Общая озабоченность общественности этой проблемой отчасти объяснима: по данным мировой статистики (например, по отчетам ФБР Computer Crime and Security Survey), компании несут максимальные убытки в результате реализаций именно этой угрозы.

В то же время внимательный анализ публикаций, выступлений и заявлений позволяет обнаружить некоторые несуразности:

* Термин «инсайдер» повсеместно употребляется без определения. Подразумевается, что значение этого слова очевидно.
* Практически «слились» понятия «инсайдер» и «злоумышленник, находящийся внутри сети».
* Многие эксперты, рассказывая об угрозах инсайдеров, приводят как пример потерю ноутбуков с конфиденциальной информацией.
* Часто описание инсайдерских угроз сбивается на перечисление обычных атак наподобие подбора пароля, попытки воспользоваться чужим логином, взлома компьютера коллеги и т.п.

Что же заставляет многочисленных экспертов по вопросам защиты от инсайдеров допускать подобные несуразности в статьях и других выступлениях? Искреннее заблуждение? Авторы недопонимают этот предмет?

Пытаются скрыть свою некомпетентность?

Стремятся воспользоваться красивыми словесами или манипулировать читателем?

Во главу угла обзоров по проблеме инсайдеров ставят борьбу с ними всеми доступными средствами.

К слову, сложившаяся ситуация немного напоминает эпопею о борьбе со спамом, которая развернулась перед читателями примерно два года назад. Никто не отрицает, что проблема спама существует.

Однако она касается по большей части не корпоративных пользователей, а провайдеров, которые вынуждены хранить на серверах значительные объемы писем. Впрочем, многих практически принудили принять за чистую монету разговоры о катастрофе, которую спам вот-вот принесет любому пользователю.

Как разобраться в предмете, понять и оценить риски, которые инсайдеры несут именно вашему предприятию? Как выбрать действительно адекватные меры защиты?

Предлагаю начать с главного, без чего нет смысла продолжать дальнейший разговор, – с определения того явления, которое мы будем обсуждать, а именно – понятия «инсайдер».
Термин «инсайдер»

Чтобы не заставлять читателя погружаться в справочники и словари, я попробовал поискать определение этого термина в сети Интернет.

Первая же найденная ссылка (http://ru.wikipedia.org/wiki/Инсайдер) порадовала исчерпывающим определением.

Понятие «инсайдер» раскрывается как «член какой-либо группы людей, имеющей доступ к информации, закрытой для широкой публики. Контекст употребления термина – соотнесенность с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер – это член группы, который обладает информацией, имеющейся только у этой группы.

Следующее определение, которое предоставил нам Интернет (http://abc.informbureau.com/html/einaeaad.htm), звучало так: «ИНСАЙДЕР (англ, insider, от inside – буквально ‘внутри’) – лицо, имеющее, в силу своего служебного или семейного

положения, доступ к конфиденциальной информации о делах компании. Речь идет о должностных лицах, директорах, основных акционерах корпорации с широким владением акциями и их ближайших родственниках».

Повторим еще раз: ключевыми словами в двух рассмотренных определениях являются «имеющие доступ к информации». Даже это наблюдение дает основания для того, чтобы пересмотреть проблему «инсайдеров».

Итак, мы приходим к следующим выводам.

* Не следует торопиться с обобщениями и стратегическими выводами, прежде чем проблема «внутреннего злоумышленника» не будет определена более четко.
* Инсайдеров следует «рассортировать» на 1) имеющих доступ к информации; и 2) сотрудников данной компании, которые стремятся получить доступ к такой информации.

Будем считать, что термин «инсайдер» мы привели к корректному значению.

Немаловажно, что в двух обнаруженных определениях упоминалось понятие информации.

Понятие «информация»

Понятие информация по своей сути является крайне дискуссионным. В каждой области знания этот термин используется по-разному. Следовательно, многие люди употребляют его и оперируют им основываясь на интуитивных и субъективных ощущениях, вкладывая в него самые разные значения.

Для дальнейшего обсуждения нам потребуется четкое понимание этого термина. Итак, предлагаю считать, что:

* Информация — это пояснение, научение, какое-либо сведение.

Предлагаю не смешивать понятие «информации» с понятием

* Данные — это представление фактов и идей в формализованном виде, пригодном для передачи и обработки в некотором информационном процессе.

Теперь для конструктивного продолжения диалога разберемся окончательно с определениями понятий. Легче всего сделать это на следующих примерах.
Факт Данные Информация
Компания готовится выпустить новый продукт Техническая документация, рекламные материалы, дистрибутив, исходный код продукта Продукт еще не готов/не оттестирован, сроки выхода будут сорваны/выдержаны
Компания стремится поднять стоимость своих акций План мероприятий, направленных на повышение данного показателя, прогнозы по стоимости акций и т.п. Компанию просто готовят к продаже
Компания набирает новых сотрудников Объявления на серверах для соискателей
Компания готовится выпустить новую услугу/вскоре открывает новый филиал

Надеюсь, что мне удалось продемонстрировать разницу между этими понятиями.

