Защита информации от кражи из информационных систем

Обзор современных методов защиты данных.

Введение

В настоящее время практически ежегодно в мире, да и в России происходит несколько крупных инцидентов, связанных с воровством конфиденциальной информации в различных учреждениях. При этом даже правоохранительные органы не всегда могут защитить свою информацию. Долгое время положение еще усугублялось тем, что ранее в России не было законов, позволяющих юридически закрепить необходимость защиты конфиденциальных данных и персональной информации клиентов, пользователей и др.

Однако юридические меры защиты приватных сведений выполняют только предупреждающую и реагирующую функцию. Очевидно, что закон сам по себе "не схватит за руку" администратора, служащего или чиновника, "сливающего" базы данных, но зато позволяет в случае, если удастся доказать вину служащего привлечь его к ответственности и, возможно, компенсировать нанесенный ущерб. Тем не менее, ежегодно происходят крупные утечки информации, которые обусловлены как техническими причинами (дырами в системе безопасности, наличие которых позволило злоумышленникам осуществить кражу), так инсайдерством (при помощи людей, имеющих легальный доступ к информации).

Далеко не полный список достаточно громких утечек информации из баз данных выглядит следующим образом:

- *в ноябре 2002 г. в Москве появился первый тираж дисков с данными об абонентах сети МТС, в январе 2003 г. вышел второй тираж – с информацией о 5,5 млн абонентов компании. Источник утечки найден не был;*
- *20 мая 2003 г. в Санкт-Петербурге появились диски с данными о 4,5 млн клиентов сотовых компаний "МегаФон", "Телеком XXI", "Северо-Западный телеком" и "Петерстар". По одной из версий, утечка произошла через правоохранительные структуры;*
- *в июле 2004 г. "Вымпелком" сообщил милиции о сайте sherlok.ru, предлагавшем информацию об абонентах "Билайна", "МегаФона" и МТС в Москве и Санкт-Петербурге. 26 ноября задержаны семеро подозреваемых, в числе которых трое сотрудников "Вымпелкома". В марте 2005 г. Останкинский суд приговорил их к различным штрафам;*
- *в феврале 2005 г. в Москве появилась база данных о банковских операциях Центробанка в 2003-2004 годах, 20 мая стало известно о выходе нового, дополненного издания. 25 октября замглавы управления безопасности и защиты информации Московского управления ЦБ Владимир Бабкин заявил, что канал утечки перекрыт, но не назвал конкретных виновных;*
- *8 ноября 2005 г. появились в продаже данные о доходах в 2004 г. 9,9 млн жителей Москвы и области. 16 ноября 2005 г. ФСБ объявила о задержании лиц, причастных к хищению баз данных Центробанка РФ и ФНС. Имена подозреваемых, а также их дальнейшая судьба неизвестны.*

  15 августа 2006 г. ряд бюро кредитных историй и банков получили по электронной почте предложение купить базу данных заемщиков, бравших потребительские кредиты. База содержала 700 тыс. записей;
- *7 сентября 2006 г. гендиректор Национального бюро кредитных историй Александр Викулин заявил, что утечка произошла из двух или трех банков. Конкретные банки названы не были;*
- *в середине декабря 2006 г. TJX Companies – управляющая компания одной из крупнейших американских торговых сетей, в ведении которой находится около 2,5 тыс. розничных магазинов, обнаружила утечку большого количества данных;*
- *в августе 2007 г. произошла кража сервера из офиса частной компании Forensic Telecommunications Services (FTS) в городке Севеноакс (Sevenoaks), графство Кент. Эта компания специализируется на извлечении информации из мобильных устройств (в том числе и поврежденных), а также ее дальнейшей передачи в качестве доказательств для судебных разбирательств. Среди клиентов FTS – знаменитый Скотланд-Ярд, а также различные полицейские инстанции Соединенного Королевства. [2]*

Как видно из инцидентов, утечка информации происходит по разным каналам – это и Интернет, и электронная почта, и просто копирование информации на разные носители, и даже кража сервера!

