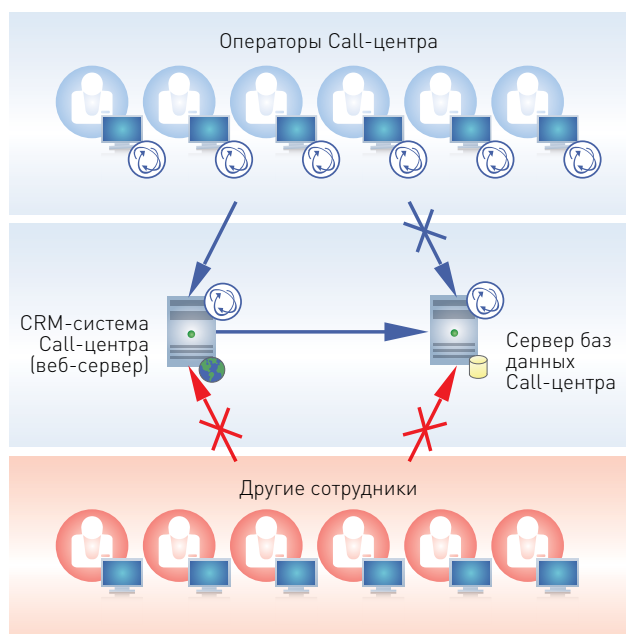
3 Имеется также усиленная версия продукта для защиты государственной тайны

Основные защитные механизмы TrustAccess перечислены в таблице:

Защитный механизм	Описание
Аутентификация сетевых соединений	Механизм аутентификации, реализованный в TrustAccess, основан на протоколе Kerberos, нечувствительному к попыткам перехвата паролей и атакам типа «Man in the Middle». Аутентификации подлежат не только субъекты доступа, но и защищаемые объекты, там самым, обеспечивается защита от подмены защищаемого объекта
Фильтрация сетевых соединений	Правила фильтрации TrustAccess обладают широким диапазоном настроек. Сетевые соединения можно ограничить на уровне сетевых протоколов, портов, пользователей, групп пользователей, параметров прикладных протоколов, временных интервалов. Возможна фильтрация сетевых соединений по протоколу Named Pipes
Защита от replay-атак	Для защиты от replay-атак применяется ISAKMP-ассоциация.
Защита сетевого взаимодействия	Защита сетевого взаимодействия достигается посредством использования протоколов семейства IPsec: <ul style="list-style-type: none"> • AH (Authentication Header) – позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP-пакета и, как следствие, обеспечивает защиту от атак типа «Man in the Middle»; • ISAKMP – предназначен для обмена ключами и согласования параметров соединения
Ограничение работы по некоторым сетевым протоколам	Можно разрешить или запретить сетевые соединения по протоколам согласно RFC 1700, а также по IPv4, IPv6 или Novell IPX
ICMP-защита	Гибкая настройка организации обмена сообщениями по межсетевому протоколу ICMP позволит обеспечить защиты от большинства атак отказа в обслуживании

Некоторые сценарии использования TrustAccess

Сценарий 1. Блокирование доступа пользователей к серверу БД



Нередко современные информационные системы, в том числе и информационные системы персональных данных, имеют многозвенную архитектуру, когда клиентское приложение обращается к серверу БД не напрямую, а посредством сервера приложений, веб-сервера и т.д.

