В чем кризис DLP-технологий?

Евгений Шемчук, *инженер ООО "НТЦ "Вулкан"*

По результатам различных исследований количество попыток кражи информации увеличивается с каждым годом, растет и число успешно реализованных краж, а также качество подхода к их реализации. Так как доля "простых утечек", связанных с неопытностью пользователей и/или отсутствием базовых политик безопасности, достаточно велика, не вызывает сомнения, что в современной компании применение DLP-систем (от англ. Data Leak/Loss Prevention) является необходимостью, а не роскошью.
Однако давайте подумаем, способна ли DLP как технология избавить конечного заказчика от утечек информации? И в чем/где назрел кризис у данной технологии?

Честно можно сказать, что DLP не является и не может являться панацеей от инсайдеров. И в данном случае термин DLP надо понимать не как решение по предотвращению утечек информации, а как решение, призванное уменьшить риски, связанные с утечкой информации.

Проблема терминологии

Существуют достаточно эффективные способы кражи информации, где применение DLP никоим образом не может спасти владельца этой информации. Речь идет о таких способах, как фото- или видеосъемка, запись на лист бумаги или, наконец, использование собственной памяти. DLP-систем, которые в ближайшем будущем смогут спасти от последнего, не предвидится просто в силу того, что подобного рода способы кражи информации не охватывают сферу их влияния. Поэтому нужно четко представлять, на какие каналы утечек распространяется действие DLP.

Возможности DLP-системы не безграничны

Действительно, современные DLP-системы могут контролировать множество каналов утечки информации: публикация на Web-ресурсы, в социальные сети, передача по электронной почте или с использованием различных мессенджеров, вывод на печать, копирование на съемные носители и т.д.

Но процесс реализации контроля над новыми каналами утечек осуществляется медленнее, чем хотелось бы. Количество возможных каналов утечек все еще значительно превышает реализованный функционал даже у самых продвинутых DLP-систем.

В связи с этим практически всегда можно найти канал утечки, используя который, можно беспрепятственно выгрузить необходимую информацию. Например: хотя контроль "Mail.Ru Агент" (протокол MMP) и заявлен у многих DLP-вендоров, контроль же голосового общения через "Mail.Ru Агент" не реализован. То же можно сказать про многие мессенджеры, поддерживающие передачу голоса. А ведь есть еще видеоканал передачи данных, который также не контролируется.

DLP весьма комфортно себя чувствует с текстовой и графической информацией за счет применения таких технологий, как сигнатурный анализ (словари), морфологический анализ, регулярные выражения, цифровые отпечатки и оптическое распознавание текста (OCR), с аудио и видео же – пока нет. Хотя определенные успехи в области контроля аудио наметились (например, производители DLP-решений научились записывать аудиотрафик с некоторых мессенджеров). Осталось лишь добавить в DLP-системы модуль преобразования речевого сигнала в текстовый.

Но нужно не забывать про развитие (обновления) контролируемого ПО, которое может "поставить в тупик" работающее с предыдущей версией ПО DLP-решение.

В итоге получается, что контролируется много, однако еще многое нужно сделать.

DLP-системы можно обойти

Как уже писалось выше, производители DLP-систем недостаточно полно охватывают различные каналы утечки информации. Вместе с тем существуют эффективные методы обхода DLP-систем, о которых наша компания неоднократно писала ранее [1, 2]. Поэтому, наряду с контролем новых каналов утечек, производителями DLP-решений вводятся технологии по борьбе с некоторыми методами обходов механизмов контроля.

Если же делать "срез" на текущий момент, то можно сказать, что в современных DLP-системах решены в большей степени проблемы, связанные с кодировками, метаданными и расширениями контролируемых файлов, а также с самозащитой DLP-агентов.

Но в меньшей степени с:

- передачей данных в графических файлах (т.к. при добавлении "шумов" в такие файлы уменьшается число положительных срабатываний);
- шифрованными файлами (т.к. не на все типы шифрованных файлов идет однозначное оповещение).

Из других методов обхода до сих пор хорошо "работают": стеганографические приемы, маскирование сетевого трафика, побитовое копирование и т.д.

В зависимости от используемого DLP-решения, а со временем всегда возможно узнать, какое решение внедрено в конкретной компании, можно подобрать наиболее эффективный способ, посредством которого трафик и/или файлы будут пропущены.