Осознавать эти отличия просто необходимо хотя бы для того, чтобы определить объект защиты (данные или информация?) и необходимые в этой связи средства/меры.
Почему инсайдеров боятся

Итак, если исходить из наших определений, инсайдерами, как правило, являются директора и старшие менеджеры, а также владельцы компании.

Сформированный за последнее время образ инсайдера включает в себя набор того, что подвергается выносу на всеобщее обозрение:

* списки клиентов;
* документы;
* базы данных;

* информацию.

Все это, по утверждениям некоторых экспертов, наносит компаниям значительный ущерб и неизбежно влечет за собой потерю клиентов.

Кстати, практически нигде не упоминается угроза уничтожения или намеренного искажения данных… Никто не обращает внимания на это? Еще не разработаны методы для защиты от этих угроз?

Если повторять, как мантру, слова о самых распространенных угрозах, становится страшно. Однако опасения действительно не напрасны: мировая статистика инцидентов гласит о реальном ущербе бизнесу и о потерях клиентов в результате действий инсайдеров. Не забудем, что теперь мы разделяем понятие инсайдера и обычного сотрудника.

Разберем этот вопрос подробнее. Имеется четыре варианта:
данные информация
сотрудник сотрудник пытается вынести данные сотрудник пытается вынести информацию
инсайдер инсайдер пытается вынести данные инсайдер пытается вынести информацию

Задачи, которые мы можем поставить себе в борьбе с инсайдерами – просто формулируются:

* соответствие требованиям нормативных актов и стандартов;
* сохранность информации;
* сохранность данных;
* выявление каналов утечки;
* доказательство непричастности.

Но все ли они могут быть реализованы легко? И какие технические средства могут нам помочь?

Борьба с инсайдерами с помощью технических средств и ее результаты

Если компания просто хочет соответствовать определенным требованиям, которые к ней предъявляет государство или профессиональное сообщество, то задача сводится даже не к приобретению и внедрению любого средства защиты, а к грамотному документированию процессов обеспечения безопасности в организации.

Далее мы подходим к наиболее интересной фазе – к борьбе с утечками информации.

Собственно по определению информации, которое мы дали, пресечь утечку информации возможно только путями:

* самоконтроля инсайдеров (для того чтобы предотвратить случайное разглашение информации);
* акцентирования внимания руководства на том, что не вся информация предназначается для широкой публики.

К сожалению, эта проблема целиком во власти человеческого фактора. Печально, но с ней не всегда справляются даже самые передовые спецслужбы.

С проблемной утечки данных (файлов, баз данных, печатных копий документов и т.п.) бороться можно. Но только и именно бороться. Победить эту проблему невозможно: как бы мы ни ограничивали доступ к информации…

* можно показать документ на мониторе/в распечатке коллеге, которому данная информация не должна быть доступна.
* сотрудник может забыть документ на принтере, в столовой, оставить без присмотра кабинет /кейс /сейф.
* можно сделать запись вручную с экрана монитора.
* можно зачитать по телефону или наговорить на диктофон определенный фрагмент конфиденциальных данных.
* можно сфотографировать экран монитора на фотокамеру сотового телефона.

* содержание документа можно передать кому-либо по памяти.

Кроме того, даже ноутбук с конфиденциальными данными может быть утерян или украден – вместе со всеми ключами (например, опасность подстережет нас, если данные на ноутбуке хранились в защищенном виде).

Технические средства помогут решить только одну проблему – отслеживание каналов утечки: собрать полную статистику обращений к ресурсу, скоррелировать факт обращения, скажем, к файлу с отправкой этого же файла по почте и т.п.

Единственная неприятность – в том, что технические средства могут дать слишком много информации, проверять и анализировать которую придется все-таки и опять же людям. И вновь мы приходим к выводу о том, что технические средства не позволят добиться хороших результатов.

Возможно ли доказать с помощью технических средств непричастность определенного сотрудника к инциденту? Вряд ли.

Причем более по политическим причинам, чем по техническим. Представьте: однажды выходит статья о том, что в компании XXX произошла очередная утечка базы данных.

Журналисты муссируют эту тему, опрашивают экспертов по безопасности о причинах, вспоминают историю утечек, гадают о причинах этой и т.п. Сенсация… Ваши заявления о том, что компания непричастна и информация утекла не от вас, мало кого интересуют, а если их и опубликуют, то «попозже», когда интерес к теме уже поулегся.

К тому же никто не сможет доказать на 100% того, что источником утечки стала не ваша организация. Вы сможете только показать, как (в том числе техническими средствами) вы заботитесь об их сохранности.

О чем не говорят борцы с инсайдерами

«Любые средства защиты создают неудобства». Это аксиома. «Любые внедряемые средства защиты нужно обслуживать». Это закон жизни.

