УДК 004.056.53

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ С ПОМОЩЬЮ DLP-СИСТЕМ

Гержан Сергей Геннадиевич, Масальская Елена Александровна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: 825800@mail.ru

В данной работе рассмотрены системы предотвращения утечки данных, их принцип работы, а также описаны основные преимущества данных систем в сравнении с остальными существующими средствами предотвращения утечек.

Ключевые слова – DLP-система, предотвращение утечки данных, безопасность информации.

ВВЕДЕНИЕ

Для борьбы с утечками данных используются различные средства защиты, однако, наибольшее развитие в последнее время получила технология DLP (Data Leakage Prevention – предотвращение утечки данных). Основное назначение DLP – обеспечивать защиту от случайного или намеренного распространения конфиденциальной информации со стороны сотрудников, имеющих доступ к информации в силу своих должностных обязанностей [1].

ЗАДАЧИ DLP-СИСТЕМ

Основными задачами систем защиты от утечек являются:

- получение описания защищаемых данных (настройка системы);
- распознавание защищаемых данных в потоке, исходящем из внутренней информационной сети компании вовне (распознавание действий, направленных на перемещение конфиденциальных данных);
- реагирование на обнаруженные попытки (формирование доказательной базы для расследования инцидентов) [2].

В первую очередь следует определить данные, перемещение которых будет контролироваться системой, "предъявить" их системе с использованием методов, описанных выше, и выявить ее реакцию на обнаруженные инциденты. Важны также и параметры реакции на инцидент – предполагает ли она блокирование какой-либо операции: отправка электронного письма, создание экранной копии защищаемого документа, запись данных на USB-накопитель. Независимо от блокирования, практически всегда в журнал системы заносится максимально подробная предметная информация об инциденте [3]. Необходимо также описать правила информирования об инциденте:

- сотрудника подразделения, отвечающего за обеспечение информационной безопасности;
- лица, являющегося владельцем информации;
- самого подозреваемого в попытке организации утечки.

В случае противодействия утечкам с использованием сетевого сценария, DLP-система позволяет осуществлять перехват (блокирование) или зеркалирование (только аудит) отправки, проводить анализ содержания отправки в соответствии с используемыми механизмами контроля (рис.1). Затем при обнаружении подозрительного содержания происходит информирование ответственного сотрудника, а детали инцидента заносятся в журнал системы. Отправка может быть приостановлена, если схема подключения DLP-модуля позволяет это сделать [4]. Большинство DLP-систем предполагает осуществление повторной доставки задержанных ранее сообщений. Назначенный сотрудник оценивает, насколько адекватным был вердикт системы и, если тревога оказывается ложной, вручную отдает команду провести отправку задержанного сообщения.

Рисунок 1. Механизм контроля

ОСОБЕННОСТИ DLP-СИСТЕМ

Основные практические достоинства DLP:

- способны классифицировать и выделять наиболее важные для защиты данные (развитые механизмы анализа содержимого);
- приспособлены для тотального охвата информационных потоков организации (множество отслеживаемых каналов, развитая система обработки инцидентов, гибкое распределение ролей);

подстраиваются под существующие бизнес-процессы (эффект от использования DLP достижим без организационных преобразований и увеличения штата). Система DLP будет просматривать все информационные потоки и информацию, выводимую на сменные устройства записи, будет обнаруживать конфиденциальные данные в потоках и активно реагировать на обнаруженные попытки распространения конфиденциальной информации

Основные недостатки DLP-систем:

- не содержат встроенных средств шифрования;
- методы классификации данных, используемые в DLP и подходящие для глобального охвата всех обрабатываемых ресурсов, могут пропустить те данные, которым система не была обучена.

ВЫВОДЫ

Применение DLP-систем рекомендуется для организаций, которые ведут активный обмен документами с внешними контрагентами, а при этом стоит задача обеспечения конфиденциальности этого процесса. Например, из медицинского учреждения не сможет беспрепятственно произойти утечка историй болезней сразу сотни человек частному лицу, из банка – баз кредитных карт и персональных данных клиентов. По результатам перемещений конфиденциальных данных ведется подробная статистика с возможностью отслеживания соответствия требованиям действующих стандартов безопасности. Для повышения эффективности работы системы следует совместить использование в едином программном комплексе, методов DLP и шифрования данных, а также адаптировать методы обучение системы.

Обучение системы осуществляется:

- вводом образцов конфиденциальной информации, разбитой по категориям (обычно организация указывает, в каких рабочих папках на серверах находятся массивы документов) для снятия цифровых отпечатков;
- вводом выгрузок из актуальных баз данных для снятия отпечатков баз данных;
- включением существующих заведенных в системе шаблонов политик обнаружения (например, номеров кредитных карт, номеров российских паспортов, ключей активации программных продуктов, реагирования на отправку зашифрованных вложений);
- вводом собственных слов и выражений, характерных для конфиденциальных данных;
- вводом исключений (например, шаблоны договоров).

Объединение методов шифрование и DLP-систем позволяет контролировать информацию, покидающую пределы корпоративной сети, защитить серверные хранилища и съемные носители, которые физически могут попасть в руки посторонних лиц. Таким образом, шифрование может существенно расширить возможности DLP-систем и снизить риски утечки конфиденциальных данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Предотвращение утечек информации (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/dlp

2. Как работают DLP-системы: разбираемся в технологиях предотвращения утечки информации (Электрон. ресурс) / Способ доступа: URL: http://www.xakep.ru/post/55604/

3. DLP-Lite (Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/post/150227/

4. Обзор DLP систем (Электрон. ресурс) / Способ доступа: URL: http://www.itsec.ru/articles2/techobzor/obzor-sistem-dlp-v-chem-raznica