Борьба с инсайдом:
новые угрозы и риски, перспективные организационные и технические средства

Алексей КОМАРОВ,
директор NGS Distribution по маркетингу и продуктовому управлению

Актуальность проблем инсайда сегодня вряд ли у кого-то вызывает сомнения. Громкие истории, связанные с утечками конфиденциальной информации, у всех на слуху. Причем широкий общественный резонанс вызывают как разглашение информации, не предназначенной для посторонних, умышленными действиями сотрудников, так и утечки, возникающие в результате ошибочных и незлонамеренных действий.

Борьба с инсайдом

Деление – на умышленных инсайдеров и непреднамеренных – является уже устоявшимся. Принято считать (во всяком случае, многие аналитические отчеты говорят именно об этом), что случайные утечки происходят гораздо чаще. Под непреднамеренным инсайдером не совсем корректно понимать только того, кто отправил вовне непосредственно саму конфиденциальную информацию. Данное понятие логично распространить на любого сотрудника, чье какое-либо действие или бездействие прямо повлекло за собой утечку. Скажем, разглашение тем или иным способом пароля постороннему лицу либо установка на рабочий компьютер троянской программы утечкой, в общем-то, не является, но к таковой вполне понятным образом ведет. С другой стороны, и слишком обобщать это понятие тоже было бы неправильно, иначе к непреднамеренным инсайдерам можно причислить и администратора, не установившего свежее обновление или неправильно настроившего систему предотвращения вторжений, в результате чего злоумышленник получил возможность доступа к конфиденциальной информации.

Завершая обсуждение терминов, стоит оговорить, что хотя формально понятие «утечка» не обязательно означает попадание информации к злоумышленнику и, следовательно, возникновение ущерба, на практике под «утечкой» понимают именно результативную утечку. В этом смысле письмо с внутренним годовым отчетом, ошибочно отправленное сотрудником по электронной почте своему дальнему родственнику, по формальным признакам является утечкой, так как конфиденциальная информация покидает разрешенный периметр, но на самом деле угрозы не несет и в рамках данной статьи приниматься в расчет не будет.

Прошлогодняя история с Эдвардом Сноуденом, бывшим сотрудником ЦРУ и Агентства национальной безопасности США, передавшего газетам похищенную им секретную информацию, показала, что бороться с умышленными инсайдерами крайне проблематично даже при наличии достаточного финансирования, квалифицированных кадров и строгих внутренних регламентов, имеющихся в распоряжении американских спецслужб.

Можно, конечно, задаться вопросом: стоит ли вообще пытаться защитить конфиденциальную информацию в какой-либо крупной или тем более не очень коммерческой компании, раз уж секретную государственную информацию не удалось эффективно защитить? Ответ очевиден: защищать информацию нужно не для того, чтобы получить 100%-ную гарантию ее сохранности (это недостижимо), а для того, чтобы повысить сложность ее кражи злоумышленником и тем самым снизить риски возникновения ущерба.

Новые угрозы и риски

Как сообщает пресса (http://www.interfax.ru/russia/390110), в августе этого года Сноуден получил вид на жительство в России сроком на три года, он трудоустроен и получает помощь от частных лиц, а через пять лет сможет претендовать на получение гражданства РФ. Вряд ли кто-либо согласится с тем, что именно это и было целью и мечтой, которые побудили Эдварда пойти на то, на что он в итоге пошел. Скорее можно предположить, что им двигало желание получить всемирную известность, но сам он озвучивает более благородные цели.

В сопроводительной записке к передаваемым им документам Сноуден написал (http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance): «Я понимаю, что мне придется страдать за свои поступки», но «я буду удовлетворен, если секретные законы, неравная безнаказанность и непреодолимая исполнительная власть, правящая тем миром, который я люблю, будут раскрыты хотя бы на мгновение»; «Я действительно хочу, чтобы в центре внимания оказались эти документы, и надеюсь, что это вызовет обсуждение среди граждан всего мира о том, в каком мире мы хотим жить».

Даже если сами слова и можно подвергнуть сомнению, то трудно отрицать, что поступок Эдварда способен, если так можно сказать, вдохновить его последователей. Тема борьбы с несправедливостью, беззаконием и ложью вполне может найти отклик и в сердцах сотрудников, добавляя к уже всем привычным факторам мотивации – деньгам и славе – теперь еще и новый тип нарушителей – благородных борцов за правду. Основная сложность в выявлении подобных нарушителей как раз и кроется в отсутствии у них личной корысти, потому и выявить их по косвенным признакам не так просто.

