Защита от инсайдера

Три четверти случаев, связанных с утечкой или потерей конфиденциальных данных коммерческими организациями, обусловлены человеческим фактором: умышленными или случайными действиями сотрудников компании. Можно ли защититься от рисков, связанных со злоупотреблениями сотрудниками предоставленным им доступом?

В последние несколько лет специалисты по информационной безопасности уделяют самое пристальное внимание защите от инсайдеров. Внутренних нарушителей не останавливают ни межсетевые экраны, ни системы предотвращения и обнаружения атак. Годами выстраиваемая эшелонированная система обороны информационной системы от внешних нападений практически бессильна против сотрудника, совершенно легально имеющего доступ к конфиденциальной информации своей компании.

Сервис анализа статистики поисковых запросов «Яндекс» наглядно демонстрирует рост интереса пользователей Internet к этой теме за последний год: в июне 2007 года ежедневно фиксировалось 676 запросов по слову «инсайдер», а к октябрю этот показатель увеличился вдвое (1224) и максимальной отметки — 1778 запросов — достиг в апреле 2008 года.

Понятие «инсайдер» трактуется достаточно свободно, и это вносит путаницу в головы пользователей и покупателей систем информационной безопасности. Такое положение дел устраивает маркетологов, поскольку позволяет предлагать для защиты от инсайдеров широкий спектр решений, которые, вообще говоря, предназначены для других целей. Самим инсайдерам это тоже на руку, ведь бороться с неизвестным на порядок сложнее.

Интересную классификацию инсайдеров, помогающую четче определить этот термин, предлагает российская компания InfoWatch (см. таблицу). Специалисты компании в качестве критерия предлагают использовать наличие умысла и корысти в действиях. Такой подход позволяет лучше понять цели и мотивацию инсайдеров и выбирать средства защиты, которые будут максимально эффективны.

Классификация инсайдеров по критерию мотивации

Тип	Умысел	Корысть	Постановка задачи	Действия при невозможности похитить информацию
Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обиженный	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Да	Сам/Извне	Отказ/Имитация/Взлом
Внедренный	Да	Да	Извне	Взлом

Источник: InfoWatch.

Неосторожные

В других источниках встречается также название «халатные». Эти сотрудники создают незлонамеренные ненаправленные угрозы, то есть нарушают правила хранения

конфиденциальной информации, действуя из лучших побуждений. Самые частые инциденты, виновниками которых становятся такие нарушители, — это вынос информации из офиса для работы дома, в командировке и т. д., с дальнейшей утерей носителя или возможностью доступа членов семьи к этой информации. Ущерб от таких утечек может быть ничуть не меньше, чем от промышленного шпионажа. Столкнувшись с невозможностью скопировать информацию, такие нарушители обычно действуют по инструкции — обращаются за помощью к коллегам или системному администратору, и те объясняют, что вынос информации за пределы офиса запрещен. Против таких нарушителей действенными являются достаточно простые технические средства предотвращения каналов утечек: контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода—вывода.

Манипулируемые

Последние годы термин «социальная инженерия» чаще всего применяется для описания различных типов мошенничества в Сети. Однако манипуляции используются не только для получения обманным путем персональной информации пользователей: паролей, персональных идентификационных номеров, реквизитов кредитных карт и адресов. Кевин Митник, пожалуй, самый известный в прошлом хакер, а ныне консультант по информационной безопасности, считает, что именно социальная инженерия сегодня является бичом информационных систем.

Примеры, которые приводит Митник в своей книге «Искусство обмана», показывают, в частности, что «добросовестная» секретарша может по просьбе злоумышленника «для надежности» продублировать почтовое сообщение, содержащее конфиденциальную информацию, на открытый почтовый ящик, не задумываясь о том, что такое рвение может обернуться утечкой конфиденциальных данных. Другой пример манипуляции — ситуация, когда ничего не подозревающий подчиненный выполняет преступные приказы своего начальника (в данном случае именно начальник будет являться инсайдером) по отправке той или иной информации заинтересованной стороне.

