УДК 004.056.5

студентка О.И. Авчинникова
ГВУЗ «Национальный горный университет»

ОБЗОР СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОТ ВНУТРЕННИХ УГРОЗ

Рассмотрены тенденции в области распространения угроз ИТ, а также характеристики, которым должна соответствовать система защиты конфиденциальных данных от внутренних угроз.

В настоящее время количество внутренних угроз и ущерб, наносимый ими, гораздо превышает соответствующие показатели внешних угроз. Динамика роста утечек информации в 2010 году в сравнении с предыдущим годом изменилась не существенно, однако, отмечен значительный рост среднего размера ущерба от утечки [3]. Среди причин столь широкого распространения внутренних угроз ИТ можно выделить следующие: отсутствие установленной ответственности за приводящие к ним нарушения, легальность и простота доступа инсайдера к информации, высокая стоимость средств защиты, несовершенство политики безопасности, широкий спектр возможных каналов передачи краденой информации и сложности в организации их контроля, недостаток полномочий у CISO (Chief Information Security Officer) – руководителей подразделений ИБ, недостаточная информированность руководителей предприятий и др.

Системы DLP (Data Loss Prevention или Data Leak Prevention) или иначе системы защиты конфиденциальной информации от внутренних угроз получают все большее распространение в связи с ростом количества угроз данного типа. Под внутренними угрозами понимаются злоупотребления (намеренные или случайные) со стороны сотрудников организации, имеющих легальные права доступа к данным, соответствующим их полномочиям [2].

Исследовательское агентство Forrester Research предложило четыре критерия которым, по их мнению, должна соответствовать DLP система [2]:

1. Многоканальность. Система должна быть способна осуществлять мониторинг нескольких возможных каналов утечки информации (запросы к

базе данных, почтовый трафик, обмен мгновенными сообщениями, файловые операции, работа с буфером обмена данными на рабочих станциях).

2. Унифицированный менеджмент. Система должна обладать унифицированными средствами управления политикой информационной безопасности, анализом и формированием отчетов о событиях по всем каналам мониторинга.

3. Активная защита. Система должна не только уметь обнаруживать факт нарушения политики безопасности, но и при необходимости принуждать к ее соблюдению. К примеру, блокировать подозрительные сообщения.

4. Учет, как содержания, так и контекста. В процессе мониторинга документов, циркулирующих по возможным каналам утечки информации, необходимо учитывать не только ключевые слова и регулярные выражения, встречающиеся в них, но и общее содержание. Учет контекста должен выражаться в дополнительном рассмотрении типа приложения обращающегося к документу, протокола передачи, активности, отправитель, получателя и др.

На примере продукта InfoWatch Traffic Monitor Enterprise от компании InfoWatch, являющегося DLP-системой и предоставляющего защиту корпоративной информации от утечки или несанкционированного распространения, рассмотрим возможности, которыми обладают данные системы.

Мониторинг и фильтрация. Осуществляет мониторинг и фильтрацию трафика, передаваемого по протоколам SMTP, HTTP, HTTPS, протоколу обмена мгновенными сообщениями. Позволяет предотвратить случайную или умышленную утечку данных, обеспечивая контроль копирования данных на съемные носители или отправку их на печать. Выполняет снятие копии с обнаруженных документов и отправляет для анализа на сервер. Помимо этого предоставляет возможность извлекать текстовую информацию из графических файлов.

Анализ и принятие решений. Изначально анализирует перехваченные данные по формальным атрибутам, затем выполняет конкретный анализ

содержимого. Основываясь на полученных данных и правил политики безопасности, принимает решение о блокировке или продолжении выполнения операции. В случае нарушения политики безопасности сотруднику службы ИБ предоставляется подробная информация о происшествии, но без прямого доступа к содержимому файла или сообщения. Благодаря чему деятельность ведется с соблюдение права сотрудников на тайну переписки.

Хранение и ретроспективный анализ данных. Перехваченные данные сохраняются в централизованном архиве. Время хранения данных не ограничено, что позволяет полностью проследить историю всех операций сотрудников с конфиденциальными данными, и предоставляет возможность мониторинга их текущей активности (оперативные запросы) и составления подробных статистических отчетов.

Перечень литературы:

1. InfoWatch Traffic Monitor Enterprise. Контроль над конфиденциальной информацией – важная задача бизнеса, 3-4.

2. DLP – что это значит. http://www.pcweek.ru/security/article/detail.php?ID=109716.

3. Глобальное исследование утечек за 2010 год. http://www.infowatch.ru/analytics/reports/462.