Сейчас только ленивый не говорит, что в России уже сформировался черный рынок нелегальных баз данных, и некоторые даже оправдывают это явление тем, что пока есть спрос на подобную информацию, то будет и предложение. И, соответственно, заявляется, что эффективно защитить такие данные невозможно. Однако, например, в Европе такие базы данных не рекламируются в Интернет, часть информации там вообще практически невозможно получить из открытого доступа. Кроме того, разглашение таких данных там может приводить к более серьезным последствиям. Получить конфиденциальные данные отдельных крупных компаний в России также практически невозможно – поскольку в данных компаниях принимаются достаточно эффективные меры по защите информации. Таким образом, как бы ни оправдывались отдельные должностные лица, ограничить доступ к приватным данным возможно, если применять грамотные организационно – технические меры.

Типичные способы кражи информации и атаки на СУБД

Огромный объем важнейшей для компании информации – сведения о финансовой деятельности, технических средствах и клиентах – хранится в легкодоступных БД.

Кроме того, информацию можно перехватить через каналы связи и системы хранения и др. Атаки на базы данных могут быть разными, например:

- DoS-атаки, направленные на отказ в обслуживании или приводящие к дезорганизации работы баз данных;
- получение информации с использованием стандартных интерфейсов путем получения или подбора идентификационной информации (пароли, имена пользователей);
- получение информации путем доступа с использованием уязвимостей в операционной системе, в базе данных, различные типы хакерских действий (SQL Injection и др);
- получение доступа с правами администратора (файловый доступ, локальный доступ);
- уничтожение информации или искажение (в том числе с использованием червей, вирусов);
- перехват информации по сети при ее передаче (удаленное подключение пользователей к базам данных).

По источникам атаки можно разделить на две категории:

- *внешние угрозы*: хакеры, черви;
- *внутренние угрозы*: операторы баз данных, администраторы серверов и баз данных; легальные пользователи; внутренние сотрудники, не имеющие официального доступа, но пользующиеся компьютерами легальных пользователей, разработчики, аналитики и др.

Злоумышленник может использовать различные приемы и действия:

- оставить "лазейку" или завести свою учетную запись в СУБД;
- загрузить троянца, который будет собирать пароли и/или данные;
- использовать сервер БД как площадку для атак на другие хосты;
- получить выборку данных из СУБД;
- изменить/переместить данные;
- поставить сниффер на свой компьютер или компьютер, находящийся в одном сегменте с серверами (или использовать возможности сетевого оборудования по перенаправлению трафика), и перехватывать SQL-трафик.

Типичные способы защиты информации

Важнейшей проблемой, стоящей перед руководством и службой безопасности предприятия, является проблема лояльности сотрудников, или, иными словами, проблема внутренних угроз информационной безопасности.

Так, по различным оценкам, от 50 до 80% атак, направленных на получение информации ограниченного доступа, начинается из локальной сети предприятия (интрасети).

Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Особую актуальность проблема внутренних угроз получила в связи с появлением и повсеместным распространением мобильных накопителей информации, подключаемых через USB порты – таких как flash-диски, винчестеры с USB-интерфейсом и т.д.

При построении системы защиты данных необходимо учитывать много факторов и делать систему защиты многоуровневой.

Информация хранится либо в обычных файлах, либо в базах данных.

Сейчас большинство компаний в мире используют базы данных от нескольких основных производителей. По данным Gartner, крупнейшими среди них являются: Oracle, Microsoft, IBM.

Общие принципы и тенденции по защите информации в данных базах данных достаточно похожи, однако частные применения нередко сильно различаются. Кроме того, появился целый класс систем безопасности сторонних производителей, который призван усилить безопасность информации.

Рассмотрим, какие виды защиты информации применимы к данным. В целом их можно разделить на несколько типов:

1. Системы разграничения доступа, основанные на построении разных интерфейсов доступа к данным и имеющие разную функциональность (Database View). Например, программа для рядовых пользователей позволяет иметь доступ только к определенным видам данных в БД, делать только определенные выборки данных и отчеты.

