ВАСИЛИЙ ЛУКИНЫХ,
менеджер по развитию бизнеса Solar Dozor компании Solar Security

Профилактика корпоративных мошенничеств с помощью DLP-системы

В 2016 году компания KPMG International представила исследование, в котором дала типовой портрет злоумышленника: в 79 % случаев это оказывается мужчина; в 69 % нарушитель принадлежит к возрастной группе 36–55 лет. Причем часто речь идет о «старожиле» – 38 % злоумышленников проработали в компании более 6 лет.

SHUTTERSTOCK.COM/VLADWEL

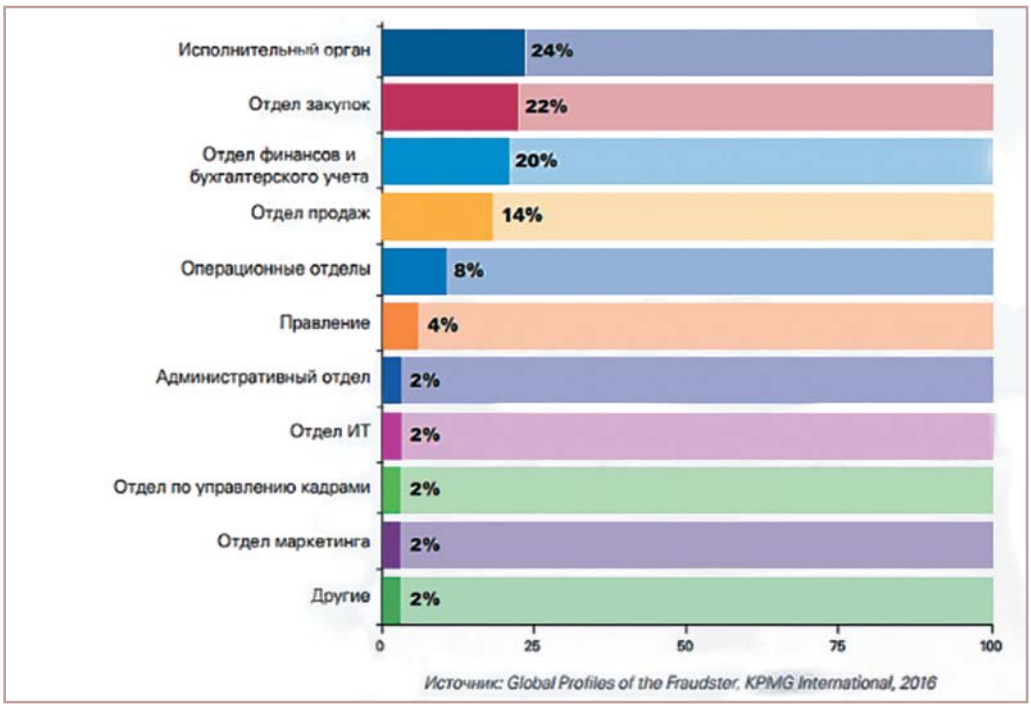
Психологический потрет нарушителя также довольно любопытен: 60 % сотрудников к мошенничеству подталкивает возможность получить личную выгоду, 36 % просто относятся к категории алчных людей, постоянно ищущих пути к обогащению, в 27 % случаев люди также руководствуются чувством превосходства и ощущением безнаказанности, их мотивация описывается фразой «because I can». Как правило, такие сотрудники уверены в себе и находятся на хорошем счету в организации.

В 62 % случаев злоумышленник вступает в сговор с третьими лицами. Это могут быть коллеги, подрядчики или клиенты (впрочем, женщины в 45 % случаев предпочитают действовать в одиночку). Рейтинг наиболее рисковых подразделений с точки зрения мошеннических действий выглядит следующим образом: в топ-3 входят топ-менеджмент (24 %), отдел закупок (22 %) и финансовый отдел (20%). За ними следуют отдел продаж (14 %), операционные отделы (8 %) и прочие.

Исследование KPMG International утверждает, что причиной большинства мошеннических действий со стороны сотрудников является слабое распространение технологий предотвращения внутренних угроз, в особенности технологий анализа данных с целью превентивного выявления потенциальных злоумышленников. Именно изучение и внедрение данных технологий в Solar Dozor находится в фокусе стратегических разработок и перспективных исследований Solar Security.

Есть вещи, которые кардинально отличают нас от конкурентов, среди них – группы особого контроля (например, группа «на увольнение»), работа с которыми находится на очень высокой степени автоматизации.