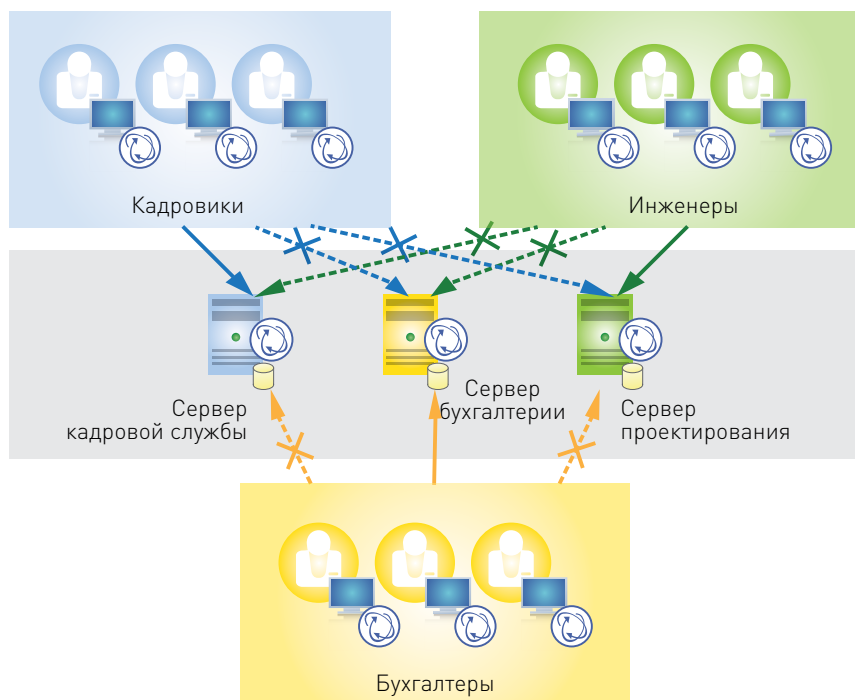
Рассмотрим данный сценарий немного подробнее на примере защиты ИСПДн в Call-центре. Операторы Call-центра принимают или совершают телефонные звонки, выполняя при этом обработку персональных данных, и фиксируют результаты в CRM-системе. CRM-система имеет трехзвенную структуру, представленную клиентским ПО на рабочем месте оператора Call-центра, веб-сервером и сервером БД.

TrustAccess позволит заблокировать сетевой доступ к серверу БД со всех ПК, кроме веб-сервера с CRM-системой Call-центра и для всех пользователей, за исключением администратора БД.

Сценарий 2. Разграничение доступа к серверу БД на основе должностей пользователей

Как правило, в организации используется несколько различных по своим функциям и характеру обрабатываемой информации информационных систем – и сервер БД также может быть не один. Например, сотрудники разных отделов могут использовать разные сервера БД.

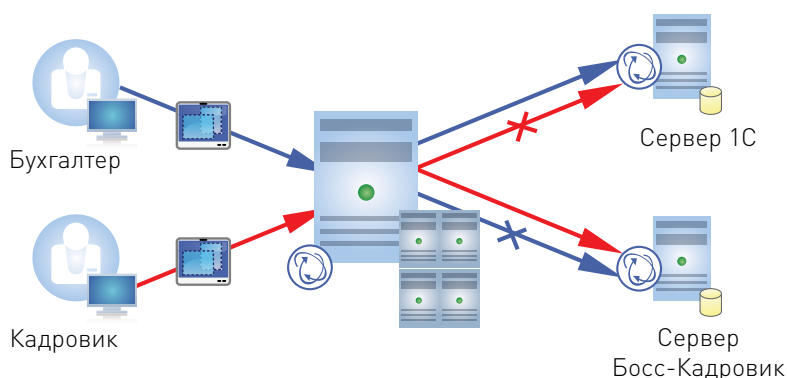
TrustAccess позволяет разграничить сетевой доступ к нескольким серверам БД на основе групп пользователей. В зависимости от того, в каком отделе работает сотрудник, он получает доступ к тому или иному серверу БД.



Сценарий 3. Разграничение доступа к серверам БД при терминальных соединениях

В случае использования решений на базе терминальных служб разные пользователи получают доступ к обрабатываемым данным с одного физического компьютера и с одного IP-адреса – сервера терминальных служб. В этом случае традиционные межсетевые экраны, где аутентификация осуществляется базе IP-адреса ПК пользователя, не позволяют разграничить доступ к серверам БД.

В отличие от них, в TrustAccess реализован более сложный алгоритм аутентификации на базе протокола Kerberos, который позволяет разграничить доступ к данным на уровне пользователей, работающих на одном физическом компьютере.



Сценарий 4. Защита сервера БД на виртуальной машине

Большинство атак на виртуальные машины уровне сети пользователей базируются на подмене подмене MAC- или IP-адресов. Тот факт, что механизмы защиты TrustAccess нечувствительны к подобным атакам, позволяет использовать его даже в случае выполнения сервера БД на виртуальной машине.

При этом TrustAccess позволит защитить сервер БД, запущенный на виртуальной машине, от сетевых атак как со стороны внешних физических машин, так и со стороны виртуальных машин.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.