2. Системы разграничения доступа, основанные на файловом принципе (разрешения по доступу к файлам данных с разными привилегиями – на запись, чтение и др.).

3. Системы шифрования файлов.

4. Системы создания виртуальных шифрованных дисков (когда доступ к информации осуществляется как к логическому диску компьютера или сервера, а данные находятся в зашифрованном файле).

5. В случае распределенной сетевой системы – On-line мониторинг SQL запросов к базе данных и отключение потенциально опасных; кроме того, разграничение доступа, основанное на сетевых адресах и др.

6. Применение специальных аппаратных средств, позволяющих автоматически шифровать информацию, попадающую в базу данных.

7. Шифрование полей и записей в базах данных с использованием внутренних механизмов баз данных.

8. Шифрование данных в системах хранения.

Современные решения по защите данных

Защиту данных в базах данных, системах хранения, особенно если система работает в режиме On-line, можно рассмотреть с точки зрения нескольких аспектов:

1. Защита при хранении.

2. Защита при передаче.

3. Защита при обработке.

Для обеспечения "трех китов" информационной безопасности (конфиденциальности, целостности и доступности),

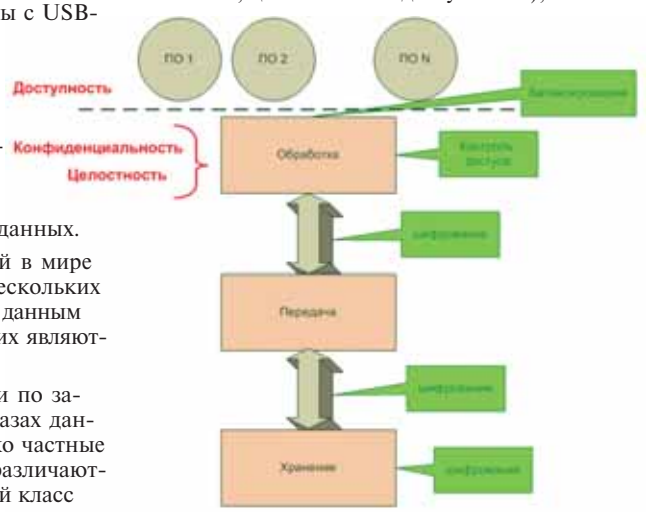

Рис. 1. Уровни защиты данных.

применительно к этим аспектам, можно использовать как программные, так и аппаратные средства.

Аппаратные средства подразумевают установку дополнительного устройства, которое не только стоит денег, но и усложняет архитектуру и без того непростой системы хранения. Следует заметить, что, безусловно, если необходимо реализовать грамотную систему защиты, то никто не будет оспаривать необходимость установки:

- межсетевых экранов;
- средств организации VPN;
- узловых систем обнаружения и предотвращения вторжений и разграничения доступа;
- балансировщиков и средств обеспечения доступности и т.д. и т.п.

Однако это темы для отдельного рассмотрения.

Вопросы, которыми мы задаемся здесь, звучат так: "Можно ли защитить информацию от кражи? Каким образом и какими продуктами это может быть сделано?"

В качестве простейших и всем известных программных средств, позволяющих защитить хранимую информацию, являются такие прикладные средства, широко используемые в сфере малого и частного бизнеса, как PGP или SecretDisk от Aladdin.

Названные программные продукты позволяют создать виртуальный логический диск, который для ОС узла выглядит как еще один раздел, а на самом деле физически представляет собой за-

шифрованный файл на обычном носителе (например, "нормальном" жестком диске) или зашифрованный раздел, который невозможно прочитать обычными средствами. Деление подобных программ на классы "более или менее" функциональные зависит от тех дополнительных возможностей, которые в них встроены.