РИС. 1. РЕЙТИНГ РИСКОВЫХ ПОДРАЗДЕЛЕНИЙ ВНУТРИ ОРГАНИЗАЦИИ



В группу «Поиск работы» система добавляет человека автоматически, как только он переходит в активную стадию поиска. Пока он просто просматривает вакансии, это не так критично, как если система фиксирует, что сотрудник активно рассылает резюме по другим компаниям.

У нас есть своя статистика, согласно которой 97 % людей, которые переходят к активному поиску работы, начинают красть корпоративную информацию, причем часто любую, к которой имеют доступ. Наиболее активный слив происходит в последние несколько дней до окончания работы. Этот пример иллюстрирует, как одно действие позволяет довольно достоверно спрогнозировать другое. Выявление факта активного поиска работы, перемещение в группу особого контроля, ужесточение политик информационной безопасности в отношении сотрудника – все это происходит автоматически.

По нашему опыту, в отношении внутренних нарушителей всегда работает правило 10–80–10. Его суть в том, что 10 % сотрудников будут заниматься мошенничеством всегда и в любой компании, это их осознанный выбор. Еще 10 % никогда не сделают чего-то подобного. Оставшиеся 80 % – это люди, которые скорее не склонны обманывать работодателя, но под давлением обстоятельств могут решиться на серьезное нарушение. Именно поэтому мы разрабатываем технологии профилирования сотрудников – чтобы выявить 10 % убежденных мошенников и выявить тот момент, когда кто-то из тех самых 80 % попадет в ситуацию, подталкивающую его к нарушению.

Второй важный момент – невозможно одинаково жестко контролировать всех сотрудников. Это даст большое количество ложных срабатываний и в разы увеличит нагрузку на офицера безопасности. Никаких ресурсов не хватит на то, чтобы отработать все инциденты. А вот выделить группу вероятных нарушителей и поставить их под прицельный контроль – причем сделать это автоматически – вполне реально.

Профилирование действий сотрудников

Одной из ключевых возможностей аналитики Solar Dozor является выявление «поведенческих флажков», по которым сотрудника можно отнести к той или иной группе риска. С точки зрения DLP-решения, деятельность человека на рабочем месте сводится к переписке по корпоративной и личной почте, коммуникациям в сети Интернет, действиям на рабочей станции и работе с различными документами в локальной файловой системе и облачных хранилищах. Все эти активности проходят фильтрацию и сохраняются в архиве. Все события по конкретному человеку сводятся воедино, тем самым Solar Dozor фактически формирует досье на каждого сотрудника. Оно содержит собственные данные DLP-системы и информацию из смежных систем – например, сведения о дате приема на работу, привилегированных правах доступа к информационным системам и пр. Офицер безопасности может в любой момент открыть досье и получить сводную всестороннюю характеристику сотрудника.

Сигнал тревоги

Но чтобы заблаговременно выявить вероятного нарушителя, надо знать, что искать. Что же указывает на потенциального нарушителя? По статистике Accosiation of Certified Fraud Examiners (ACFE), в первую очередь это несоответствие расходов и доходов человека. Покупки в интернет-магазинах, поисковые запросы, фото в социальных сетях с новым автомобилем или дорогими аксессуарами – все это сигналы того, что человек живет не по средствам. Это может быть признаком обычной расточительности, но, по статистике ACFE, 44 % нарушителей тратили больше, чем официально зарабатывали, так что такие сигналы требуют внимания безопасника.

Те из сотрудников, кто не замечен в неожиданно крупных тратах, но испытывает финансовые трудности, находятся на втором месте по уровню риска – они составляют около трети мошенников.

РИС. 2. ПОВЕДЕНЧЕСКИЕ «КРАСНЫЕ ФЛАЖКИ»

Даже личные связи с поставщиками и заказчиками реже оборачиваются нелегитимными действиями, направленными против компании, – в 21 % случаев.

Примерно так же часто возникают проблемы с людьми, которые категорически не готовы делегировать полномочия. Такой подход не только грозит проблемами с дедлайнами, но также служит признаком того, что в деятельности сотрудника не все чисто.

Такие обстоятельства, как развод и другие проблемы в семье, были отмечены у 17 % нарушителей, а различные зависимости (от алкоголя до игромании и членства в секте) – у 12 %. Однако поводом насторожиться могут быть не только внешние обстоятельства, но и черты характера, особенности личности сотрудника. В 18 % случаев у внутренних нарушителей отмечалась склонность к авантюризму, в 15 % – раздражительность и подозрительность.