Поскольку манипулируемые и неосторожные сотрудники действуют, исходя из своего понимания блага компании, два этих типа нарушителей иногда объединяют в тип незлонамеренных. Ущерб не зависит от намерений, зато от них зависит поведение нарушителя в случае невозможности осуществить свое действие. Столкнувшись с техническим блокированием попыток нарушить регламенты хранения и движения информации, манипулируемые сотрудники вполне могут обратиться за помощью к коллегам, техническому персоналу или руководству, которые в свою очередь укажут на недопустимость планируемых действий и, вполне возможно, пресекут попытку утечки.

Следующая группа нарушителей — злонамеренные, осознающие, в отличие от сотрудников, описанных выше, что своими действиями они наносят вред компании, в которой работают. По мотивам враждебных действий, которые позволяют прогнозировать их поведение, они подразделяются на три типа: саботажники, нелояльные и мотивируемые извне.

Саботажники

Саботажники (в других источниках — обиженные сотрудники) — это сотрудники, стремящиеся нанести вред компании из личных мотивов. Чаще всего такими мотивами становятся обида вследствие недостаточной оценки их роли в компании (недостаточного размера материальной компенсации, неподобающего места в корпоративной иерархии),

отсутствие моральной мотивации или отказ в выделении корпоративных статусных атрибутов (ноутбука, автомобиля, личного секретаря и пр.).

Для оценки моделей поведения нарушителя-саботажника отметим два ключевых отличия: во-первых, сотрудник не собирается покидать компанию и, во-вторых, цель сотрудника — нанести вред, а не похитить информацию. Другими словами, он стремится к тому, чтобы руководство не узнало, что утечка произошла из-за него, и, столкнувшись с технической невозможностью похитить информацию, он может направить свою разрушительную энергию на что-нибудь другое, например, уничтожить или фальсифицировать доступную информацию или похитить материальные ценности. При этом сотрудник, исходя из собственных представлений о ценности информации и нанесенном вреде, определяет, какую информацию имеет смысл похитить и кому ее передать. Чаще всего он передает ее представителям прессы или теневых структур, соответственно цель таких действий — разглашение корпоративных тайн или шантаж. Примером может служить передача экологической прессе данных о состоянии затопленных ядерных подводных лодок одним из сотрудников предприятия, ответственного за мониторинг этого состояния.

Нелояльные

В последнее время увеличилось число похищений интеллектуальной собственности высокотехнологичных европейских и американских компаний стажерами из развивающихся стран, поэтому временных сотрудников иногда также относят к этому типу. По нацеленности угроза, исходящая от таких нарушителей, является ненаправленной — нарушители стараются унести максимально возможное количество доступной информации, часто даже не подозревая о ее ценности и не имея представления, как ее потом использовать.

К этому же типу относятся и сотрудники, которые, решив сменить место работы, еще не сообщили об этом начальству и коллегам, но уже начали действовать в своих интересах в ущерб компании. Самый частый способ получить доступ к информации или скопировать данные (если такая возможность не предусмотрена должностной инструкцией) — это имитация производственной необходимости. От предыдущего типа нелояльные нарушители отличаются в основном тем, что, похитив информацию, они не скрывают данного факта. Более того, иногда похищенная информация используется как залог комфортного увольнения — с компенсацией и рекомендациями — либо как способ повысить свою оценку у нового работодателя, например, имея на руках клиентскую базу с предыдущего места работы. Иногда получить контакты всех клиентов компании бывает не так сложно, как кажется на первый взгляд. Конечно, в системах CRM и ERP информация надежно защищена, и доступ к ней, особенно в консолидированном виде, строго контролируется. Однако раз в год все контакты выгружаются в обычный файл Excel для рассылки новогодних поздравлений, и этот файл, как правило, хранится на локальном компьютере ассистента отдела маркетинга — обычно юной особы — и подчас, чтобы втереться к ней в доверие, бывает достаточно коробки конфет.