Так, если система позволяет загрузиться с зашифрованного раздела, то это повышает защищенность комплекса в целом, поскольку злоумышленник не сможет физически извлечь НЖМД и подключить его на другом сервере с целью получения доступа к параметрам рабочей среды и получения ее параметров настройки. Другим фактором может быть возможность аутентификации пользователя при доступе к комплексу не только по парольной фразе, но и с помощью данных учетной записи, хранящейся в ОС или внешних аппаратных средствах аутентификации (например, USB-токен или смарт-карта).

Решения IBM

Решение IBM Tivoli SecureWay Security Manager предназначено для активного предотвращения попыток несанкционированного доступа к системам и является ярким представителем системы разграничения доступа. Tivoli SecureWay Security Manager позволяет объединить разнородные модели безопасности системы и сделать различия между централизованной и распределенной системой безопасности прозрачными для администраторов. Оно обеспечивает полное применение стратегии безопасности независимо как от географических, так и от платформенных ограничений. Tivoli SecureWay Security Manager также предоставляет гибкие возможности для аудита системы и позволяет выделить определенные группы ресурсов, для которых будет вестись наиболее подробный аудит. Безопасность при управлении атрибутами и службами пользователей в гетерогенных распределенных сетях обеспечивает другой продукт, входящий в состав программного пакета Tivoli Enterprise – Tivoli SecureWay User Administration. Он обеспечивает возможность централизованного управления большой распределенной сетью, содержащей компьютеры на разных платформах, основанное на разных подходах: на основе политик, по подписке, защищенное предоставление прав доступа и платформенно-независимое наследование, что позволяет сэкономить время и уменьшить число ошибок.

Другие методы, обеспечивающие разграничение доступа, были применены в продукте Centera компании EMC.

Для предприятий, где действуют строгие нормы регулирования, EMC предлагает продукт Centera Compliance Edition. Он следит за тем, чтобы управление записями велось согласно установленным бизнес-правилам, в частности, запрещает уничтожать объекты прежде, чем закончится их срок хранения. Кроме того, каждому объекту хранения дается "цифровой отпечаток пальца" – уникальный идентификатор, благодаря чему Centera надежно хранит информацию и выдает содержание только тем, у кого есть соответствующие права (поддерживается автоматическая аутентификация). Изюминкой решения является то, что информация в системе хранится в таком виде, что, просто подключившись к системе, получить доступ к информации без специальных данных невозможно, информация "размазана" по системе хранения и чтобы собрать воедино данные, необходимо будет потратить большое количество времени, а иногда это и невозможно. В сочетании с другими методами защиты (криптографическими) такая система дает неплохие результаты.

Большинство решений по защите СУБД не предусматривают защиту хранящейся в них информации как таковой. Для эффективного предотвращения НСД к информации в базах данных защита должна быть спроектирована таким образом, чтобы обеспечивать защиту непосредственно самой информации, вне зависимости, каким образом она используется или к ней осуществляется доступ.

Решения RSA

Компания RSA, подразделение EMC по безопасности, в феврале этого года объявила об изменениях в стратегии защиты данных предприятия (EDP), которые позволят защитить конечные точки шифрования по всему предприятию, независимо от местонахождения данных. Основную роль в этом сыграло объявленное компанией RSA соглашение о приобретении компании Valyd Software и установление стратегических партнерских соглашений с компаниями CipherOptics, Decru, NeoScale Systems и Epicor/CRS.

Предлагаемый компанией RSA обновленный продукт Database Security Manager работает напрямую с базой данных и обеспечивает защиту ее выделенных критичных элементов. В основе работы RSA Database Security Manager лежат мощные технологии шифрования промышленного стандарта – прозрачные для всех пользователей и приложений, которым необходим доступ к СУБД, и позволяющие существующим бизнес-процессам и информационным потокам протекать как обычно. Таким образом, RSA Database Security Manager подходит для работы СУБД в гетерогенных средах, что обеспечивает единообразный подход к безопасности в разных системах независимо от производителя.

В данный момент RSA Database Security Manager может использоваться для целого ряда систем управления базами данных: IBM, Microsoft, Oracle, Sybase и Teradata.