Более редкими, но не менее значимыми являются такие признаки, как стрессовая нагрузка на работе, отказ брать отпуск, неудовлетворенность уровнем заработной платы и некоторые другие.

Сотрудников, в отношении которых выявлены данные факторы, мы относим к группам риска. Отдельно хочется отметить, что иногда принадлежность к той или иной группе сама по себе некритична. Например, ключевой сотрудник, имеющий доступ к важной для компании информации, выплачивает ипотеку. Само по себе это некритично, не так ли? А теперь представим, что этот же человек переживает сложный развод. Очевидно, что и уровень риска мошенничества со стороны этого сотрудника возрастает. Таким образом, когда к одному профилю добавляется другой, их критичность по совокупности может сильно возрасти. Если у человека, почти выплатившего ипотеку, кардинально меняются внешние обстоятельства, он с большой вероятностью пойдет на противоправное действие, чтобы сохранить то, во что уже вложено столько денег и сил.

Рассмотрим чуть подробнее, как Solar Dozor выявляет принадлежность сотрудника к той или иной групп на примере самых опасных «красных флажков».

Группа риска «Несоответствие расходов и доходов»

Тот факт, что человек живет не по средствам, определяется благодаря его расходам. Информация о них аккумулируется из различных источников. Это может быть переписка с риэлтором или менеджером по продаже в различных мессенджерах или почте. Поисковые запросы, серфинг по тематическим сайтам часто указывают на то, что человек всерьез обдумывает крупную покупку.

Может прозвучать неожиданно, но еще один тревожный звоночек – это частое посещение сайтов эскорт-услуг. На каждом втором пилоте мы выявляем сотрудников, которые тратят на эти развлечения суммы, не соответствующие их доходам. Вторая проблема состоит в том, что такое времяпрепровождение может компрометировать человека, занимающего высокую позицию в крупной компании, а любой компромат – это возможность вербовки. Если речь идет, скажем, об ОПК, эти риски могут обернуться очень серьезными последствиями.

Офицер безопасности может в любой момент получить сводную характеристику сотрудника

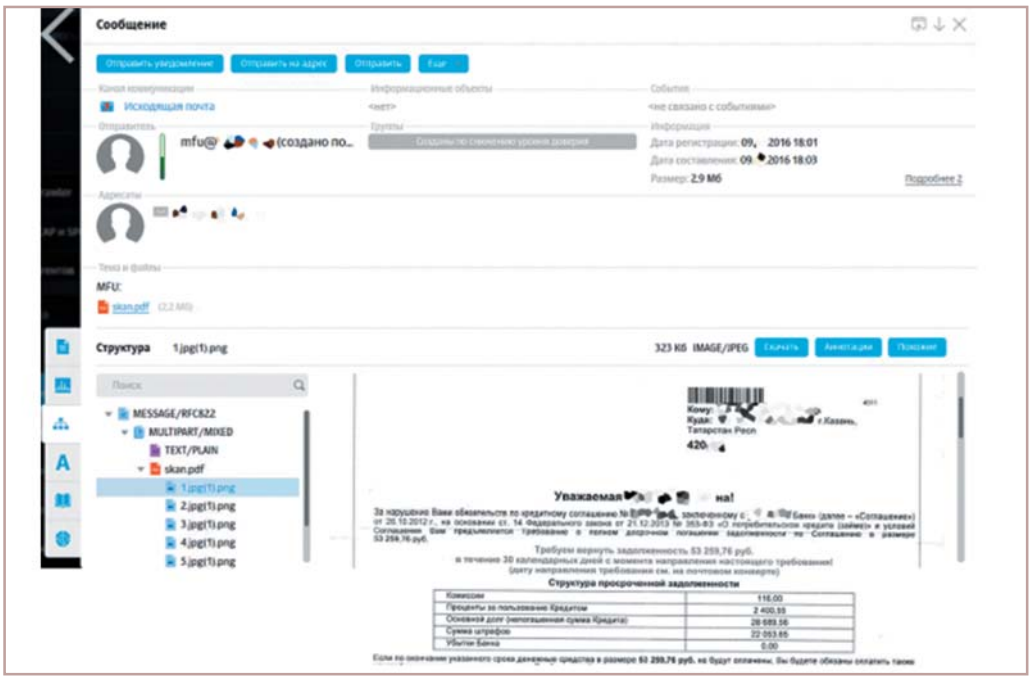
Что характерно, эти действия сотрудники осуществляют без малейшего страха и стремления что-либо скрыть, даже если знают о том, что в компании работает DLP-система. Поскольку технически все это не является утечкой информации, такая активность оказывается вне поля зрения большинства DLP-решений. И если даже DLP ее детектирует, то оценивает как незначительное нарушение (посещение нерабочих сайтов), и информация об этом теряется в ворохе логов, ускользая от внимания офицера безопасности.

