Практические аспекты защиты от утечки конфиденциальной информации

Виктор Сердюк, генеральный директор ЗАО «ДиалогНаука»

На сегодняшний день все больше российских компаний задумываются о внедрении средств защиты от утечки конфиденциальной информации. В первую очередь это обуславливается увеличивающимся с каждым годом количеством инцидентов, связанных с кражей информации, представляющей ценность для организации. В данной статье рассматриваются некоторые аспекты защиты от инсайдеров. Однако прежде чем переходить к описанию средств защиты от утечки конфиденциальной информации кратко рассмотрим основные виды внутренних угроз безопасности.

Модель внутренних угроз безопасности

В рамках модели угроз ключевым элементом является понятие «инсайдера». Инсайдер это сотрудник компании, являющийся нарушителем, который может иметь легальный доступ к конфиденциальной информации. В результате действий инсайдера конфиденциальная информация может попасть в посторонние руки. При этом важно отметить, что действия инсайдера могут быть как умышленные, так и совершенные по неосторожности. Так, многие инциденты, связанные с утечкой конфиденциальной информации, совершаются вследствие халатности сотрудников. Например, сотрудник может потерять ноутбук с рабочими файлами или по ошибке отправить электронное письмо с коммерческой тайной чужому адресату.

Ниже в таблице 1 представлены возможные категории нарушителей, действия которых могут привести к утечке конфиденциальной информации.

Таблица 1

Примеры категорий внутренних нарушителей

Категория нарушителя	Описание
Категория 1	Сотрудники, имеющие легальный доступ к ЛВС, но не имеющие доступа к конфиденциальной информации
Категория 2	Сотрудники, имеющий ограниченный доступ к конфиденциальным информационным ресурсам ЛВС с рабочего места
Категория 3	Сотрудники, имеющий удаленный доступ к конфиденциальным информационным ресурсам ЛВС через сеть Интернет
Категория 4	Сотрудники с полномочиями системного администратора
Категория 5	Сотрудники с полномочиями администратора безопасности
Категория 6	Программисты-разработчики (или поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение
Категория 7	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств, установленных в ЛВС

На сегодняшний день можно выделить следующие основные каналы утечки конфиденциальной информации, которыми может воспользоваться инсайдер:

- несанкционированное копирование конфиденциальной информации на внешние носители и вынос её за пределы контролируемой территории предприятия. Примерами таких носителей являются флоппи-диски, компакт-диски CD-ROM, Flash-диски и др.;
- вывод на печать конфиденциальной информации и вынос распечатанных документов за пределы контролируемой территории. Необходимо отметить, что в данном случае могут использоваться как локальные принтеры, которые непосредственно подключены к компьютеру злоумышленника, так и удалённые, взаимодействие с которыми осуществляется по сети;
- хищение носителей, содержащих конфиденциальную информацию – жёстких дисков, магнитных лент, компакт-дисков CD-ROM и др.;
- несанкционированная передача конфиденциальной информации по сети на внешние серверы сети Интернет, расположенные вне контролируемой территории предприятия.

Ниже рассмотрены примеры каналов утечки, которые могут использоваться

злоумышленниками для передачи конфиденциальных данных за пределы предприятия:

- протокол передачи электронной почты SMTP. На сегодняшний день практически любая компания использует сервис электронной почты для обмена информацией с клиентами, партнерами и сотрудниками. Данный вид коммуникаций обладает большим количеством преимуществ, такими как дешевизна, простота использования, доступность и др. Вместе с тем, потенциальный нарушитель может использовать электронную почту в качестве инструмента для кражи информации. Для этого ему достаточно отправить письмо с вложенным конфиденциальным документом на внешний электронный адрес и затем уже из дома получить доступ к данным;
- протокол передачи гипертекста HTTP. Протокол HTTP является базовым протоколом для взаимодействия с Интернет-ресурсами, однако с его помощью потенциальный злоумышленник может публиковать конфиденциальную информацию на форумах, блогах, журналах LiveJournal и других сайтах, после чего она станет доступной неавторизованным лицам. Кроме этого, посредством HTTP можно передавать файлы с конфиденциальной информацией через Web-почту на серверах www.mail.ru, www.yandex.ru, www.google.ru и других используя внешние учетные записи пользователей;
- протокол передачи файлов FTP. Данный протокол также может использоваться для копирования конфиденциальных данных на внешние файловые серверы, расположенные в сети Интернет;
- протоколы пиринговых сетей P2P. Пиринговые сети, такие как BitzTorennt, eMule и другие позволяют пользователям обмениваться файловыми ресурсами между собой. При этом, в случае отсутствия средств контроля такого обмена, потенциальный нарушитель может с их помощью передать конфиденциальную информацию через Интернет;
- протоколы обмена речевой и текстовой информацией через сеть Интернет. Наиболее распространенным протоколом данного типа является Skype;
- протоколы систем обмена мгновенными сообщениями ICQ, AOL, Windows Messenger и др. Протоколы данного вида также могут использоваться для несанкционированной передачи файлов с конфиденциальными данными между абонентами.

