

Издание: Byte

Город: Москва

Дата публикации: 25 февраля 2008 г.



## Новый «крысолов» от InfoWatch

Сегодня корпоративных клиентов уже не нужно убеждать в актуальности проблемы защиты не только от внешних, но и от внутренних угроз. Сегодня на рынке можно найти десятки продуктов, в той или иной мере уменьшающих риск утечки информации через собственных сотрудников. Однако следует иметь в виду, что большинство таких средств контролирует один-два канала утечки и не позволяет организовать всестороннюю защиту.

Одно из комплексных решений для обнаружения и предотвращения утечки конфиденциальной информации — система InfoWatch Traffic Monitor. В канун 2008 г. (года Крысы по восточному календарю) его разработчик, компания InfoWatch ([www.infowatch.ru](http://www.infowatch.ru)), выпустила новую версию продукта — IW TM 3.0, способную решать следующие основные задачи:

- выявлять и предотвращать утечку конфиденциальной информации через каналы электронной почты и Интернет (в том числе Web-почту, форумы, чаты и т. п.);
- контролировать перенос информации на портативные устройства хранения (компакт-диски, дискеты, USB-устройства памяти и т. д.);
- предотвращать утечку информации через выводимые на печать документы;
- создавать единый архив электронной корреспонденции, распечатанных документов и файлов, записанных на внешние носители, с возможностью дальнейшего анализа.

InfoWatch TM 3.0 отслеживает операции вывода конфиденциальной информации из информационной системы компании (пересылка по корпоративной и Web-почте, публикация в Интернете, печать, копирование файлов на сменные носители и т. д.), в автоматическом и полуавтоматическом режиме блокируя подозрительные операции. Система хранит содержимое всех операций по выносу информации за пределы информационной системы по любому из перечисленных выше каналов, а также позволяет делать аналитические выборки для расследования случаев утечки данных. С централизованной консоли управления офицер ИТ-безопасности может контролировать работу всех компонентов решения, вести мониторинг действий пользователей, настраивать политику ИТ-безопасности и создавать статистические отчеты.

Архитектура комплексного решения InfoWatch Traffic Monitor 3.0 имеет распределенный характер и включает в себя ряд программных компонентов: ядро и различные перехватчики. Ядро

системы — хранилище информационных объектов и событий в системе, система централизованного управления перехватчиками и центральная консоль офицера ИТ-безопасности.

Перехватчик IW Web Monitor (IWWM) контролирует движение информации в Интернет, в том числе Web-почту, форумы и чаты. IWWM сканирует исходящий Интернет-трафик, выделяет подозрительный и запрещенный к отправке через эти каналы контент, блокирует пересылку информации, которая содержит или может содержать конфиденциальные данные. Перехватчик реализован в двух архитектурах: Transparent Proxy и модуль plug-in для сервера Microsoft ISA.

Перехватчик IW Mail Monitor (IWMM) предназначен для предотвращения утечки информации через корпоративную почтовую систему. IWMM сканирует почтовый трафик (текст электронных сообщений и вложенные файлы) и блокирует пересылку корреспонденции, которая содержит или может содержать конфиденциальные данные. Перехватчик реализован в двух архитектурах: SMTP-Gateway и модуль plug-in для сервера Lotus Notes.

Перехватчик IW ICQ Monitor (IWIM) в режиме реального времени сканирует трафик обмена информацией через ICQ, и при выявлении конфиденциального контента может блокировать передачу данных. Перехватчик реализован в архитектуре Transparent Proxy.

Перехватчик IW Device Monitor (IWDM) контролирует действия пользователей с отчуждаемыми устройствами хранения информации. Он позволяет организовать использование портативных устройств хранения информации и коммуникационных портов, а также передавать на анализ ядру системы содержание копируемых на сменные носители файлов. Перехватчик реализован в виде агента на рабочей станции.

Перехватчик IW Print Monitor (IWPM) выполняет мониторинг документов выводимых на печать, и при обнаружении конфиденциальных данных может блокировать распечатку документа. Перехватчик реализован в виде виртуального принтера.

Система поставляется в виде ядра и минимум одного перехватчика. Все перехватчики передают информационные объекты в ядро системы для атрибутивного и контентного анализа, на основании которого выполняется заранее определенный сценарий — пропуск информации, ее блокирование, оповещение офицера безопасности, помещение в карантин и т. д. Хранилище информационных объектов и событий, составляющее часть ядра системы, накапливает информацию о событиях, инцидентах и маршрутах перемещения конфиденциальных данных, покидающих корпоративную сеть. Тем самым обеспечивается ведение протокола операций с чувствительной информацией, что является необходимым требованием большинства законодательных норм и стандартов.

Обработку информации, накопленной хранилищем, выполняет сервер отчетов. С его помощью можно создать широкий диапазон как стандартных, так и настроенных офицером ИТ-безопасности отчетов. Рабочее место офицера безопасности представляет собой консоль управления, функционирующую через обычный Web-браузер, на которую поступают оповещения о нарушении политики внутренней безопасности. Интеграция ядра системы с Active Directory обеспечивает единую идентификацию пользователей, выполнивших действие с информационным объектом независимо от канала, по которому оно было перехвачено.

В силу многомодульного характера IW TM 3.0 требования к аппаратному обеспечению формулируются для каждого компонента решения отдельно и зависят от объема информационных потоков, а также от объема хранимой информации. Неотъемлемая часть комплексного

решения IW ТМ 3.0 — сопроводительные и консалтинговые услуги, а также техническая поддержка, включая поставки дополнительных функций продукта по подписке. Кроме того, необходимо упомянуть услугу помощи заказчику в создании адекватной нормативной базы (в том числе модификаций трудовых договоров), а также в обучении менеджмента и персонала.

<http://www.bytemag.ru/articles/detail.php?ID=9188>