Глупо устанавливать средство защиты и не следить за тем, какие результаты оно выдает.

Теперь о результатах.

Допустим, что необходимо содержать сеть порядка 1 000 компьютеров, на каждом из которых хотя бы раз в день в USB-порт подключают флешку /мобильный телефон /фотоаппарат. Следовательно, ежедневно требуется анализировать минимум 1 000 событий, связанных с использованием этих устройств. Не думаю, что терпения обслуживающего персонала хватит более чем на два дня.

Решение запретить все – тоже не всегда самое правильное. Через несколько минут начальник спросит, почему не читается его флешка, а сотрудник отдела рекламы будет спрашивать о том, как теперь ему передавать в типографию макеты листовок и т.п.

Если доступ к файлу имеют все без исключения, то в случае инцидента под подозрение в первую очередь попадут те, кому он не нужен. Однако никаких гарантий по верному определению преступника здесь нет, и без бывалого оперативника мы не разберемся.

Если доступ к файлу был разграничен, вы узнаете, что информацией пользовались те, кто допущен к ней. Это ценно, но… бесполезно. Можно выявить некоторые особенности: например, кто-то обратился к файлу посреди ночи.

Необычно, но ни о чем не говорит, особенно если хозяин учетной записи не отрицает факта обращения.

Говоря о контроле, будем помнить, что от инсайдера мы не защитимся, а для сотрудника

этот файл должен быть закрыт.
Так слежение или разграничение?

Золотое и потому невыполняемое правило: необходимо внедрять средства защиты в соответствии с политиками безопасности.

Конечно, неплохо, что внедрение системы контроля электронной почты заставило организацию разобраться, что возможно пересылать определенным лицам и что является конфиденциальной информацией.

Если бы представление о том, что можно, а что нельзя, было сформировано заранее, компания подобрала бы более выгодное решение, согласившись с потребностью в данном средстве.

Но и это еще не все.

Ответственные за безопасность в организации! Раз и навсегда решите сами для себя, что эффективнее и проще:

* хранить все данные без разграничения доступа и пытаться найти того, кто отослал ее за пределы организации;
* разграничить доступ к данным так, чтобы они были доступны только тем, кому они нужны для выполнения работы.

Первый вариант зрелищен и демонстративен. Все наблюдают за тем, как специалисты отдела безопасности ползают на корточках перед системными блоками компьютеров и заклеивают USB-порты. «А что это почта сегодня так и не заработала?» – «А это, коллега, внедряют новую систему контроля».

Второй вариант подразумевает кропотливую работу по анализу потребностей разных

сотрудников, трудоемкие настройки механизмов разграничения доступа и т.п.

Каждый выбирает свой путь сам. Добавлю лишь то, что первый напоминает поиск монетки под фонарем: ее ищут рядом с фонарем не потому что потеряли именно там, а потому что там светло.

Лукавая статистика инцидентов

Когда раскрывать тему борьбы с инсайдерами взялись профессионалы пера, явление инсайда подверглось губительному обобщению. Смешали все.

Хотелось бы отметить, что никаким образом под понятие «угрозы инсайдеров» не попадают следующие явления и, следовательно, они не являются техническими средствами контроля информации:

* потери ноутбуков, флешек и т.п. (это халатность!);
* кражи ноутбуков, компьютеров, винчестеров с резервными копиями (предлагаю считать это явление родственником взлома);
* утечка информации в результате воздействия вирусов;
* утечки информации при взломе сети (даже если осуществлен сотрудником пострадавшей организации).

К инсайдерской угрозе не относятся и такие случаи, как утечка базы клиентов вместе с директором по продажам.

Увольняя директора по продажам, забирайте его телефонную книжку. Но как отобрать сложившиеся отношения с заказчиком, годы учебы в институте с важными клиентами и т.п.?

Важно не позволять втянуть себя в решение проблемы, которой нет или которая не решается принципиально.

Выводы

Сделать конкретный вывод по проблеме о способах ее решения нельзя. Правда жизни заключается в многочисленности проблем, связанных с инсайдерами. Некоторые специалисты по безопасности, как это ни прискорбно, порой ограничены во взглядах на ту или иную проблему именно в силу своего профессионализма.

К примеру, информация для них – это файлы и базы данных. (Первая ошибка – путаница понятий «данные» и «информация».) С утечками этих объектов профессионал начинает бороться известными ему средствами: банальный отказ от отчуждаемых носителей, контроль почты, контроль за числом печатных копий документа и постановка их на учет, проверка портфелей на выходе из здания и еще, и еще… При этом настоящие инсайдеры, часто хорошо осведомленные об этих средствах контроля, воспользуются для отправки документа факсом.

Так может, прежде чем кидаться в омут борьбы с проблемой, стоит оценить эту проблему, сравнить ее с другими и сделать более обоснованный выбор?