электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 03, март 2016

УДК 004.056.5

Технологии защиты информации на предприятии от внутренних нарушителей

***Бобров Н.В.**, магистр*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы обработки информации и управления»

Научный руководитель: Кесель С.А., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы обработки информации и управления»
chernen@bmstu.ru

Справляться с угрозами информационной безопасности извне многие компании научились уже довольно неплохо. Внешним нарушителям порой весьма непросто проникнуть в корпоративную информационную систему. Ситуация коренным образом меняется, если речь заходит о внутренних угрозах.

Современный уровень развития технологий предотвращения утечек конфиденциальной информации из-за внутренних угроз, в частности, DLP-систем (Data Leackage Prevention) не может полностью удовлетворить потребностей компаний в обеспечении информационной безопасности. Новые каналы передачи, через которые могут происходить утечки, появляются быстрее, чем разрабатываемые для них меры контроля и защиты.

Стоит отметить, что не все DLP-системы справляются с обработкой больших объемов данных. С одной стороны нет сложностей в осуществлении хранения всего переданного трафика, а с другой стороны услуга по индексации мега объемов данных и запуску инструментов поиска и аналитики все еще оказывается слишком дорогой для компании. Но основной проблемой для корректной работы технических средств защиты информации является человеческий фактор: человек как элемент информационной системы плохо предсказуем и трудно контролируем. Однако полностью исключить его из процесса обработки информации невозможно даже в теории.

Под нарушителем информационной безопасности будем понимать лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам компании.

Под атакой на ресурсы корпоративной сети будем понимать попытку нанесения ущерба информационным ресурсам систем, подключенных к сети. Атака может осуществляться как непосредственно нарушителем, так и при помощи процессов, выполняющихся от лица нарушителя, либо путем внедрения в систему программных или аппаратных закладок, компьютерных вирусов, троянских программ и т.п.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников обслуживающих подразделений:

– обслуживающий персонал (системные администраторы, администраторы баз данных, администраторы приложений и т.п., отвечающие за эксплуатацию и сопровождение технических и программных средств);

– программисты, отвечающие за разработку и сопровождение системного и прикладного программного обеспечения;

– технический персонал (рабочие подсобных помещений, уборщицы и т.п.);

– сотрудники бизнес подразделений предприятия, которым предоставлен доступ в помещения, где расположено компьютерное или телекоммуникационное оборудование.

В зависимости от способа осуществления доступа к ресурсам системы и предоставляемых им полномочий внутренние нарушители информационной безопасности подразделяются на категории.

1. Категория А – не зарегистрированные в системе лица, имеющие санкционированный доступ в помещения с оборудованием. Лица, относящиеся к категории А могут иметь доступ к любым фрагментам информации, распространяющейся по внутренним каналам связи корпоративной сети; располагать любыми фрагментами информации о топологии сети, об используемых коммуникационных протоколах и сетевых сервисах; располагать именами зарегистрированных пользователей системы и вести разведку паролей зарегистрированных пользователей.

Категория В – зарегистрированный пользователь системы, осуществляющий доступ к системе с удаленного рабочего места. Лица, относящиеся к категории В располагают всеми возможностями лиц, относящихся к категории А; знают, по крайней мере, одно легальное имя доступа; обладают всеми необходимыми атрибутами, обеспечивающими доступ к системе (например, паролем); имеют санкционированный доступ к информации, хранящейся в БД и на файловых серверах корпоративной сети, а также на рабочих местах

пользователей. Полномочия пользователей категории B по доступу к информационным ресурсам корпоративной сети предприятия должны регламентироваться политикой безопасности, принятой на предприятии.

Категория C – зарегистрированный пользователь, осуществляющий локальный либо удаленный доступ к системам входящим в состав корпоративной сети. Лица, относящиеся к категории C обладают всеми возможностями лиц категории B; располагают информацией о топологии сети, структуре БД и файловых систем серверов; имеют возможность осуществления прямого физического доступа к техническим средствам ИС.

