Отсекая важное
DLP-системы как средство защиты информации

Денис ГАСИЛИН,
руководитель отдела маркетинга, SafenSoft

Утечка информации: угрозы, риски и тенденции

Концепция информационной безопасности подразумевает не только защиту от внешних воздействий на ИТ-инфраструктуру организации. Внутренние угрозы так же актуальны, как и наружные, причем в последнее время количество инцидентов, связанных с вредоносными или неосторожными действиями сотрудников компаний, непрерывно растет. В 2012 г., согласно данным InfoWatch, взятым исключительно из открытых источников, зарегистрировано 934 случая утечки конфиденциальной информации, что на 16% больше, чем в 2011 и 2010 гг. (794 и 801 случаев соответственно), т. е. в среднем 2,5 утечки в день, 75–80 утечек в месяц. При этом склонность компаний к замалчиванию инцидентов позволяет предполагать, что реальное число инцидентов выше как минимум на порядок.

Типы утечек распределились так: 89,4% – персональные данные; 6,0 – коммерческая тайна; 4,1 – государственная тайна; 0,5% – не определено.

Утечки происходили по следующим каналам: 22,3% – бумажные документы; 15,0 – персональные компьютеры; 9,6 – ноутбуки, смартфоны; 8,6 – носители резервных копий; 6,7 – веб; 6,3 – электронная почта; 6,0 – съемные носители информации; 22,5% – канал утечки не определен.

DLP-системы призваны отвечать именно на эти вызовы. Около трети всех компаний, согласно Gartner, уже используют такие системы, и их популярность продолжает расти. Однако эта отрасль относительно молода, и большинство имеющихся на рынке продуктов неспособно гарантировать полноценную защиту от утечек данных. На это есть несколько причин, и мы рассмотрим их ниже, но для начала необходимо сформулировать общие тенденции и требования в области разработки и использования данного вида программного обеспечения. Кроме того, уже сейчас из-за распространения принципа BYOD (Bring Your Own Device), в рамках которого сотрудники используют свои собственные устройства для работы, концепция защиты информации от утечек трансформируется из идеи «периметра безопасности» в защиту информации «всегда и везде», а не только на территории хранилищ данных компании и рабочих мест сотрудников. Согласно проведенному Ponemon Institute исследованию, сотрудники компании нередко (17% случаев) или часто (37%) хранят конфиденциальную информацию на личных мобильных устройствах, при этом либо не уделяя времени на обеспечение безопасности вообще (56%), либо затрачивая минимальное время с минимальным результатом (25%).

В первую очередь нужно отметить, что объем случайных утечек по вине неосторожных сотрудников сокращается. Представленные на рынке DLP-системы успешно справляются с ними в автоматическом режиме.

Согласно проведенному Ponemon Institute исследованию, 78% организаций страдает от инцидентов с утечкой данных. При этом только в 19% случаев сотрудники сами сообщают о произошедших по их вине нарушениях в политике безопасности, влекущих за собой утечку данных. Системы защиты данных обнаруживали подобные инциденты в 36% случаев, а самой распространенной ситуацией является случайное обнаружение инцидента.

Среди рискованных с точки зрения утечки информации действий можно выделить основные:

- подключение компьютеров к сети Интернет через небезопасные беспроводные сети;
- хранение информации на компьютере, после того как необходимость в этом отпала;
- сообщение своих паролей другим людям;
- использование одних и тех же имен пользователя и паролей в разных ресурсах;
- использование обычных USB-накопителей, не защищенных от утечки информации шифрованием данных или другими способами;
- оставление компьютера без присмотра на время отсутствия на рабочем месте;
- потеря USB-накопителя без немедленного информирования работодателя;
- работа на мобильном устройстве вне офиса без использования мер предосторожности, направленных на сокрытие информации на экране от окружающих;
- подключение к сети компании с помощью личного мобильного устройства.