Но наибольшую опасность представляют не эти два типа нарушителей. Саботажники и нелояльные сотрудники все же сами определяют информацию для похищения и место ее «сбыта». Коммерческий директор, решивший уволиться, унесет с собой базу данных клиентов, но, возможно, он найдет работу в компании, напрямую не конкурирующей с нынешним работодателем. Переданная прессе саботажником информация может и не оказаться сенсацией, а значит, не будет напечатана. Стажер, похитивший чертежи перспективной разработки, может не найти на них покупателя. Во всех этих случаях утечка

информации не нанесет вреда владельцу. Более того, еще на этапе реализации своего плана, наткнувшись на невозможность похитить информацию, нарушители вряд ли будут искать технический способ обойти защиту, к тому же, скорее всего, они не обладают должной технической подготовкой.

Однако, если еще до похищения информации саботажник или нелояльный сотрудник выйдет на потенциального покупателя конкретной информации, будь то конкурент, пресса, криминальные структуры или спецслужбы, он становится самым опасным нарушителем — мотивированным извне. Теперь его дальнейшая судьба — работа, благосостояние, а иногда жизнь и здоровье напрямую зависят от полноты и актуальности информации, которую он сможет похитить.

Нарушители, мотивированные извне

Мотивированные извне — это сотрудники, цель которым определяет заказчик похищаемой информации. К этому типу сотрудников относят внедренных, то есть специально устроенных на работу для похищения информации, и завербованных, то есть изначально лояльных, но впоследствии подкупленных или запуганных. Опасность, которую представляют нарушители этого типа, заключается в том, что в случае технических ограничений на вынос информации за пределы корпоративной информационной сети «заказчики» могут снабдить их соответствующими устройствами или программами для обхода защиты.

Технические средства защиты

В литературе продукты, обеспечивающие защиту от инсайдеров, делятся на классы и сегменты по-разному. Рассмотрим основные, при этом особое внимание уделим практической стороне вопроса, а именно эффективности решения поставленной задачи.

Системы предотвращения утечек

Решения, относящиеся к классу систем предотвращения утечек (Anti Data Leakage, ADL, в некоторых источниках Anti-Leakage Software), предназначены для контроля электронной почты, Internet-трафика, мобильных носителей информации, принтеров и других каналов.

Суть их работы состоит в том, чтобы отслеживать локальные действия сотрудников с файлами и их сетевую активность. Система может, например, анализировать все операции по сохранению, печати или копированию файлов на внешний носитель и при обнаружении несанкционированных действий заблокировать попытку и уведомить об этом сотрудника по безопасности. Аналогично проверяются отправляемые электронные письма и исходящий трафик. Эффективный контроль возможен только при глубоком анализе с использованием так называемой контентной фильтрации. Помимо внешних атрибутов документа (его размер, тип и т.п.) проверяется наличие ключевых слов, а также сходство с документами, которые заведомо являются секретными и хранятся в специализированной базе системы.

Наполнение базы и выбор ключевых слов — важные моменты при внедрении подобной системы, ведь от правильности выбора запрещенных слов и полноты базы с образцами секретных документов фактически зависит работоспособность системы в дальнейшем.

К сожалению, гарантировать стопроцентную защиту от утечек информации не способна ни одна из подобных систем. Нарушитель может попытаться выслать файл в измененной виде: например, провести транслитерацию документа, «разбавить» его случайными

словами, перевести на иностранный язык автоматическим переводчиком — простор для фантазии огромный. Провести настолько глубокий анализ измененного до неузнаваемости отправляемого файла, чтобы предотвратить утечку, не представляется возможным, ведь в арсенале инсайдера, помимо рассмотренных, есть и другие методы: шифрование, отправка документа в виде картинки (например, снимок экрана), использование многократного архивирования, перевод файла в «экзотические» форматы.