Продукт RSA File Security Manager предназначен для защиты от внутренних и внешних атак важных данных, которые хранятся в виде файлов. RSA File Security Manager отвечает за централизованное управление, четкое распределение обязанностей и другие особенности политики безопасности в отношении важных файлов, независимо от их места нахождения. Централизованное управление ключами шифрования обеспечивает быструю идентификацию ключа, что снижает вероятность несанкционированного доступа к данным или их потери.

Комбинация продуктов RSA Database Security Manager и RSA File Security Manager с решениями в области шифрования ее партнеров должно обеспечить более тесную интеграцию решений по безопасности и средств управления ключами, предусмотренными в продукте RSA Key Manager.

Решения Oracle

Внутренние механизмы СУБД Oracle также позволяют дополнительное разграничение полномочий внутри базы данных с реализацией ограничения доступа к данным защищаемых приложений со стороны администратора баз данных, а также ограничение доступа и контроль в зависимости от IP-адреса, времени, операции при помощи компоненты Database Vault, которая позволяет создать защищенные области (realms). Комплекс решений по защите и управлению инфраструктурой приложений IAMS реализует механизм разделения прав и привилегий со стороны приложений, пользователей, сервисов, ролевой механизм управления в масштабах всей информационной системы на базе принципа "need-to-know" и усиленную аутентификацию. Технология мандатного механизма контроля доступа с использованием меток конфиденциальности (Label Security) обеспечивает построчный контроль доступа к данным. Использование Advanced Security Options (ASO) позволяет осуществлять прозрачное шифрование данных в БД и обеспечивает защиту клиентского трафика.

Необходимо отметить, что шифрование колонок таблиц и администрирование ключей в IBM® DB2® Universal Database также реализовано просто и удобно: ключ шифра достаточно задать всего один раз за сеанс, вместо того, чтобы указывать его при каждом обращении к механизму шифрования. Но, в отличие от IBM, в СУБД Oracle9i реализована декларативная модель обеспечения безопасности на уровне отдельной записи, превосходящая по мощности и выразительным возможностям реализованный в DB2 (и в Microsoft SQL Server) механизм контроля доступа к записям через представления. Кроме того, продукты Oracle поддерживают исполнение компонентов Enterprise JavaBeans непосредственно в среде СУБД, тогда как DB2 использует механизмы WebSphere.

Решения Microsoft

В ОС Microsoft, начиная с версии 2000, есть встроенная служба шифрования данных. В своей работе она, в свою очередь, использует службу PKI, которая позволяет в (полу)автоматическом режиме генерировать ключи шифрования для пользователей. Точнее говоря, она позволяет генерировать ключевые пары, которые используются впоследствии для защиты ключей шифрования, на которых уже за-

Рис. 2. Взаимодействие компонент во встроенной службе шифрования данных Microsoft ОС.

щищаются данные пользователя (рис. 2).

При этом секретный ключ пользователя из ключевой пары, который и используется для защиты ключей шифрования, хранится в специальном контейнере ОС, который недоступен для программного окружения, либо может применяться внешнее аппаратное хранилище (USB-токен или смарт-карта). Однако и здесь есть нюансы. Во-первых, если файл или данные зашифрованы на ключе пользователя, то никто, кроме него, не может их расшифровать. Приходим к необходимости использования модели с полной матрицей доступа, а, следовательно, присущим ей недостаткам.

Таким образом, нерешенной остается проблема, с одной стороны, надежной защиты секретных ключей шифрования, а с другой – обеспечения оперативного и прозрачного доступа к ним с рабочего места пользователя, содержащие совершенно полярные требования!

Может быть, отказаться от шифрования данных на серверах или рабочих станциях с помощью программных дополнительно устанавливаемых агентов шифрования и доверить защиту специализированному ПО на уровне самой системы хранения, а не файловой системы, где физически размещаются файлы с данными?

Неплохой вариант, тем более, что такие гиганты индустрии, как Microsoft и Oracle в своих СУБД уже давно реализовали подобные механизмы.