Трудно сказать, насколько распространено сегодня желание правды и справедливости, достаточно сильное для совершения противоправных действий, но в современном цифровом мире границы если и не полностью стерты, то значительно расширены, скорость распространения информации колоссальна, поэтому своих последователей может найти, пожалуй, практически любая идея, в том числе и такая.

Имеющее место размытие границ в информационном пространстве способно существенно усилить потенциальный ущерб и от самих утечек: скандальные новости распространяются мгновенно, нанося серьезный ущерб репутации, а информация, выложенная для общего доступа, с высокой вероятностью найдет того, кто сможет «правильно» ею воспользоваться, опять же причиняя максимально возможный вред.

Среди технологий, меняющих привычные способы взаимодействия людей друг с другом в ходе обмена информацией, нельзя не отметить две особенно сильно повлиявшие на принципы обращения сотрудников с конфиденциальной информацией. Речь о мобильных устройствах и облачных технологиях.

Мнение специалиста

Игорь БОГАЧЕВ,

руководитель практики инфраструктурных решений «Астерос Информационная безопасность» (группа «Астерос»):

Тема «благородных борцов за правду» не нова. На заре компьютерной эры именно такими мотивами прикрывались почти все хакеры. Со временем технологии стали доступнее и среди злоумышленников возобладала жажда наживы, но «белые хакеры» и хактивисты никуда не делись, просто их доля сильно уменьшилась. Каждый громкий случай типа «Сноудена» привлекает к себе всеобщее внимание, а говоря на языке профессионалов, повышает вероятность рисков, связанных с действиями данного типа нарушителей. Со временем этот бум затихает, пока не произойдет очередной подобный случай. Тем не менее при разработке модели нарушителя «благородные мотивы» всегда учитываются.

В современном мире гораздо сильнее противоположный тренд: получение материальной выгоды. Если существует возможность хорошо нажиться, пусть и не совсем законным способом, нынешние нарушители готовы в это серьезно вкладываться: объединяться в ОПГ, разрабатывать специально под «клиента» вредоносное ПО, довольно долго выжидать его, даже устроиться на работу в интересующую их компанию. Безусловно, стоимость мер противодействия должна быть оправдана стоимостью защищаемой информации. Далеко не всем нужны суровые методы, но если информация действительно того стоит, не скупитесь. Помимо RM и MDM за последние несколько лет технологически сильно продвинулись системы предотвращения утечек (DLP), контроль действий администраторов, анализ исходного кода. Набирают обороты решения по выявлению целенаправленных атак (APT). При всей этой динамике вполне можно если и не быть на шаг впереди, то хотя бы не отставать от противника, и не важно, какие средства защиты вы в конечном итоге выберете, важно понимать принципы. Например, такие:

- Управление информационными потоками. Если автоматизировать бардак, то получится автоматизированный бардак. Прежде чем приступать к защите информации, необходимо идентифицировать конфиденциальную информацию, правильно ее категорировать и оценить, определить места и способы ее обработки, права доступа. Это база, основной шаг, определяющий эффективность всех последующих. Казалось бы, прописная истина, но именно этот первый и самый важный шаг либо вообще не делается, либо делается некачественно. Проблема усугубляется тем, что эту задачу должен выполнить сам владелец бизнеса, ни один интегратор не сможет полноценно сделать это за него, а у владельца зачастую не хватает для этого ни компетенции, ни времени.
- Комплексная система защиты. Здесь ключевые слова и «комплексная», и «система». Защита как от внешних нарушителей, так и от инсайдеров должна представлять собой комплекс мер, иногда организационных, иногда технических, но связанных как между собой, так и со смежными системами и протекающими в них изменениями.
- Анализ рисков. Стоимость мер защиты должна быть адекватной вероятному ущербу, на предотвращение которого они направлены. В некоторых ситуациях оправдано применение дублирующих механизмов, просто для того, чтобы снизить вероятность утечки, в некоторых, наоборот, нет никакой необходимости в защите.
- Постоянное развитие. Нельзя сделать систему защиты раз и навсегда. Даже при неизменности среды функционирования необходимо регулярно пересматривать угрозы, переоценивать риски, искать новые методы противодействия старым угрозам.

Для эффективной защиты конфиденциальной информации от утечек необходимо, с одной стороны, понимать, где она находится, и контролировать все места ее хранения, а с другой – отслеживать реальные и потенциальные пути ее распространения.

Совмещение облачных и мобильных технологий в конечном итоге приводит к тому, что конфиденциальная информация может оказаться в облачном хранилище, строго говоря, слабо контролируемом ИТ-департаментом организации, при этом доступ к ней сотрудники могут осуществлять с помощью мобильных устройств, которые также достаточно сложно контролировать стандартными средствами.

