DLP на страже информации

Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*
Роман Ванерке, *руководитель отдела технических решений АО "ДиалогНаука"*

Информация – та самая точка опоры, с помощью которой можно перевернуть мир. Это стало очевидно после публикаций Эдварда Сноудена, Панамского досье, переписки Демократической партии США. Другими словами, в современном мире есть информация, которая обладает особой ценностью – ее легко потерять, но сложно приобрести. Кроме этого, есть еще и требования законодательства по защите различных типов информации – персональные данные, банковская тайна, коммерческая тайна и т.п. Если компания работает с такого рода информацией, ей очень важно не допустить утечек ценных сведений. В противном случае компании может быть нанесен значительный финансовый и репутационный ущерб.

Построение эффективной системы защиты от утечки конфиденциальной информации базируется на комплексе организационных и технических мер. Прежде всего служба информационной безопасности должна определить, что относится к конфиденциальной информации, определить критерии отнесения информации к тому или иному типу, а также владельцев такой информации.

Актуальность защиты от утечек информации усиливается по мере развития и использования информационных технологий – ценность информации возрастает, а доступность и мобильность информации увеличивается. В результате компаниям, которые обладают подобной информацией, приходится прилагать немало усилий по защите ее от утечки. К счастью, производители средств защиты разработали специальный класс продуктов – Data Loss Prevention (DLP), который и предназначен для предотвращения утечки конфиденциальной информации.

Каналы утечек

Чтобы предотвратить утечку, нужно сначала определить модель предполагаемого нарушителя. Для этого необходимо в том числе проанализировать информационную систему с целью выявления возможных каналов передачи нарушителем данных за пределы периметра безопасности. Наиболее частыми каналами утечек являются следующие.

Электронная почта

Сервис корпоративной электронной почты на сегодняшний день является основой для построения документооборота внутри любой компании. При этом пользователи могут случайно ошибиться, нажать не ту кнопку при выборе адреса получателя, и конфиденциальная информация случайно будет отправлена на посторонний адрес. Кроме того, электронная почта предоставляет возможность передавать файлы любого формата и размера, что и позволяет использовать ее в качестве возможного канала утечки.

Интернет-доступ

Протоколы доступа к сети Интернет используются в основном для получения информации из сети, однако они также могут использоваться в различных сервисах, таких как Web-почта,Web-архив хранения данных, заметки, календари и справочники Google и многих других Web-сервисов, которыми можно пользоваться как через Web-браузер, так и на мобильном устройстве. Пользователи применяют эти сервисы для синхронизации данных между различными своими устройствами, однако в результате таких действий конфиденциальная информация может покинуть границы контролируемого периметра.

Рабочая станция/мобильные устройства/носители

Достаточно часто компании предоставляют своим сотрудникам удаленный доступ к корпоративной сети с помощью мобильных устройств, используют в рабочем процессе различные мессенджеры или же дают возможность записывать информацию на внешние носители. Кроме того, на "удаленке", как правило, работают приложения для связи со сторонними сервисами, с помощью которых конфиденциальные данные также могут "утечь" за пределы корпоративного периметра контроля, или обычный архиватор, который позволит зашифровать архив. Здесь уже блокировать сторонние сервисы и обеспечивать контроль оказывается непросто – необходим специальный агент на мобильном устройстве, который будет следить за действиями пользователей и блокировать сохранение конфиденциальных данных вовне. Целесообразно также шифровать информацию на устройстве и внешних носителях, чтобы исключить простое воровство носителя и устройства – за пределами корпоративного периметра ценная информация должна быть зашифрована.

Печать

Еще один достаточно популярный канал утечек – печать. Информация из корпоративной сети просто распечатывается и уносится с собой. При этом документы могут выводиться на печать как на локальном, так и на сетевом принтере.

Конечно, есть и другие каналы утечек, такие как побочное электромагнитное излучение, фотографирование экрана компьютера на камеру личного телефона, ксерокопирование экрана монитора, начитывание текста на диктофон или через телефон – к сожалению, любой злоумышленник может придумать новые способы организа-

ции утечек. Математически доказано, что всегда найдутся способы скрытой передачи данных через защищаемый периметр. Однако пользоваться экзотическими способами достаточно сложно и объем информации, которую таким образом можно будет получить, окажется не очень большим.

Методы защиты

Построение эффективной системы защиты от утечки конфиденциальной информации базируется на комплексе организационных и технических мер. Прежде всего служба информационной безопасности должна определить, что относится к конфиденциальной информации, определить критерии отнесения информации к тому или иному типу, а также владельцев такой информации, например, посредством ввода режима защиты коммерческой тайны на предприятии в соответствии с российским законодательством. Далее необходимо провести классификацию информации по уровню значимости данных – это позволит правильно расставить приоритеты при ее защите. После этого необходимо локализовать места, где конфиденциальная информация хранится, куда она может передаваться, а где ее не должно быть. В идеальной ситуации – заранее определить централизованные места хранения защищаемой информации, поскольку это также позволит реализовать аудит доступа к защищаемой информации (всегда полезно иметь такую информацию, как при регулярном аудите, так и при проведении расследований). Тогда есть возможность определить правила управления конфиденциальной информацией, ее поиска и защиты.