Как видно из таблицы, оба продукта реализуют сходный набор сервисов защиты, при этом у компании Oracle есть четкое разделение (и, соответственно, позиционирование) различных версий своих продуктов.

Если рассматривать функциональность “топовых” версий продуктов, обозначенных в таблице, то мы практически не найдем разницы. Таким образом, можно сделать вывод, что для адекватной защиты информации на уровне

Таблица. Сравнение Oracle и SQL Server (ист.: [1]).

Функция	SQL Server 2005	Oracle 10g Standard Edition	Oracle 10g Enterprise Edition	Oracle 10g Enterprise с Advanced Security Option
Интегрированный единый вход в Windows (Single Sign-On)	ДА	Недоступно	Недоступно	ДА
Шифрование сетевых пакетов	ДА	Недоступно	Недоступно	ДА
Шифрование данных	ДА	Недоступно	Недоступно	ДА
Инфраструктура Открытого Ключа	ДА	Недоступно	Недоступно	ДА
Поддержка Kerberos	ДА	Недоступно	Недоступно	ДА
Схемы	ДА	ДА	ДА	ДА
Роли базы данных и сервера	ДА	ДА	ДА	ДА
Аудит	ДА	ДА	ДА	ДА
Профили/Политики	ДА	ДА	ДА	ДА
Службы Сертификатов	ДА	Недоступно	Недоступно	ДА
Выполнение с наименьшими	ДА	ДА	ДА	ДА

СУБД следует иметь не только эффективные средства шифрования, но и удобные механизмы работы с ними.

Внешние решения

Другие производители предлагают достаточно интересные решения по защите информации в базах данных и системах хранения.

Например, устройства Decru DataFort устанавливаются между клиентами и системами хранения, где находится вся информация баз данных или другая информация, и позволяют прозрачно шифровать информацию, которая находится в базе данных или системе хранения. При этом шифруется только информация – служебные данные таблиц не шифруются – что дает полную прозрачность решения и высокую совместимость устройства с системами хранения данных и базами данных.

Поскольку информация зашифрована, кража ее с носителей или другим способом невозможна. Остается только участок между клиентом и собственно шифратором, но тут используются другие методы защиты.

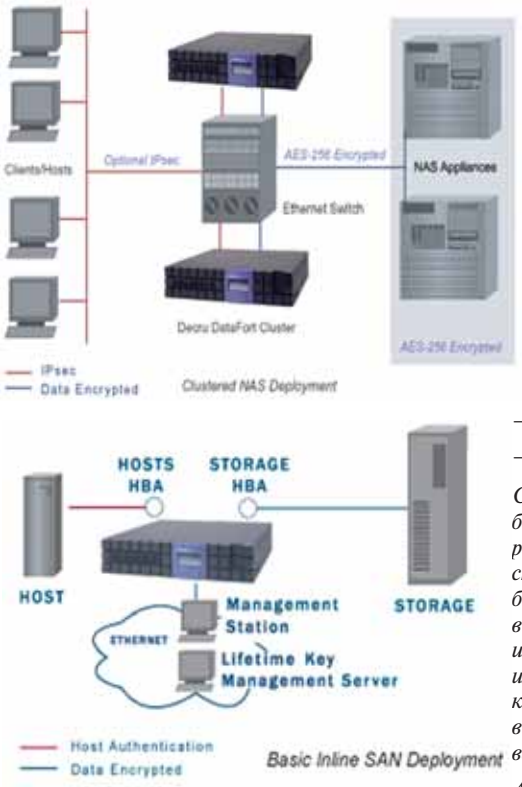

Рис. 3. Типовые схемы включения устройств Decru DataFort.

Устройства Decru DataFort сочетают функциональность контроля доступа, аутентификации и шифрования хранилищ данных для обеспечения надежной защиты конфиденциальной информации. Комплексы на базе Decru DataFort могут быть развернуты в среде SAN, NAS и DAS, использоваться для защиты дисковых хранилищ данных и резервных копий на ленту. Устройства DataFort “прозрачны” для всех элементов сетевой инфраструктуры и не требуют изменений конфигурации серверов, рабочих станций, приложений и информационных потоков (рис. 3).