Компании, которые предоставляют неограниченный и неконтролируемый доступ с мобильных устройств к корпоративным данным, сильно рискуют, ибо предотвратить утечку информации техническими методами при таком подходе практически невозможно. Организационные методы способны помочь вне зависимости от конкретных каналов распространения информации и методов работы с ними, поскольку ориентированы прежде всего на самих сотрудников.

Перспективные организационные и технические средства борьбы

Организационные методы борьбы с инсайдерами – самые эффективные, но и самые дорогостоящие, так как в любом случае требуют ручного анализа с привлечением квалифицированного персонала.

Как и в случае с гигиеной, мониторинг общего морального климата в коллективе и выявление аномалий в поведении того или иного сотрудника путем тесного взаимодействия с доверенными сотрудниками, играющими, если использовать аналогии, роль агентов, на порядок эффективней любого технического решения, пытающегося предотвратить уже совершаемую утечку. Вместе с тем, такой способ борьбы по понятным причинам и самый дорогостоящий, поэтому на практике к нему прибегают лишь довольно крупные организации, располагающие достаточными ресурсами.

Говоря о предотвращении непредумышленных утечек организационными методами, нужно упомянуть такой немаловажный аспект, как повышение осведомленности персонала по вопросам информационной безопасности. Среди наиболее часто применяемых в комплексном подходе мер можно отметить инструктаж и ознакомление новых сотрудников с основными положениями и регламентами, регулярное обучение и тренинги как внутри компании, так и с привлечением внешних специалистов (курсы по повышению осведомленности можно найти в программах многих ведущих учебных центров). Наконец, помимо первичного знакомства с базовыми принципами и регулярных тренингов необходимо организовать постоянное информирование персонала путем электронных рассылок, публикаций на внутреннем портале,

наглядной агитации и другими доступными средствами.

Возвращаясь к чисто техническим методам, нужно отметить, что «волшебную таблетку», решающую все проблемы с утечками сразу, пока не удалось создать ни одному разработчику, несмотря на заявления в рекламных буклетах и на презентациях.

При техническом подходе важны комплексность и четкое целеполагание – любая система защиты будет эффективной только лишь при работе в тесной связке с остальными компонентами общей системы обеспечения безопасности, а при ее внедрении нужно заранее определить и принять ее реальные возможности и слабые места, не возлагая излишних неоправданных надежд.

Взвешенный и сбалансированный подход к выбору средств защиты от утечек информации предполагает классификацию информации в целях выделения действительно важной, нуждающейся в наибольшей защите, сужение круга лиц, допущенных к работе с ней, и ограничение количества потенциальных каналов ее распространения. Контроль явно выделенной из общего массива конфиденциальной информации при ее отправке конкретными сотрудниками по небольшому числу разрешенных каналов является гораздо более простой с технической точки зрения задачей, чем тотальная слежка за всем и всеми.

К сожалению, в реальных условиях такой подход имеет целый ряд ограничений, возникающих, в частности, из-за того, что в компании любого размера регулярно возникают все новые и новые данные, происходит ротация сотрудников, появляются новые бизнес-процессы и задействуются дополнительные каналы передачи и места хранения конфиденциальной информации в соответствии с требованиями бизнеса, например, как ответ на агрессивную конкурентную среду.

В таких условиях одним из возможных подходов является внедрение IRM-систем (Information Rights Management – управление правами доступа), позволяющих присваивать конкретным файлам права доступа на основе политик, определяющих, кто, когда, где и что имеет право делать с ними. Скажем, можно запретить чтение конкретного документа с мобильных устройств при подключении не к корпоративной сети Wi-Fi или запретить его редактирование в нерабочее время.

Жесткое ограничение разрешенных действий (копирование, чтение, снимок экрана и т. д.) достигается при помощи агентов, устанавливаемых на рабочие места, и их работы только после получения соответствующего разрешения от сервера политик (Policy Server). Использование IRM-систем позволяет защитить файл на всем пути его следования от одного пользователя до другого, причем при необходимости взаимодействия, например, с внешними клиентами либо партнерами, система фактически подменяет сам файл на ссылку, отправляемую по электронной почте или другим разрешенным каналом, что предотвращает утечку конфиденциальной информации в процессе ее передачи.

Большой сложностью при внедрении IRM-систем является организация процесса присвоения правильных политик доступа. В идеальной ситуации этим должен заниматься сам пользователь, являющийся автором документа: именно он (на основании предположения о его добронамеренности) лучше всех понимает, для кого предназначен вновь создаваемый документ и кто в соответствии с доведенными до него положениями и регламентами компании имеет право с ним работать.