Разработчикам систем предотвращения утечек приходится добавлять все новые и новые проверки для того, чтобы их продукты были адекватны возникающим угрозам. Отчасти такое противостояние напоминает извечную борьбу авторов вирусов и специалистов антивирусных компаний. Постоянно изобретаются новые методы и приемы и с завидной регулярностью выходят обновления сигнатурных баз и эвристических анализаторов. Однако не стоит забывать, что контекстный (морфологический, лексический и др.) анализ является крайне ресурсоемкой операцией. Задержка в несколько минут для электронного письма не будет так заметна, а вот низкая скорость файловых операций и значительные задержки при работе в Internet совершенно немыслимы.

Итак, данный класс решений способен эффективно бороться со случайными утечками, то есть с незлонамеренными инсайдерами (неосторожными и манипулируемыми). Саботажники и нелояльные уже могут попытаться обойти запреты системы, но подвергать себя серьезному риску или идти напролом, скорее всего, не будут.

Эффективность же решений ADL против нарушителя, мотивированного извне, вооруженного специализированным ПО вкупе с креативным мышлением, будет на порядок меньше. Можно прогнозировать, что в случае широкого распространения подобных систем инсайдеры начнут «холодную войну», разрабатывая новые способы обойти защиту. То, что при этом злоумышленники всегда будут на шаг впереди, к сожалению, почти не вызывает сомнений.

Средства строгой аутентификации

Немаловажным фактором при принятии инсайдером решения о совершении злодеяния является ощущение собственной безнаказанности. Многие специалисты по информационной безопасности сегодня сходятся во мнении, что для предотвращения преступления важна не тяжесть наказания, а его неотвратимость.

Если в организации применяются пароли, которые пользователи ежедневно вводят, чтобы получить доступ в информационную систему, то доказать виновность злоумышленника будет затруднительно. Инсайдер всегда может сослаться на то, что его паролем мог воспользоваться кто-то другой, к тому же сам он при возможности будет использовать чужую учетную запись. Действительно, узнать пароль своего сослуживца не так сложно, как кажется. Зачастую его просто записывают на видном месте или сообщают, например, по телефону с просьбой проверить, нет ли в почте важного сообщения. На практике приходится сталкиваться и с ситуациями, когда целые отделы работают под одной-единственной учетной записью пользователя, потому что «так удобнее».

Внедрение строгой двухфакторной аутентификации с использованием аппаратных средств (смарт-карт или USB-токенов) само по себе дисциплинирует пользователя. Выданное устройство — это уже не пароль, и даже психологически передать его коллеге, да еще и сообщить соответствующий ПИН-код, не так просто, как раскрыть свой пароль. Если токены, как это принято в государственных организациях, выдаются под роспись, а сотрудникам

объясняется, что они несут ответственность за все действия в системе, выполненные под их учетными записями, то эффект будет еще сильнее.

Фактически при использовании аппаратных средств аутентификации пользователь ставит свою электронно-цифровую подпись (ЭЦП) под всеми своими действиями, будь то отправка письма или копирование файла с сервера на мобильный носитель. Впоследствии при возникновении инцидента работодатель сможет найти того, кто именно похитил информацию и доказать его вину.

Важно отметить, что внесение в информационную систему компании дополнительного элемента в виде устройств аутентификации не требует кардинальных изменений в инфраструктуре, так как большинство современных программных продуктов, производимых мировыми вендорами, имеет нативную (встроенную) поддержку смарт-карт и USB-токенов. Внедрение системы строгой аутентификации позволяет максимально полно использовать возможности по обеспечению безопасности, реализованные, например, в продуктах Microsoft, Cisco, Check Point, Citrix и др.

Так как основной способ противодействия утечкам лежит в области психологии, то подобное решение наиболее эффективно позволит бороться с нелояльными и саботажниками, то есть теми, кто осознают, что делают. Из страха быть раскрытыми они попробуют

добиться своих целей не путем кражи информации, а другими способами. Напрямую нарушителей, мотивированных извне, средства строгой аутентификации не остановят, но позволят привлечь их к ответственности в случае необходимости.

