Петрянин Д.Л., Горячев Н.В., Юрков Н.К.
Пензенский государственный университет

АНАЛИЗ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

В настоящее время массовое применение персональных компьютеров (ПК) в разных сферах деятельности растет все более интенсивно. Основным инструментом хищения информации в базах данных (БД) являются вредоносные программы: трояны, руткиты и другие вредоносные программы, препятствующие нормальной работе компьютера, разрушающие файловую структуру жестких дисков и наносящие значительный ущерб хранимой в компьютере информации.

Информационная безопасность, как и защита информации – задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

В настоящее время сформулировано три базовых принципа, которые обеспечивают информационную безопасность:

целостность данных — защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;

конфиденциальность информации;

доступность информации для всех авторизованных пользователей.

Обеспечение безопасности информации требует затрат, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Средства зашиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ потенциальных угроз. [1]

Рассмотрим некоторые существующие системы защиты информации в БД.

Компания «Аладдин Р.Д.» разработала линейку программных продуктов для повышения уровня безопасности корпоративных информационных систем.

а) Крипто БД для Oracle

«Крипто БД» — средство криптографической защиты информации (СКЗИ), хранящейся в БД Oracle от несанкционированного доступа:

рекомендуется для защиты персональных данных, хранящихся в системах управления базами данных (СУБД) Oracle, в соответствии с №152-ФЗ «О персональных данных»;

соответствует требованиям ФСБ России к СКЗИ класса КС1, КС2;

позволяет выполнить наиболее критичные требования стандарта PCI DSS для систем, использующих банковские карты;

дополняет штатные средства безопасности Oracle Database Server, включая редакции Standard Edition и Standard Edition One;

может быть использовано для защиты персональных данных в облачных средах.

СКЗИ «Крипто БД» состоит из следующих компонент:

компоненты сервера «Крипто БД»;

клиентское программное обеспечение (ПО) — SecurLogon для Oracle;

консоль управления администратора безопасности;

коллекторы аудита (опционально).

б) SecurLogon для Oracle

Продукт SecurLogon для Oracle представляет собой программное решение для усиления возможностей аутентификации, заложенных в СУБД Oracle и позволяет реализовать:

двухфакторную аутентификацию пользователей БД с использованием USB-токенов и смарт-карт;

шифрование передаваемых данных с использованием возможностей протокола SSL;

взаимную аутентификацию клиента и сервера.

По сравнению со средствами защиты информации, встроенными в СУБД Oracle, решение SecurLogon для Oracle имеет следующие преимущества:

эффективно решает проблему защищенного хранения ключей и сертификатов пользователей;

существенно облегчает администрирование функций безопасности информационной системы за счет централизованного управления функциями аутентификации и ключевыми носителями.

В то же время решение SecurLogon для Oracle имеет свои ограничения:

на рабочем месте требуется установка дополнительного ПО;

необходимо приобретение лицензий на использование продукта;

решение основано на применении западных криптографических алгоритмов. [2]

Сетевой защитой информации занимается компания Zecurion.

DLP расшифровывается как Data Loss Prevention и используется для обозначения продуктов и систем для защиты от утечек информации.

DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности, или, иными словами, на защиту корпоративной информации от инсайдеров. Инсайдерами являются абсолютно все сотрудники компаний, ведь утечки могут происходить не только по злому умыслу, но и по невнимательности сотрудников или незнанию правил информационной безопасности. Более того, согласно статистике, 78% зарегистрированных инцидентов приходится именно на случайные утечки.

Существует множество подходов к классификации DLP-систем, однако более-менее устоявшиеся представления рынка указывают на несколько характеристик, позволяющих относить ИТ-решения к классу DLP:

Потенциальные каналы утечки информации составляют две большие группы: сетевые каналы (к ним относится электронная почта, интерактивные веб-сайты, блоги, форумы и т.п.) и локальные (принтеры, а также любые периферийные устройства, на которые можно скопировать конфиденциальную информацию).

DLP-системы перехватывают весь трафик, выходящий за пределы корпоративной сети предприятий, и анализируют его на предмет наличия в нем конфиденциальной информации. Существует более десятка типов данных, обнаружить которые можно только с помощью различных специализированных технологий детектирования.

На основании данных анализа DLP-система принимает решение согласно установленным политикам безопасности о разрешении или запрете передачи сообщения, записи или печати файла.

Весь перехватываемый трафик DLP-система помещает в собственный архив, который создает полноценную базу для расследования инцидентов информационной безопасности.

Zecurion DLP позволяет контролировать:

Переписку в корпоративной электронной почте.