> «Волшебную таблетку», решающую все проблемы с утечками сразу, пока не удалось создать ни одному разработчику.

Понятно, что в условиях реальной работы вряд ли можно ожидать неукоснительного выполнения всех требований по правильному определению и установке соответствующих разрешений. Именно по этой причине хороший практический синергетический эффект дает внедрение одновременно систем управления правами доступа и систем классификации информации, которые позволяют выявлять места хранения файлов в компании, анализировать их содержимое на предмет наличия конфиденциальной информации, правильно ее классифицировать и сообщать IRM-системе требуемые политики, за применением и соблюдением которых в дальнейшем система управления правами доступа и следит.

При работе с мобильных устройств установка дополнительных агентов затруднительна – как вследствие малой производительности самих устройств, так и в силу их архитектурных особенностей или требований производителя устройства, ограничивающего работу приложений сторонних разработчиков условной «песочницей», когда одно приложение оказывается изолированным от другого. При таком подходе никакой агент системы контроля не сможет отследить ни буфер обмена, ни текст, набираемый в соседнем приложении и отправляемый сотрудником вовне.

В подобных случаях разумно сочетание ограничения доступа с мобильных устройств путем выявления действительно требуемых ресурсов из общего пула корпоративных серверов и приложений, перенаправления всего трафика через серверы компании, где осуществляются глубокий его анализ и разбор (возможно использование и серверов облачных провайдеров, оказывающих услуги по очистке и контролю трафика), применения систем управления мобильными устройствами, позволяющих управлять использованием мобильных устройств сотрудниками в части установки требований к политикам безопасности и устанавливаемым приложениям, а также создавать отдельную замкнутую среду (часто в виде отдельного приложения) для работы со всеми корпоративными ресурсами организации.

В заключение отметим важность использования, вне зависимости от конкретных применяемых систем, приложений и сервисов, надежных решений по аутентификации пользователей. Никакая система управления правами доступа или система контроля утечек конфиденциальной информации не сможет работать эффективно, если на этапе проверки пользователя будет допущена ошибка и за легитимного сотрудника будет признан злоумышленник. Усиление классической парольной аутентификации за счет использования дополнительных факторов аутентификации (SMS, мобильное приложение, одноразовый код и т. п.) существенно снижает риски, возникающие при взломе/подборе/краже паролей пользователей. Кроме того, современные единые платформы аутентификации позволяют эффективно решать проблему проверки подлинности пользователей при доступе с любых мобильных устройств и при их обращении как к внутренним, так и к внешним, например облачным, сервисам. ■

Мнение специалиста

Алексей КУРСКИХ,

руководитель направления «Дозор-Джет» Центра информационной безопасности, компания «Инфосистемы Джет»:

Статья, безусловно, описывает важность использования IRM. Однако стоит отметить несколько нюансов. Во-первых, конфиденциальная информация – это не только какие-либо конкретные «документы». Это – информация в самом широком смысле этого слова: слухи, картинки, сканы, факсы, фотографии, переписка людей, данные наблюдений за ними вне ИС предприятия, выписки из систем документооборота и клиент-банков и др. Во-вторых, «инсайдер» – прежде всего конкретный человек, сотрудник, имеющий доступ к определенной информации и желание ее куда-либо передать с корыстными целями.

Само по себе отслеживание жизненного цикла документов в организации – это неплохо. И даже, может быть, очень хорошо, поскольку позволяет навести порядок и в какой-то мере служит препятствием для утечки документов вовне. Хотя априори нелояльного сотрудника в этом смысле сложно остановить: та же фотосъемка документов на телефон с трудом контролируется средствами IRM. Хотя если пойти дальше и оборудовать все рабочие места камерами наблюдения, то и этот момент будет фиксироваться. А при повышенном уровне внимания к мониторам с камер можно будет отлавливать и факты физического выноса документов. Но запретить сотруднику запоминать и пересказывать кому-либо их содержание невозможно.

Следовательно, ИБ-департаменты должны прийти к той же мысли, к которой уже давно пришли все настоящие службы безопасности: нелояльных сотрудников нужно вычислять и применять к ним определенные организационные меры.

Возвращаясь к ИБ, стоит отметить, что технические средства вычисления потенциально нелояльных сотрудников уже существуют. В их числе:

- возможность автоматического вычисления уровня доверия к сотруднику;
- определенные инструменты для ИБ- и СБ-служб для вычисления нелояльных личностей информационными средствами (средствами продукта);
- инструменты для СБ-служб, позволяющие коррелировать данные, полученные посредством применения двух предыдущих пунктов, с данными, полученными за пределами информационного поля предприятия.