Юлия Мастихина

DLP-системы на страже корпоративной информации

Проблема защиты от инсайдерства и утечек информации стала в последнее время едва ли не самой актуальной для компаний. В условиях продолжающегося экономического кризиса многие компании-разработчики решений в области информационной безопасности наблюдают смещение интереса корпоративных клиентов в сторону защиты от внутренних угроз. Причины этому довольно очевидны. В первую очередь, это связано с негативными тенденциями на рынке труда, увольнениями и понижениями доходов сотрудников. Аналитики и эксперты отмечают, что вирусные атаки и неавторизованный доступ постепенно уступают место в общей структуре угроз ИБ утечкам конфиденциальной информации. По данным исследовательского центра компании InfoWatch в 2008 году 42% утечек информации произошло неумышленно по неаккуратности или забывчивости пользователей, вследствие нарушений политик корпоративной безопасности организаций. Более 40% информации ушло по Интернет-каналам, и 30% – по мобильным устройствам. Ежегодно более 65% информации утекает из коммерческих предприятий, около 20% из образовательных и 24 % из государственных предприятий.

Каналы утечки информации с точки зрения предотвращения инсайдерского инцидента достаточно разнообразны: мобильные накопители, Интернет (веб-почта, форумы), средства мгновенного обмена сообщениями (ICQ, MSN и др.), электронная почта, печатающие устройства, фотопринадлежности и другие.

Разумеется, при выборе решения для защиты ИТ-инфраструктуры от внутренних угроз компании, прежде всего, обращают внимание на перечень перекрываемых каналов утечки. Но, по мнению экспертов, единого решения, способного минимизировать абсолютно все внутренние риски, на сегодняшний день просто не существует. Именно поэтому для обеспечения всесторонней защиты специалисты ИБ выбирают многоуровневый подход, основанный на комплексном использовании DLP-решений.

В последнее время термин DLP (Data Loss/Leakage Prevention) стал очень популярным на рынке информационной безопасности, его одинаково часто используют вендоры и заказчики ИБ-решений. Согласно исследовательскому агентству Forrester Research, принадлежность того или иного решения к классу DLP-систем определяется следующими критериями:

- **Многоканальность.** DLP-решение должно охватывать максимальное количество каналов: e-mail, Web и IM, а также мониторинг файловых операций.
- **Унифицированный менеджмент**. Система должна обладать унифицированной консолью управления всеми компонентами, которых, как правило, насчитывают три: менеджмент-сервер (отвечает за хранение политик групп пользователей); устройство, которое отслеживает утечку через сеть; агенты для рабочих станций, серверов, файловых-хранилищ.
- **Активная защита**. Система должна не только предупреждать офицера безопасности о случившихся фактах утечки конфиденциальной информации, но должна давать возможность ее блокировать.
- **Классификация информации с учетом содержания и контекста**. Мониторинг фактов утечки конфиденциальной информации должен базироваться не только на содержимом пересылаемой информации, но также на контексте: какой используется протокол, какое приложение, от какого пользователя, куда и т.д.

Прежде чем рассмотреть производителей DLP-систем, представленных на российском рынке, следует дать краткое описание основных классов технических средств защиты от инсайдеров.

Системы выявления и предотвращения утечек

Решения Anti-Leakage Software (в некоторых источниках Anti Data Leakage) обеспечивают контентный анализ почтового и веб-тафика, контроль операций с

конфиденциальными документами, контроль мобильных носителей информации, принтеров и других каналов.

Одна из основных задач решений этого класса заключается в том, чтобы отслеживать локальные действия сотрудников с файлами и их сетевую активность. Так, например, в случае сохранения, печати или копирования конфиденциального документа на внешний носитель, система блокирует попытку несанкционированного действия и оповещает об этом сотрудника по безопасности. Также система осуществляет сканирование электронной корреспонденции и фильтрацию веб-трафика. Помимо разграничения прав работы с данными, решения класса Anti-Leakage Software осуществляют конспектирование операций с документами и приложениями, предоставляя на выходе консолидированные отчеты действий должностных лиц с конфиденциальной информацией.

Разумеется, эффективное внедрение средств защиты конфиденциальной информации невозможно без проведения мероприятий организационного характера: компании необходимо создать ряд документов, описывающих политику обращения с электронной конфиденциальной информации, проводить регулярные тренинги персонала. Политика должна описывать виды информации, хранящейся и обрабатываемой в информационной системе компании, присваивать каждому виду информации категорию конфиденциальности и определять правила работы ней.

Системы сильной аутентификации

Решения этого класса (аутентификация, авторизация, безопасное администрирование) служат в основном для защиты от несанкционированного доступа к данным. В их основе лежит двух- или трехфакторный процесс аутентификации. В первом случае сотрудник доказывает, что он знает пароль или PIN-код, предъявляет определенный персональный идентификатор (смарт-карту, электронный ключ или USB-токен). Во втором – пользователь предъявляет еще и третий тип идентификационных данных, например, биометрику.