С технической точки зрения DLP-система должна иметь возможность выявлять факты утечки при передаче информации по коммуникационным каналам, а также во время хранения и обработки данных. Основные методы обнаружения утечек, которые сейчас используются в различных системах, следующие.

Ключевые слова и регулярные выражения

Для наиболее общих случаев предотвращения утечки конфиденциальной информации вполне возможно определить поиск по ключевым словам или описать такую информацию с помощью регулярных выражений. В частности, этот метод можно использовать для предотвращения утечек паспортных данных, сведений о кредитных картах, договорах и других хорошо формализованных документов. При этом можно выстраивать достаточно сложные методы принятия решений о секретности документа по ключевым словам, определяя веса для слов, сочетаний и частоту их использования в документе. Если на предприятии введен режим коммерческой тайны, то конфиденциальные документы стоит помечать специальной меткой, например "конфиденциально", по которой можно будет в дальнейшем осуществлять поиск.

Цифровые отпечатки или сигнатуры

Для снятия цифровых отпечатков DLP-системе необходимо указать, какие именно документы или таблицы базы данных являются конфиденциальными. Обычно для этого просто указывают каталог, где хранятся конфиденциальные документы, или настраивается ODBC-подключение к базе данных. В дальнейшем система просто определяет, насколько похожи проходящие через нее документы на те, с которых были сняты цифровые отпечатки. При достаточно высокой степени похожести документ относится к конфиденциальным. Система работает автоматически и не требует создания сложных правил, однако чем больше документов отнесены к категории конфиденциальных, тем больше ресурсов требуется на проверку.

Машинное обучение

В случаях, когда затруднительно снять цифровые отпечатки со всех конфиденциальных документов (например, в силу сложившегося подхода к обработке такой информации данные хранятся локально на рабочих станциях пользователей) или описать эти документы более общими ключевыми словами/регулярными выражениями, удобнее использовать технологии машинного обучения. Система обучается на наборе конфиденциальных и неконфиденциальных данных одного типа и позволяет в дальнейшем выявлять факты передачи похожей информации.

Распознавание

Следует отметить, что первые два метода рассчитаны прежде всего на анализ текстовой информации. В случае же простого преобразования текста в изображение злоумышленники могут обойти существующую на предприятии систему защиты. Для предотвращения такого простого метода обхода защиты используется механизм распознавания изображений. При этом можно не только выделять текст, существующих методов распознавания достаточно для визуального распознавания электронных документов – штрих-кодов, печатей, подписей, меток конфиденциальности и других графических элементов. Точно такой же метод используется для контроля документов, отправляемых на печать.

Есть и другие механизмы контроля распространения конфиденциальной информации. Например, не стоит забывать и о поиске конфиденциальной информации в сети Интернет с помощью специализированных поисковых систем. Примерами таких систем являются продукты "Крибрум" или "Лавина-Пульс".

Архитектура DLP-решений, как правило, носит распределенный характер. Часть компонентов системы размещается в точке подключения корпоративной сети к Интернету с целью контроля электронной почты и Web-трафика. Агенты DLP-системы могут устанавливаться на корпоративных рабочих местах и мобильных устройствах сотрудников с целью контроля локальной активности, в том числе записи информации на съемные носители. Кроме того, в DLP-системе могут быть специальные компоненты, которые регулярно сканируют корпоративную систему хранения, чтобы обнаружить факты несанкционированного хранения конфиденциальных документов. Все компоненты DLP-системы взаимодействуют с ядром системы, которое собирает поступающую информацию, анализирует ее для последующей подготовки отчетов и проведения расследований инцидентов безопасности. ●

Заключение

Система DLP – сложный технологический комплекс, и настроить его на защиту от утечек ценной информации бывает непросто. Так, настройка ключевых слов при кажущейся простоте требует специальной подготовки и большого объема времени, чтобы минимизировать ложные срабатывания, но, как правило, не оправдывает затрат. Поиск по цифровым отпечаткам документов и информации баз данных технологически проще для внедрения, однако для этого нужно внедрить соответствующий регламент для работы с конфиденциальными документами, чтобы они сохранялись в соответствующих каталогах и были правильно помечены владельцами. Это должны делать люди, а изменить их работу часто бывает сложнее, чем настроить поиск по ключевым словам. Кроме того, юридическое оформление DLP-контроля также может составлять проблему при внедрении, поскольку в соответствии с законодательством о наличии данной системы нужно предупредить работников. Предупреждение о наличии DLP работает не хуже самого DLP – сотрудники, которые знают, что за ними следят, работают аккуратнее и допускают меньше оплошностей, чтобы лишний раз не тревожить DLP.

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА"
см. стр. 48