Системы контроля побочных каналов

В отличие от систем предотвращения утечек, данный класс решений целиком блокирует каналы утечек в соответствии с политиками организации, ведь избавившись от побочных нежелательных и трудно контролируемых каналов утечек конфиденциальных данных, можно сосредоточиться на контроле основных.

Примером такого решения может быть специализированное программное обеспечение, не позволяющее пользоваться внешними сменными носителями. Как правило, такие средства имеют возможности тонкой настройки разрешений и запретов по группам пользователей, типам носителей, размерам файлов, а также времени и дням недели. При правильных настройках и грамотном внедрении риски хищения ценной информации практически полностью исключаются — с условием, что рабочие места пользователей не имеют связи с внешним миром.

Тенденция, однако, такова, что таких изолированных рабочих мест с каждым днем становится все меньше. Лишить сотрудника, например, электронной почты и доступа в Internet невозможно, но установить границы дозволенного — прямое право работодателя.

Современные высокотехнологичные продукты в области информационной безопасности и контентной фильтрации позволяют корректно, в строгом соответствии с политикой корпоративной безопасности, запретить:

- использование Internet-пейджеров;
- отправку вложений, защищенных паролями;
- пересылку файлов определенных форматов с проверкой по бинарной структуре файла;

- программы для удаленного управления и туннелирования трафика;
- SIP-телефонию (Skype);
- использование клиентов файлообменных сетей (P2P);
- передачу информации на внешние ftp-серверы и др.

Более того, предусмотренная категоризация Web-ресурсов оградит сотрудников от посещения сайтов, не связанных с работой (развлекательные порталы, ресурсы для скачивания потокового аудио и видео и др.). Помимо этого, современные контентные фильтры позволяют контролировать деятельность сотрудника в сети (например, не дают вводить свои реквизиты на сомнительных ресурсах) и обладают функциональностью по разграничению запретов для разных групп пользователей.

Подобные продукты могут иметь дополнительный функционал по фильтрации спама, многоуровневой защите от шпионского программного обеспечения, «троянов» и т.п. Стоит отметить, что этот класс продуктов одинаково эффективен против всех типов нарушителей: использование ICQ или отправку файлов можно запретить всем сотрудникам и никаким самым изощренным способом этот запрет обойти не удастся. Другое дело, что тотальный запрет порой невозможен и для отдельных групп пользователей приходится идти на послабления.

Ключевые тенденции

Рассмотренная классификация инсайдеров помогает лучше понять, какие требования необходимо предъявлять к программным продуктам, призванным с ними бороться. Заметим, что за рамками данной статьи остались решения для контроля нецелевого использования ресурсов сети, системы управления правами доступа, продукты для архивирования почтовой корреспонденции и многие другие смежные сегменты, например, обеспечивающие шифрование информации.

Каждый тип продукта служит для решения конкретной задачи, но максимальный эффект достигается при использовании комплексных решений. В последние годы наметилась устойчивая тенденция роста закупок решений, борющихся с утечками не на локальных рабочих местах, а на шлюзах компании. Несмотря на стремление крупных игроков к разного рода слияниям, влекущим расширение функционала существующих решений за счет возможностей продуктов от поглощаемых компаний, далеко не всегда «гибридное» решение оправдывает себя. К тому же текущий уровень разработки программного обеспечения пока позволяет создавать высокоэффективные и надежные решения только для узкого круга задач, а попытки сделать «комбайны», то есть продукты, объединяющие все в одном «флаконе», пока не очень успешны.

В связи с этим наиболее интересны решения, которые легко интегрируются с другими. Возможно это только в том случае, если решение поддерживает промышленные стандарты, например LDAP-каталоги для хранения информации, имеют возможность кластеризации стандартными методами, а программное обеспечение совместимо с современными серверами или, что предпочтительнее, поставляется предустановленным на аппаратные платформы вендора, то есть в виде «приставок» (appliances).