Письма и вложения, отсылаемые через сервисы веб-почты.

Общение в социальных сетях, на форумах и блогах (HTTP/HTTPS).

Сообщения интернет-пейджеров — ICQ, Mail.Ru Агент, QIP, Google Talk и более десяти других систем, включая Skype.

FTP, POP3, IMAP, SMTP и другие сетевые каналы.

Файлы, записываемые на USB-накопители и любые внешние устройства.

Печать на локальных и сетевых принтерах и другие каналы утечки.

Наличие конфиденциальных данных, хранящихся на компьютерах пользователей и серверах.

Доступ к информации, хранящейся на серверах, магнитных лентах и оптических дисках.

Основные преимущества Zecurion DLP:

Контроль всех наиболее опасных каналов утечки.

Гибридный анализ перехваченных данных (эффективность более 95%) с использованием морфологии, «цифровых отпечатков», регулярных выражений, OCR и собственной технологии SmartID.

Поддержка анализа более 500 типов файлов.

Возможность блокирования утечек в режиме реального времени.

Архивирование всей перехваченной информации, возможности последующего поиска и анализа данных архива.

Сканирование локальных и сетевых хранилищ для поиска файлов с конфиденциальной информацией.

Защита данных в местах хранения — на серверах и резервных носителях информации.

Единая консоль управления.

Комплекс Zecurion DLP объединяет в себе Zgate для контроля всего сетевого трафика, Zlock для контроля периферийных устройств, Zdiscovery для обнаружения нарушений политик хранения конфиденциальных документов и Zecurion Zserver для шифрования серверов.

Шифрование данных при хранении:

В условиях динамичной конкурентной среды корпорации стремятся к централизации данных для обеспечения возможности оперативно реагировать на изменяющиеся условия рынка. Вместе с тем централизация данных создает дополнительные угрозы безопасности конфиденциальной информации.

Проблема заключается в том, что средства защиты периметра сети и антивирусы не смогут предотвратить утечки информации, если злоумышленник получит физический доступ к носителю информации. Вот некоторые возможные варианты утечки информации, когда обычные средства защиты периметра не помогут защитить информацию:

Размещение серверов в стороннем дата-центре (collocation).

Отправка серверов или жестких дисков в ремонт.

Перевозка компьютеров из одного офиса в другой, например при переезде.

Утилизация компьютеров, серверов, жестких дисков и лент.

Хранение магнитных лент в специальном депозитарии (off-site storage).

Перевозка ленты, например в депозитарий.

Кража или потеря жестких дисков или лент.

Попадание в руки злоумышленника жесткого диска с конфиденциальной информацией может нанести серьезный ущерб деятельности компании и даже поставить под угрозу дальнейшее ее существование. В такой ситуации единственной возможной защитой данных является шифрование информации на носителе. Шифрование является широко признанным простым и эффективным способом защиты информации на носителях. При этом данные постоянно хранятся в зашифрованном виде и становятся доступны для использования только при загрузке ключа шифрования.

Комплекс Zecurion Zserver Suite предназначен для шифрования данных, размещенных на жестких дисках, на дисковых массивах (RAID-массивы любых конфигураций) и в хранилищах SAN, а также резервных копий информации на магнитных лентах и оптических дисках. Zserver Suite использует только современные криптостойкие алгоритмы шифрования, надежные методы генерации и хранения ключей. [3]

Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок второго рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки первого рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. [4]

Программное обеспечение SafeNet ProtectDB совместно с аппаратно-программным комплексом DataSecure обеспечивает надежную защиту конфиденциальной корпоративной и клиентской информации, которая хранится в БД.

С его помощью можно шифровать информацию на уровне столбцов в БД, на уровне приложений, а также в ходе пакетного преобразования данных и различных транзакций. Программное обеспечение ProtectDB позволяет избежать рисков, связанных с доступом привилегированных пользователей, за счет возможности распределения административных задач. Аппаратно-программное решение DataSecure поддерживает централизованное управление ключами и политиками, что упрощает внедрение шифрования данных почти в любое количество БД, используемых в разнородных средах. [5]

Гарда БД — система аудита сетевого доступа и защиты БД. Система предназначена для защиты информации в БД предприятий, позволяет отслеживать неправомочное обращение к БД в соответствии с критериями и правилами анализа, задаваемыми сотрудниками отдела информационной безопасности. Система подключается пассивным образом к корпоративной сети и позволяет вести мониторинг обращений к БД в режиме реального времени. При обнаружении подозрительных операций сотрудников система уведомляет сотрудника отдела ИБ и протоколирует соответствующий запрос и ответ БД (рис. 1).