Важно заметить, что вышеперечисленные действия совершаются большинством сотрудников в организациях на регулярной основе. 67% ИТ-специалистов, участвовавших в исследовании Human Factor in Data Protection, уверены, что развернутых в организации систем защиты информации недостаточно для предотвращения таргетированной атаки. Вероятность совершения каждого отдельного потенциально вредоносного действия различается в среднем на 10% для сотрудников в компаниях со штатом до 100 человек включительно и для сотрудников в крупных компаниях с численностью от 100 человек – в неблагоприятную для меньших организаций сторону.

Объем корпоративных данных постоянно растет. Возможности накопления и сбора данных расширяются, а процедуры сбора упрощаются и становятся все более эффективными. Такое сочетание провоцирует руководителей компаний и отделов информационной безопасности на создание политик безопасности, которые заключаются в сборе всех возможных данных, невзирая на их избыточность. В дальнейшем вся эта информация хранится и создает иллюзию безопасности. Как правило, большей частью данных никто никогда не воспользуется. Современные DLP-системы в состоянии автоматически предотвращать только случайные утечки информации, происходящие по вине нерадивых сотрудников, игнорирующих инструкции и правила, а предотвращение действий вредоносного инсайдера требует мониторинга со стороны ответственных сотрудников.

> Огромной проблемой с точки зрения безопасности являются мобильные устройства, используемые сотрудниками для работы, в частности смартфоны и планшеты.

Перечень используемых форматов файлов обычно достаточно четко регламентирован и даже ограничен, тем не менее количество форматов объектов, которые должна контролировать система предотвращения утечек данных, значительно. Особо стоит отметить требования по автоматическому анализу графических файлов. Это создает некоторые сложности с хранением данных вследствие существенного увеличения их объемов, но в связи с постоянным наращиванием базы корпоративных данных технические сложности реализации такого функционала сходят на нет.

Огромной проблемой с точки зрения безопасности являются мобильные устройства, используемые сотрудниками для работы, в частности смартфоны и планшеты. Такие устройства крайне разнообразны, а контроль над ними затруднен. Конечно, можно обязать сотрудника использовать мобильное устройство только в рамках ограниченных рабочих процессов, но тогда у работника появляется другое устройство, которое уже не контролируется ИТ-службой вообще. Интересная особенность и одновременно важная проблема – использование мобильных устройств руководителями. Топ-менеджмент не склонен уделять должного внимания собственной безопасности, перекладывая ее на сотрудников ИТ-служб, однако не выполняя исходящие от них распоряжения. Получается, что руководители являются основной целью атак злоумышленников, и при этом именно они чаще всего пренебрегают установленными правилами безопасности.

Что касается контроля активности сотрудников в социальных сетях, то здесь никаких особых проблем не возникает. Взаимодействие с ними можно регламентировать, а доступ ограничить без применения каких-то новых технологий. Сложнее ситуация с использованием облачных сервисов. С одной стороны, если профессионально организовать этот процесс, то контроль можно обеспечивать на должном уровне, с другой – мало кто может позволить себе такой высокий уровень выделенных специалистов. Как следствие, в большинстве случаев реализуются половинчатые решения, что становится уязвимым местом ИТ-безопасности компании.

Правильно организованные политики безопасности не должны влиять на бизнес-процессы в организации – как в процессе функционирования, так и при оперативном изменении сценариев поведения системы и настройки доступа сотрудников. При четко налаженной

работе ИТ-службы в целом и службы администрирования в частности решить эти задачи несложно. Решение определяется двумя факторами – человеческим и процессуальным. Главное – определить уровень возможных рисков и действовать исходя из их оценки.

Использование DLP-решений в корпоративной системе ИБ

Очень интересным и сложным вопросом является расследование инцидентов в рамках DLP-систем. Мало кто понимает важность не только пресечения инцидента, но и расследования всех его деталей. Для успешного расследования инцидента необходимо наличие двух факторов: информации для исследования и специалистов, способных построить систему анализа информации и разобраться в информации, проводя расследования. Наличие информации – не проблема для современных систем предотвращения утечки данных, так как технические возможности сбора и обработки больших объемов информации существуют и не требуют особых затрат. Сложности возникают на втором этапе – построения эффективных систем анализа информации. Специалистов такого класса единицы, и, как правило, не многие компании могут себе позволить их иметь, а поручать это внешним специалистам опасаются, что негативно сказывается на раскрытии и предупреждении злонамеренных инцидентов. Причем упростить процесс со стороны разработчика системы невозможно: принципы управления информацией изменить нельзя, а их непонимание при настройке системы в любом случае приведет к неудовлетворительным результатам работы системы.