Категория D – зарегистрированный пользователь системы с полномочиями системного (сетевого) администратора. Лица, относящиеся к категории D: обладают всеми возможностями лиц категории C; обладают полной информацией о системном и прикладном программном обеспечении ИС; обладают полной информацией о технических средствах и конфигурации сети; имеют доступ ко всем техническим и программным средствам ИС и обладают правами настройки технических средств и ПО. Концепция безопасности требует подотчетности лиц, относящихся к категории D и осуществления независимого контроля над их деятельностью.

Категория E – программисты, отвечающие за разработку и сопровождение общесистемного и прикладного ПО, используемого в ИС. Лица, относящиеся к категории E обладают возможностями внесения ошибок, программных закладок, установки троянских программ и вирусов на серверах корпоративной сети; могут располагать любыми фрагментами информации о топологии сети и технических средствах ИС.

Эта классификация справедлива с учетом того, что несанкционированный доступ на объекты системы посторонних лиц исключается мерами физической защиты (охрана территории, организация пропускного режима и т.п.).

Рассмотрим основные технологии, применяемые в настоящее время для нейтрализации внутренних угроз, их преимущества и недостатки.

1. Контроль документов

Технология контроля документов воплощается в таких современных продуктах как Microsoft Windows Rights Management Services, Adobe LiveCycle Rights Management ES, Oracle Information Rights Management.

Принцип работы данных систем заключается в назначении правил использования для каждого документа и контроля этих прав в приложениях, работающих с документами данных типов.

При использовании технологий контроля документов необходимо учитывать естественные ограничения этой технологии:

– возможен контроль только файлов-документов, если речь идет о неструктурированных файлах или базах данных, данная технология не работает;

– при наличии у нарушителя информационной безопасности ключа шифрования, он может открыть документ и запустить приложение от имени пользователя, имеющего минимальный уровень доступа к документу, т.е. данная технология защиты будет обойдена;

– возникают существенные сложности при внедрении данной технологии в компании, имеющей большой объем неклассифицируемой документации.

2. Защита от утечек

Термин защита от утечек (data loss prevention, DLP) появился сравнительно недавно. Как правило, аббревиатурой DLP обозначают системы, контролирующие возможные каналы утечки и блокирующие их в случае попытки пересылки по этим каналам какой-либо конфиденциальной информации. Кроме этого, в функции подобных систем часто входит возможность архивирования проходящей по ним информации для последующего аудита, расследования инцидентов и ретроспективного анализа потенциальных рисков.

Концепция DLP в настоящее время является полноправным средством в арсенале корпоративных служб безопасности в условиях постоянно усиливающегося на них давления по обеспечению внутреннего контроля и защите от утечек.

Одной из основных проблем при реализации и внедрении DLP-систем является способ детектирования конфиденциальной информации, т.е. принятие решения о том, является ли передаваемая информация конфиденциальной. Для этого производится анализ содержимого передаваемых документов (контентный анализ).

Кроме этого, определенную проблему в работе DLP может создать шифрование трафика. Если по требованиям безопасности необходимо шифровать сообщения электронной почты или использовать протокол SSL при соединении с какими-либо веб-ресурсами, проблема определения наличия конфиденциальной информации в передаваемых файлах может быть весьма сложноразрешимой.

Тем не менее, несмотря на все сложности, при правильной настройке и серьезном подходе использование DLP-систем может значительно снизить риск утечки конфиденциальной информации и дать организации удобное средство для внутреннего контроля.

3. Концепция IPC

Суть концепции IPC (Information Protection and Control) заключается в объединении методов DLP и шифрования: с помощью DLP контролируется информация, покидающая по техническим каналам пределы корпоративной сети, а шифрование используется для защиты носителей данных, которые физически попадают или могут попасть в руки

посторонних лиц.

В концепции IPC применяются следующие технологии шифрования: шифрование магнитных лент, серверных хранилищ, ноутбуков и съемных носителей.

Шифрование значительно расширяет возможности DLP-систем и снижает риски утечки конфиденциальных данных.

Следует отметить, что защита информации – проблема комплексная, и решить ее с помощью только какого-либо одного средства, как правило, не удается.

Все выше обозначенные аспекты, с которыми сталкиваются разработчики DLP-систем, способствуют развитию новых технологий в данной сфере. Так, по прогнозам аналитиков, в ближайшие годы рынок защиты данных от утечки ждет стабильный рост на 30–40% ежегодно.

