

Эффективность DLP-систем: на стороне заказчика



Об эффективности, особенностях внедрения и работе с DLP-системами, а также о новой версии продукта InfoWatch Traffic Monitor Enterprise 3.5. рассказал Рустем Хайретдинов, заместитель генерального директора компании InfoWatch.

– Насколько эффективны сегодня решения по предотвращению утечек информации?

– Если говорить о полноценной DLP-системе, контролирующей

все возможные каналы передачи информации, а не часть из них, то после должной настройки предотвращается 100% случайных утечек и некоторая часть умышленных.

Согласно общемировой статистике, доли случайных и умышленных утечек колеблются в районе 50/50 ±15%. В целом же эффективность противодействия злоумышленным инсайдерам сильно зависит от квалификации этих злоумышленников относительно квалификации службы информационной безопасности. Когда человек борется против человека, то уровень техники играет не основную роль. Мозг тут важнее компьютера.

С другой стороны, практика показывает, что эффективность систем, развернутых на предприятиях, измеряется не только количеством отловленных утечек, но и деньгами. Если компанию устраивает то, как хранится и обрабатывается конфиденциальная информация, значит система эффективна. Эффективность собственно программного обеспечения сильно зависит от того, как им пользоваться – можно неэффективно пользоваться хорошей системой, а можно эффективно – плохой.

Здесь необходимо учитывать, насколько точно прокатегорированы данные в компании, как категории присваиваются новым и входящим документам, как формализованы критерии легитимности передачи конфиденциальных

данных, как эффективно действует система поощрений и наказаний за соблюдение правил обращения с конфиденциальной информацией и т.д. Часто сам факт наличия в компании системы защиты от утечек информации, ставший достоянием гласности, уже эффективен – большинство сотрудников будет внимательнее относиться к передаче конфиденциальных данных.

Если же говорить об эффективности конкретного ПО на тестовом стенде, то независимых тестов типа Virus

– Существуют ли на сегодняшний день какие-либо критерии оценки эффективности DLP-систем?

– Система противодействия утечкам на предприятиях – сложный комплекс организационно-технических мер. В него входят регламенты и традиции обращения с конфиденциальными данными, правильно организованная информационная система, принципы работы с персоналом, специализированное программное обеспечение и система поддержки внутренних рассле-

Для того чтобы эффективно использовать многолетний опыт борьбы с утечками, реализованный в программном обеспечении DLP-систем, компаниям придется принять то, что существенная часть работы по обеспечению защиты от утечек должна быть сделана на стороне заказчика, поскольку никто лучше его не знает собственных информационных потоков.

Bulletin пока не проводилось. Если бы такие тесты существовали, то также не давали бы объективной информации для клиентов – если у всех атакуют одни и те же вирусы, то структура трафика у каждого предприятия своя. Факт, например, что один продукт ловит 3000 форматов файлов, а другой всего 100, практически не означает ничего для большинства компаний, поскольку реально в компаниях используется не более 30 форматов.

Для того чтобы эффективно использовать многолетний опыт борьбы с утечками, реализованный в программном обеспечении DLP-систем, компаниям придется принять то, что существенная часть работы по обеспечению защиты от утечек должна быть сделана на стороне заказчика, поскольку никто лучше его не знает собственных информационных потоков.

дований. Поэтому сложно оценивать систему по одному из элементов, когда их несколько. Как правило, составляется набор процедур и политик, вытекающий из стандартов по ИБ, лучших практик, специфики ситуации и ценности защищаемой информации.

Для количественной оценки необходима статистика, а внутренние угрозы устроены так, что за редким исключением об успешных утечках никому не становится известно. Поэтому иногда за критерий эффективности принимается доступная информация – например, данные о попытках случайных утечек – сколько раз человек вставил флешку и попытался на нее что-то записать, сколько раз пытался послать документ по недопустимому адресу и т.д. Ведь DLP-система в режиме блокирования показывает такие попытки. Но это самый точный способ, поскольку сам факт наличия DLP останавли-

Думать, что DLP-решение все сделает само, было бы ошибкой, и слоганы "внедрение за один день", "включил и забыл" здесь неуместны. Необходимо понять, что в компании конфиденциально, а что нет, какую информацию по каким каналам куда можно передавать.

ваек многих инсайдеров, таким образом, многие предотвращенные инциденты остаются в альтернативной реальности и никак не фиксируются.

– Что стоит учитывать при организации и использовании таких систем?

– Если внимательно изучить то, как используются российскими компаниями продукты для защиты от утечек, то можно увидеть, что собственно именно с утечками никто не борется. Большинство компаний не обладает сегодня квалификацией и инструментами для динамической категоризации корпоративного контента, поэтому в большинстве случаев точно не могут определить, является ли перемещение информации утечкой или нет. Думать, что DLP-решение все сделает само, было бы ошибкой, и слоганы "внедрение за один день", "включил и забыл" здесь неуместны. Необходимо понять, что в компании конфиденциально, а что нет, какую информацию по каким каналам куда можно передавать.