По этой причине немаловажно удобство интерфейса управления системой. Интерфейс решения по безопасности в принципе не может быть простым, если он предназначен для решения серьезных задач, что снова возвращает нас к проблеме профессиональных кадров. Профессионалу не составит труда разобраться в любом интерфейсе, если же поручать обслуживание систем безопасности неспециалистам, то и результаты будут соответствующими.

Здесь возникает вопрос о разумности использования аутсорсингового сервиса DLP. Его решение зависит исключительно от того, как возможные потери от утечек данных соотносятся с затратами на полноценную систему. Если компания хочет иметь максимально эффективную систему безопасности, то она должна строить свою систему, со своими специалистами, со своими решениями. Естественно, построение и поддержание собственной системы безопасности потребуют немалых затрат, и тут следует определить, соизмеримы ли они с возможными потерями.

Очевидным требованием выглядит интеграция DLP-системы с используемыми в бизнес-процессах компании корпоративными системами. Система безопасности должна получать всю необходимую информацию, а без интеграции с используемыми системами это просто невозможно.

Адаптация DLP-решений под актуальные угрозы привела к некоторым положительным результатам. Доля утечек через web, электронную почту и ПК сокращается. В целом традиционные технологии лучше понимают как разработчики, так и пользователи решений по защите информации. Пожалуй, единственная проблема, которую не удается решить в этой области, – утечка данных по «бумажным» каналам. Существуют технологии, способные следить за каждой копией электронного документа, разрешать и запрещать доступ отдельных людей к нему, контролировать распространение файла по любым каналам информации или на внешние хранилища данных. В частности, есть решения, накладывающие определенные ограничения и запреты на печать файлов. Но с момента успешной печати файла программное обеспечение уже не способно отслеживать перемещения бумажной копии, так что данная проблема целиком подпадает под меры безопасности нормативного характера.

Однако покупатели DLP-решений оценивают сейчас не только и не столько защиту традиционных каналов утечки информации. В рамках набирающей популярность концепции BYOD становятся актуальными технологии обеспечения безопасности информации на мобильных устройствах, которые часто хранят конфиденциальную информацию и при этом являются легкой добычей мошенников, поскольку доступ к ним осуществляется за пределами «периметра защиты» организации. Наибольший успех на рынке гарантируется системам, способным контролировать файл на любом устройстве и носителе информации, а также на облачных сервисах, а при необходимости даже на домашних компьютерах и в личных электронных почтовых ящиках сотрудников. Иными словами, концепция защиты данных смещается от защиты устройств от несанкционированного доступа к защите самих файлов, представляющих высокую ценность. Все данные, интересующие злоумышленников, должны храниться в зашифрованном формате и иметь защиту от копирования. Доступ к ним должен предоставляться только в рамках принятых политик безопасности организации вне зависимости от физического местонахождения.

Впрочем, в России, согласно исследованию компании «Б152», решающими факторами при защите персональных данных являются нежелание выплачивать штрафы регуляторам (63% опрошенных) и обеспечение чистоты перед законом (41%). Большинство опрошенных ориентируются в первую очередь на стоимость услуг (59%), вторым по важности фактором считается скорость реализации проекта (49%). Поэтому сложность и многофункциональность DLP-систем должны определяться разработчиком с учетом требований рынка и готовности организаций, на которые направлено их решение, обеспечивать предоставляемый уровень защиты соответствующими затратами. Логичным решением для разработчика выглядит создание линеек DLP-систем разного уровня цен и сложности, ориентированных на определенные ниши на рынке. ■