Следующим этапом развития технологий предотвращения утечек конфиденциальной информации станет появление DLP-систем с возможностью распознавания смысла.

Уже у существующих систем DLP имеются развитые средства лингвистического анализа, т.е. детектирование происходит не просто по маске, а с учетом форм слова, синонимов, опечаток и т.д. DLP скоро станут выполнять поиск фрагментов, близких к образцу не только по форме, но и по смыслу. Кроме того, ожидается, что они смогут находить сходные с образцом изображения и мультимедийные объекты. Также системы DLP должны обладать отдельной функциональностью по детектированию персональных данных.

Одним из подходов к защите от внутренних угроз является «сужение периметра». Данным способом защищается информация, содержащая гостайну, но лишь в последнее время появились относительно недорогие и массовые способы внедрения такого решения в частных компаниях.

Чтобы не выискивать конфиденциальную информацию по всему офису, на рабочих станциях, их USB-разъемах и CD-приводах, в кабелях и принтерах, вся защищаемая информация концентрируется на одном сервере и здесь же обрабатывается. Пользователи получают доступ по протоколу X-Windows. Таким образом, по сети передаются лишь графические копии экрана, но не сама информация. За конфиденциальной информацией, сконцентрированной на одном сервере, следить значительно проще.

В результате остается один канал утечки — пользователь. Но этот канал перекрывать техническими средствами не представляется возможным.

Кроме существенного сокращения охраняемого периметра информационной системы решение обещает экономию средств. Персональные компьютеры можно заменить дешевыми бездисковыми рабочими станциями (терминалами) и таким образом заметно уменьшить не только стоимость техники, но и трудоемкость настройки и администрирования.

Наращивание функциональности DLP-систем будет проходить в следующих направлениях:

– вместо запрета доступа к «непрофильным» или развлекательным ресурсам следует разрешить такой доступ, но с ограничением по времени;

– некоторые запреты, как показали исследования, вообще являются излишними, поскольку не увеличивают, а снижают производительность, поэтому от них надо отказываться (даже если заказчик высказывает пожелания такого рода, например о блокировании доступа к социальным сетям);

– для оператора DLP появятся новые формы представления информации, такие как новые типы диаграмм, автоматическое преобразование текстов, звуковое представление событий, визуализация корреляции разных событий;

– точно так же, как системы антивирусов и антиспамов, DLP научатся скачивать обновления сигнатур и правил с сервера производителя или из центрального офиса предприятия.

Проблема защиты от внутренних нарушителей информационной безопасности крайне сложна в разрешении. В сложных ситуациях (например, если на компанию проводиться спланированная атака конкурентов) понадобится напряжение всех сил как служб информационной безопасности организации, так и юридической службы и высшего руководства компании.

Организация при этом проходит проверку на прочность как в части технической инфраструктуры, так и в части морального климата внутри коллектива. Усилия служб информационной безопасности должны быть направлены в равной степени, как на выявление фактов утечки, так и на сбор доказательств причастности сотрудников к этим утечкам.

Грамотное применение технических средств борьбы с внутренними нарушителями информационной безопасности вкупе с правовыми способами защиты информации многократно повысят эффективность работы в кризисной ситуации и позволят выйти из неё с минимально возможными потерями.

Список литературы

[1]. Орлов С. От DLP к защите от внутренних угроз // Журнал сетевых решений/LAN. 2013. № 5. С. 22-27

[2]. Барабанов А.В., Марков А. С., Найханова И. В. Методика оценки соответствия средств защиты информации общим критериям // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2013. № 2(91). С. 48-58.

[3]. Свинарёв Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.П., Перетокин О.И. Инструментальный контроль и защита информации: учебное пособие. Воронеж: ВГУИТ, 2013. 192 с.

[4]. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в интернет, ДМК Пресс, 2011. 396 с.

[5]. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. М.: Альпина Паблишерз, 2011. 338 с.

[6]. Милославская Н., Сенаторов М., Толстой А. Управление инцидентами информационной безопасности и непрерывностью бизнеса. 2-е изд. М.: Горячая линия-Телеком, 2014. 170 с.

[7]. Бирюков А. Информационная безопасность: защита и нападение. М.: ДМК-Пресс, 2013. 474 с.