Стоит также учесть, что собственно продукт – не основной элемент системы защиты от утечек на предприятии, хотя его приобретение зачастую становится катализатором изменений и в архитектуре информационной системы, и в организационной и юридической практике и в работе с кадрами. Иногда заказчики просто недооценивают затраты на поддержание и настройку DLP-системы, поскольку ей требуется постоянный "ручной" анализ и пересмотр поисковых образцов при изменении обстоятельств бизнеса (например, при открытии нового проекта).

Организационная поддержка со стороны заинтересованного подразделения и одного из влиятельных руководителей – важное условие для внедрения контроля утечек. Как и всякое средство безопасности, DLP-система создает дополнительные неудобства для рядовых сотрудников. Если результат никому, кроме начальства, не нужен, одни начнут обходить средства контроля, а другие – закрывать на это глаза. В результате любая безопасность превращается в формальность.

Также необходимо помнить, что DLP-система сама по себе находится в рамках закона, она не является ни вредоносной программой, ни специальным техническим средством для негласного получения информации. Однако ее неаккуратное применение легко приводит к нарушению конституционных прав на тайну связи и тайну частной жизни. Поэтому как

общения. Таким образом, можно отследить все действия конкретного сотрудника (если он, например, попал под наблюдение): какие файлы он копировал на съемные носители, какие отправлял по почте или ICQ, что распечатывал или публиковал в Интернете.

Функция зон ответственности, реализованная в продукте, позволяет разграничить доступ

InfoWatch Traffic Monitor Enterprise 3.5. позволяет осуществлять единую идентификацию пользователей, независимо от того какой канал был использован для отправки сообщения.

внедрение, так и эксплуатация DLP требует солидной юридической "подложки", пересмотра некоторых нормативных документов компании, обучения пользователей.

– Ваша компания недавно выпустила новую версию продукта InfoWatch Traffic Monitor Enterprise 3.5. Каковы его основные особенности и преимущества?

– InfoWatch Traffic Monitor Enterprise 3.5. – решение для крупных компаний и корпораций, позволяющее полностью контролировать информационные потоки организации, точно понимать, какие данные являются конфиденциальными, где и как они хранятся, а также как передаются и кто их использует.

В новой версии InfoWatch Traffic Monitor Enterprise существенно доработана интеграция с Active Directory, что дает возможность автоматически импортировать карточки сотрудников и списки групп пользователей. Для каждого сотрудника в системе возможно создать (или автоматически импортировать из Microsoft Active Directory) карточку, которая будет содержать его личные данные и контактную информацию, например адрес корпоративной электронной почты, UIN в любой системе обмена мгновенными сообщениями, адрес его личной электронной почты и другие параметры. Это существенно облегчает настройку продукта и делает его эксплуатацию более удобной.

InfoWatch Traffic Monitor Enterprise 3.5. позволяет осуществлять единую идентификацию пользователей, независимо от того какой канал был использован для отправки со-

общения. Таким образом, можно отследить все действия конкретного сотрудника (если он, например, попал под наблюдение): какие файлы он копировал на съемные носители, какие отправлял по почте или ICQ, что распечатывал или публиковал в Интернете.

Функция зон ответственности, реализованная в продукте, позволяет разграничить доступ к событиям, связанным с сотрудниками этого подразделения и ограничить доступ к другим событиям.

В InfoWatch Traffic Monitor Enterprise 3.5. расширены возможности поиска: благодаря введению личных карточек сотрудников теперь можно осуществлять поиск по большому количеству критериев, что обеспечивает большую точность и гибкость поиска.

Благодаря техническим доработкам монитора ICQ в новой версии продукта улучшен мониторинг и анализ ICQ-трафика, отправляемого по протоколу HTTP, включая возможность перехвата файлов.

Новая версия InfoWatch Traffic Monitor Enterprise позволяет также анализировать информацию, отправляемую с помощью функции SMS-over-ICQ (SMS-сообщения, отправляемые через систему обмена сообщениями ICQ).

За счет дополнительной оптимизации работы ряда сетевых компонентов примерно в 2 раза увеличена производительность новой версии продукта. Кроме того, пользовательский интерфейс консоли управления стал более удобным, дружелюбным и современным. ●

DLP-система создает дополнительные неудобства для рядовых сотрудников. Если результат никому, кроме начальства, не нужен, одни начнут обходить средства контроля, а другие – закрывать на это глаза. В результате любая безопасность превращается в формальность.

ИИИ

**АДРЕСА И ТЕЛЕФОНЫ
компании INFOWATCH
см. стр. 68**