В связи с этим методы обхода DLP – это серьезная проблема, требующая большого внимания со стороны разработчиков.

Легко и дешево. Сложно и дорого

Заслуживает внимания тот факт, что провайдеры Web-сервисов стали чаще использовать шифрование (HTTPS), что несколько усложняет работу DLP (необходимо организовать "разбор" такого трафика на прокси-сервере с последующей передачей его на сетевую часть DLP или повсеместно использовать "агенты"). И в первом, и во втором случаях также необходимо настроить исключения из перехвата шифрованных ресурсов (например, системы клиент-банк, сайты электронных торговых площадок и т.д.). Все это так

или иначе предъявляет более высокие требования к данным решениям, к сетевой ИТ-инфраструктуре, а также к инженерам по внедрению, что, несомненно, скажется в большую сторону на итоговой стоимости всего DLP-проекта и на времени ввода DLP-системы в эксплуатацию.

DLP-системы – это место аккумуляции критичной информации

В силу того, что в DLP-системе скапливается большое количество чувствительной информации, как минимум часть в виде теневых копий, логичным будет вывод, что "местом утечки" может быть сама DLP-система. Будь то персонал, занимающийся администрированием системы (инсайдер), или злоумышленник, получивший доступ к DLP несанкционированно.

Векторами атак на DLP-системы могут быть:

- модули и компоненты ОС, на которой функционирует DLP;
- сторонние модули и библиотеки, используемые в DLP (OCR-модули, СУБД, и т.д.);
- непосредственно компоненты самой DLP.

В особенности подобные атаки становятся актуальными в эпоху четырех цифровых "всадников Апокалипсиса" (Heartbleed, Shell-Shock, Winshock и Kerberos), при условии, что вышеперечисленные компоненты DLP-систем не обновляются или обновляются несвоевременно, а к сожалению, на практике Patch Management далеко не всегда покрывает зону средств защиты информации и уж особенно сертифицированных по требованиям безопасности информации. И получается, что, с одной стороны, DLP предотвращает утечки информации по одним каналам, а с другой – открывает новые "пути входа" для доступа к чувствительной информации.

Поэтому важно помнить как минимум о регулярных обновлениях ИТ-инфраструктуры, к которой относится и DLP.

А со стороны разработчиков необходимо применять методы защищенного программирования и углубленного тестирования на ошибки и уязвимости.

Шпионские "игры"

С учетом вышесказанного ставится понятно, что DLP – это лакомый кусок не только для злоумышленника, но и для различных спецслужб. В особенности такие выводы напрашиваются после громких разоблачений Э. Сноудена, выделения компании Websense в совместное с Raytheon предприятие, развития промышленного шпионажа на уровне государств и т.д.

Таким образом, все эти моменты добавляют ложку дегтя в DLP-бочку меда.

С точки зрения заказчика, если он покупает DLP-систему, а это решение по предотвращению утечек критически важной для него информации, на выходе он должен получить именно предотвращение утечек.

Резюмируя

- DLP не оправдывают в ряде случаев ожиданий заказчиков, т.к. требуются дополнительные, сторонние решения в области защиты информации;
- DLP до сих пор не способны контролировать все актуальные именно для класса DLP каналы утечки информации;
- DLP недостаточно защищены от различного рода уязвимостей проектирования и программирования (а их число все растет и растет);
- DLP сами несут риски, связанные с утечкой информации (ввиду уязвимостей, неправильной настройки, некорректного доступа обслуживающего персонала DLP к данным и т.п.);
- DLP далеко не всегда способны самостоятельно контролировать все чаще используемый HTTPS-трафик;
- DLP до сих пор не в полной мере способны противодействовать доступным для рядовых пользователей методикам обхода;
- DLP не гарантируют отсутствия "потайных механизмов" доступа к информации для различных третьих лиц;
- DLP обладают высокой стоимостью владения и внедрения.

Все вышесказанное постепенно привело к кризису DLP-технологии, из которого, конечно, можно выйти, делая упор на минимизацию вышеперечисленных замечаний, а также применяя комплексный и сбалансированный подход в рамках защиты информации в организации. ●

Литература

1. Кузнецов А. Защита от утечек данных: Комплексная терапия // Information Security. – 2012. – № 3. – С. 28–29.

2. Кузнецов А., Товстолип А. DLP-система как объект… атаки // Information Security. – 2013. – № 3. – С. 16–17.