Методы защиты от утечки конфиденциальной информации

Для эффективной защиты от внутренних угроз безопасности необходимо применять комплексный подход, предусматривающий применение организационных, нормативно-методических и технических мер защиты информационных ресурсов. Так, на предприятии должны

быть разработаны и внедрены организационно-распорядительные документы, определяющие список конфиденциальных информационных ресурсов, возможные угрозы, которые с ними связаны, а также перечень тех мероприятий, которые должны быть реализованы для противодействия указанным угрозам. Такими документами являются «Концепция информационной безопасности» и «Политика информационной безопасности», а также должностные инструкции сотрудников компании и др. В дополнении к организационным средствам защиты должны применяться и технические решения, предназначенные для блокирования перечисленных выше каналов утечки конфиденциальной информации. Технические средства защиты класса DLP можно условно разделить на три класса:

- средства защиты на уровне рабочих станций пользователей, предназначенные для локального контроля за информационными потоками в рамках АРМ пользователя;
- средства защиты на уровне шлюза, позволяющие обеспечить контроль информационных потоков на периметре ЛВС организации;
- комплексные средства защиты, которые сочетают в себе возможности первых двух классов.

Системы защиты от утечки информации на уровне рабочих станций пользователей

Системы защиты от утечки конфиденциальной информации представляют данного типа собой специализированные программные комплексы, предназначенные для выявления несанкционированных действий пользователей, связанных с попыткой передачи конфиденциальной информации за пределы контролируемой территории предприятия. Системы данного типа состоят из следующих компонентов:

- агенты, устанавливаемые на рабочие станции пользователей и обеспечивающие сбор информации о событиях, регистрируемых на этих станциях;
- сервер управления, предназначенный для централизованного управления агентами системы;
- база данных, обеспечивающая хранение результатов работы системы защиты;
- консоль управления администратора безопасности.

На основе настроек, заданных администратором безопасности, агенты позволяют контролировать доступ пользователей к конфиденциальной информации, а также накладывать ограничения на те действия, которые пользователь может выполнить с этой информацией.

Преимуществом использования систем защиты данного типа является возможность создания виртуальной изолированной среды обработки конфиденциальной информации без физического выделения отдельной автоматизированной системы для работы с данными

ограниченного доступа. Однако, применение систем защиты влечёт за собой установку дополнительного ПО на каждую рабочую станцию, что потенциально может привести к увеличению сложности администрирования, а также к возможным конфликтам в работе программ системы.

Системы защиты от утечки информации на уровне шлюза

Системы защиты от утечки информации на уровне шлюза обеспечивают возможность обработки сетевого трафика, отправляемого за пределы контролируемой территории с целью выявления возможной утечки конфиденциальной информации. Используются они, как правило, для анализа исходящего почтового и web-трафика, отправляемого в сеть Интернет.

Такие средства защиты устанавливаются в разрыв канала связи между сетью Интернет и ЛВС предприятия, таким образом, чтобы через них проходили все исходящие пакеты данных.

Технологии выявления утечки конфиденциальной информации

В настоящее время можно выделить две основные технологии выявления попыток кражи конфиденциальной информации. Первая из них базируется на поиске в анализируемом потоке данных ключевых слов, заданных администратором безопасности. Так, например, появляется возможность блокировать сообщения, которые содержат такие ключевые слова, как – «секретно», «конфиденциально» и др.

Вторая технология позволяет выявлять потенциальные утечки на основе так называемых «цифровых отпечатков», которые снимаются с конфиденциальной информации. Данные «цифровые отпечатки» представляют собой специальным образом вычисленную контрольную сумму и позволяют идентифицировать конфиденциальный документ даже в том случае, если он был умышленно изменен злоумышленник.

Однако ни одна из этих технологий не позволяет гарантировать стопроцентное выявление сообщений, содержащих конфиденциальную информацию. В частности, если нарушитель перед отправкой сообщения зашифрует его или замаскирует под видом графического или музыкального файла при помощи методов стеганографии, то средства контентного анализа в этом случае окажутся практически бессильными.

Заключение

В настоящее время одной из наиболее актуальных проблем в области информационной безопасности является проблема защиты от утечки конфиденциальной информации. Для эффективной защиты от такого рода угроз необходимо применять комплексный подход,

предусматривающий применение как организационных, так и технических мер защиты информационных ресурсов.

Необходимо подчеркнуть, что наибольшая эффективность может быть получена при комплексном использовании различных типов средств защиты, основные из которых были рассмотрены в настоящей статье.