В системах SAN и при работах с базами данных возможно просто включение в разрыв. Возможно и отказоустойчивое включение, в том числе и при смешанном хранении данных (рис. 4).

Таким образом, решения по защите на внешних устройствах позволяют вынести процессы шифрования на отдельные защищенные устройства и снизить нагрузку на основные серверы, обезопасив процессы шифрования и ключи от перехвата злоумышленниками.

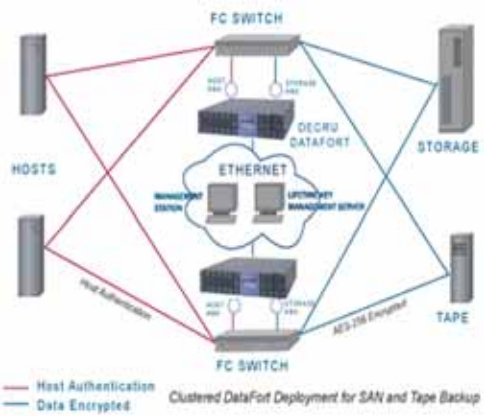

Рис. 4. Отказоустойчивое включение устройств шифрования в SAN (в том числе и при смешанном хранении данных).

Заключение

При обеспечении защиты данных от несанкционированного доступа и от кражи, необходимо применять комплексные методы обеспечения безопасности:

– настройки внутренних механизмов безопасности систем;

– разграничение доступа на уровне сети, пользователей и др.;

– технологии строгой аутентификации и SSO (однократной регистрации в системе);

– функции аудита;

– средства шифрования данных.

Средства администрирования и настройки безопасности играют непосредственную роль в обеспечении защиты данных, поскольку организационную составляющую безопасности невозможно исключить ни в одном процессе. Если администратор не имеет эффективных средств настройки или не знает, как ими пользоваться, то какие бы глубокие и надежные механизмы в них не были бы реализованы, воспользоваться ими он не сможет.

Аудит и контроль доступа позволяет отслеживать режимы доступа, отметки времени, тип, а также дополнительные характеристики, включая содержимое запросов, что позволяет упростить как труд разработчиков при отладке программных комплексов, так и администраторов безопасности, регулярно проверяющих журнал событий на предмет выявления подозрительной активности.

Конечно, самым действенным средством защиты данных на сегодняшний момент является шифрование информации. Если данные зашифрованы, то риск утечки информации значительно уменьшается, кроме того, это единственный метод, позволяющий защищаться от несанкционированных действий администратора баз данных и сисадмина, управляющего всей системой. Технология Decru обеспечивает разграничение доступа к данным в соответствии с полномочиями и позволяет снизить нагрузку на серверы (шифрование достаточно емкий процесс, приводящий к сильному снижению производительности) и вынести процессы шифрования на отдельное устройство – соответственно, сисадмин и разработчики не смогут отключить (случайно или намеренно) процессы шифрования.

Наиболее интересными встроенными механизмами безопасности обладают решения компаний Oracle и Microsoft. Они позволяют более просто интегрироваться с другими системами безопасности (разграничения доступа, User Authentication, Authorization, Auditing, Network Encryption, Data Encryption и Single Sign-On (SSO), системы Identity Management и др.), выпускаемыми данными вендорами, обеспечивая комплексную безопасность системы в целом.

В данной статье авторы постарались рассмотреть только существующие подходы к обеспечению конфиденциальности и целостности данных при их хранении, а адекватный уровень защиты можно обеспечить только построением комплексной системы защиты, включающей организационно-технические меры, средства межсетевого экранирования, VPN, IDS/IPS, системы аудита, мониторинга и т.п.