Фактически, при использовании аппаратных средств аутентификации пользователь ставит свою электронно-цифровую подпись (ЭЦП) под всеми своими действиями, будь то отправка письма или копирование файла с сервера на мобильный носитель.

Предотвращение нецелевого использования IT-ресурсов

Данный класс решений способен целиком блокировать каналы утечек в строгом соответствии с политиками корпоративной безопасности. Системы позволяют запретить использование Internet-пейджеров; отправку вложений, защищенных паролями; пересылку файлов определенных форматов с проверкой по бинарной структуре файла; программы для удаленного управления и туннелирования трафика; SIP-телефонию (Skype); использование клиентов файлообменных сетей (P2P); передачу информации на внешние ftp-серверы и др. Подобные продукты фильтруют трафик HTTP и FTP, проверяют запрашиваемые страницы по базе URL, авторизует пользователей при доступе к сети и протоколирует все их действия. В некоторых случаях системы предотвращения нецелевого использования сетевых ресурсов могут иметь дополнительный функционал по фильтрации спама, многоуровневой защите от шпионского программного обеспечения, «троянов» и т.п.

Сегодня на глобальном IT-рынке существует не менее 10 крупных производителей, чьи DLP-продукты в своем большинстве являются результатами поглощений: Websense, поглотившая в свое время PortAuthority; McAfee – Onigma; RSA (EMC) – Tablus; Symantec – Vontu; Raytheon - Orchestria; Trend Micro – Provilla; IBM- Consul, Cisco – IronPort, InfoWatch, Verdasys и др.

В России в настоящий момент широко представлены InfoWatch, McAfee, Websense. В числе российских разработчиков на этот рынок также выходят компании S.N. Safe&Software и Perimetrix.

InfoWatch

Основной механизм распознавания конфиденциальной информации в продуктах InfoWatch - анализ содержания (на базе лингвистического «движка») и формальных атрибутов отправки. Решения InfoWatch предоставляют средства контроля сетевых сценариев утечки с использованием корпоративной почты и веб-соединения. Фильтрация данных осуществляется посредством универсального прозрачного прокси—сервера. В линейку продуктов InfoWatch также входит средство шифрования InfoWatch CryptoStorage, InfoWatch Traffic Monitor, предназначенный для мониторинга и анализа данных, и хранения теневых копий перехваченных данных, InfoWatch Device Monitor, обеспечивающий контроль над копированием конфиденциальных документов или их частей на сменные носители, контроль использования беспроводных протоколов IRDA и Bluetooth.

Websense

Решения компании Websense разработаны на базе запатентованной технологии «цифрового отпечатка» PreciseID, в рамках которой также поддерживаются методы идентификации на уровне правил, статистического анализа и словарей. Решение Websense Data Security Suite позволяет задавать пороговые значения количества пересылаемых записей, отслеживать отправку этой информации в теле, теме или во вложениях письма, контролирует все основные каналы передачи данных, включая исходящую и внутреннюю электронную почту, исходящий веб-трафик, ftp, HTTP, приложения обмена мгновенными сообщениями, сетевую печать, конечные компьютеры.

McAfee

В основе решения McAfee Host DLP лежит механизм тэггирования (установки меток) документов и снятия «цифровых отпечатков». Установленная на компьютер программа-агент контролирует все операции пользователя с конфиденциальной информацией, даже если ноутбук пользователя находится вне сети организации. Программное решение McAfee Host DLP осуществляет мониторинг и блокирование отправки информации через корпоративную почтовую систему, HTTP, FTP, системы передачи мгновенных сообщений, блокирует фрагментарное копирование или изменение защищаемого документа через clipboard и снятие экранной копии. Сегодня в линейку McAfee Data Protection включены также возможности по шифрованию данных и контролю внешних устройств.

S.N. Safe&Software

В основе ядра программы Safe’n’Sec Enterprise Suite - проактивные технологии поведенческого анализа и передовой разработки V.I.P.O. (Valid Inside Permitted Operations). На основе определенного списка правил поведенческий анализатор контролирует активность всех приложений в корпоративной сети и блокирует любые подозрительные действия сотрудников с конфиденциальной информацией. Решения Safe’n’Sec обеспечивают полномочное разграничение доступа пользователей к корпоративным ресурсам, постоянный мониторинг и контроль сетевой активности пользователей, контроль и анализ исходящего и входящего веб-трафика, теневого копирования данных, использование беспроводных протоколов Wi-Fi, IrDA, Bluetooth, программ мгновенных сообщений и др. Система фиксирует все сетевые события и создает консолидированный отчет с широкими возможностями фильтрации.

Perimetrix

В основе решений этой компании лежит концепция Secret Documents Lifecycle™, предполагающая защиту секретных документов на всех этапах жизненного цикла, мониторинг каналов коммуникаций, аудит электронных операций и каждого документа. Интегрированное решение Perimetrix SafeSpace, состоящее из пяти модулей, осуществляет настройку доступа пользователей к конфиденциальными данными, мониторинг защищённых рабочих станций и всех документов, покидающих сеть, автоматическую классификацию входящих и новых документов, а также хранение истории всех пользователей и каждого документа.