Михаил Романов

Список литературы:

1. http://www.infowatch.ru/threats?chapter=147151398&id=207732899

2. http://business.km.ru/magazin/view.asp?id=01BC3B56C638476098CD8AF3A3FD352

3. Mitch Ruebush, Сравнение моделей безопасности SQL Server 2005 и Oracle 10g. Апрель, 2005

4. Gordon Arnold, Introduction to Storage Security. SNIA, March, 2007

5. Michael Fahey, Alternative approaches to storage security. SNIA, March, 2007

6. Eric Hibbard, A Chief Information Security Officer View of Storage Security, SNIA, March, 2007

Cisco, EMC и Microsoft объединяют усилия в защите информации

Июль 2007 г. – Компании Cisco®, EMC® и Microsoft объявили о формировании альянса *(www.SISAalliance.com)* поставщиков технологий, имеющего целью создание максимально универсальной и защищенной коммерческой технологической архитектуры для полноценного обмена информацией с поддержкой компонентов различных производителей. Такая архитектура позволит защитить конфиденциальную официальную информацию при обеспечении коллективного доступа к ней. Архитектура для обмена защищенной информацией (сокращенно SISA) объединит в себе приложения, инфраструктуру и сетевые технологии от ведущих поставщиков и позволит повысить эффективность инвестиций клиентов в IT-системы. Эта архитектура предлагает единый подход, позволяющий обычно разрозненным IT-инфраструктурам компаний работать вместе и обеспечивать максимальную защиту конфиденциальной деловой информации (о кадрах, финансах и др.), используемой группами пользователей с соответствующими правами доступа.

Традиционно технологии защиты информации внедрялись в отдельных системах, защищая разрозненные конгломераты данных. Некоторые государственные учреждения сталкиваются с проблемами, пытаясь предоставить ролевой доступ к конфиденциальной информации даже внутри собственных организаций – а при необходимости предоставления такого доступа представителям разных ведомств проблемы, конечно, усугубляются. В сотрудничестве с SISA, государственные службы смогут намного эффективнее создавать защищенные виртуальные сети для различных авторизованных пользователей и сообществ и предоставлять им доступ к секретным файлам, хранящимся в различных системах защиты информации. SISA позволит применять новые сценарии обмена информацией между организациями. Например, в будущем SISA может применяться, чтобы позволить руководителям системы здравоохранения отслеживать, например, получаемые от различных госслужб и из баз данных частного сектора конфиденциальные данные об эпидемиях, с тем чтобы координировать необходимые ответные усилия своих основных партнеров как в государственном, так и в частном секторе.

Cisco, EMC и Microsoft поставят основные технологии для SISA. Это облегчит процесс обмена информацией, содержащейся в разрозненных IT-инфраструктурах. Используя свои передовые решения, Cisco обеспечит защиту сетей, увеличит безопасность взаимосвязи виртуальных сетей и функции защиты данных, чтобы конфиденциальная информация могла использоваться по всей сетевой платформе. Сетевые системы хранения EMC, программное обеспечение для управления информацией и ее защиты позволяют создать гибкую информационную инфраструктуру для хранения данных, управления ими и помощи в защите важнейшей и конфиденциальной информации. Microsoft предоставляет системы по управлению идентификацией, клиентами и сетями, а также схему сотрудничества, позволяющую держать информацию под контролем авторизованных пользователей.

Альянс SISA также включает поставщиков технологий, обеспечивающих инновационный подход к удовлетворению конкретных требований пользователей. Компания Liquid Machines (Уолтхем, штат Массачусетс) предлагает решения, расширяющие возможности SISA в области защиты информации путем развития технологии Microsoft® Digital Rights Management. Корпорация Swan Island Networks (Портленд, штат Орегон) создает и внедряет системы обмена конфиденциальной информацией. Предприятие Titus Labs (Оттава, Канада) обладает решениями по маркировке и классификации данных для определения необходимой степени их защиты. По мере развития потребностей пользователей альянс планирует привлекать к работе новых поставщиков технологий, чтобы гарантировать максимально передовой подход к решению возникающих проблем.