Группа риска «Финансовые сложности»

Сотрудники с финансовыми сложностями есть практически в каждой организации. Анализ лексики помогает и здесь. С его помощью можно выявить в коммуникациях сотрудника просьбы о займах, банковские требования о погашении задолженности или кредита, обсуждение возможности перекредитования.

На одном из проектов был случай, когда сотрудник регулярно рассылал коллегам письма с просьбой одолжить денег. В письмах приводились разные описания затруднительной ситуации, в которую якобы попал человек, причем легенды различались в зависимости от того, кто был адресатом – мужчина или женщина. Постепенно круг адресатов стал расширяться с коллег на партнеров и даже заказчиков.

РИС. 3. СКАНИРОВАНИЕ НА КОРПОРАТИВНОМ МФУ ДОКУМЕНТА О ЗАДОЛЖЕННОСТИ БАНКУ



С помощью лингвистического анализа Solar Dozor отнес сотрудника к группе «финансовые сложности», а офицер безопасности, в свою очередь, увидел, что человек не просто просит денег в долг, но делает это регулярно и, более того, с помощью заранее заготовленных шаблонов. Через некоторое время сотрудник попал в еще одну группу контроля – игромания, и все окончательно встало на свои места.

Вторая технология – мониторинг поисковых запросов и посещения тематических сайтов. Это может быть поиск услуг по подготовке документов, мониторинг банковских услуг перекредитования, посещение форумов, на которых обсуждаются подобные жизненные ситуации. Еще один источник информации – корпоративные периферийные устройства, которые часто используются сотрудниками в личных целях.

Группа риска «Терроризм и деструктивные секты»

Сотрудники, занимающиеся мошенничеством, не часто оказываются связаны с террористическими организациями, и потому эта группа стоит несколько особняком. Однако очевидно, что каждый работодатель хочет знать, если ли такие люди в его коллективе, поэтому довольно много запросов от заказчиков связаны с выявлением сотрудников, поддерживающих террористические организации.

Как мы это делаем? Прежде всего Solar Dozor отслеживает посещение сайтов и групп в соцсетях, принадлежащих радикальным религиозным организациям. Весь объем коммуникаций сотрудников – как с коллегами, так и на интернет-форумах – анализируется на предмет употребления характерной лексики. Наконец, для контроля принадлежности сотрудников к этой группе очень полезен мониторинг загружаемых из интернета файлов или документы, отправляемые на печать, поскольку часто это оказываются книги соответствующего содержания.

Мониторинг сотрудников на предмет интереса к деструктивным религиям и экстремистским идеологиям – функциональность, очень актуальная для оборонных предприятий. Еще в 2015 году таких запросов было сравнительно немного, но в прошлом году они выделились в отдельный сильный тренд, и это вполне логично. Скажем, на одном из заводов, изготавливающих взрыватели, Solar Dozor выявил сотрудника, который активно интересовался экстремистской идеологией. Понятно, что о таких сотрудниках очень важно вовремя узнавать, чтобы поставить их на особый контроль.

Профилирование сегодня и завтра

Очень важно понимать, что какие-либо выводы о сотруднике можно сделать, только опираясь на общую картину, оценивая всю совокупность признаков и «красных флажков». На данный момент отнесение к группе риска – это автоматизированное, но не автоматическое действие. Это значит, что итоговый вывод о вероятности наступления рисков со стороны того или иного сотрудника все равно должен делать человек. Задача DLP-системы – предоставить ему всю информацию «в одном окне», чтобы не приходилось тратить большое количество времени и сил на ее сбор и анализ.

И все же за профилированием действий пользователей будущее DLP-систем. Заказчиками DLP-решений, как правило, являются достаточно зрелые компании со штатом в несколько тысяч пользователей и развитой ИТ-инфраструктурой. Вследствие этого офицер безопасности вынужден работать с огромными объемами данных и оповещений и легко может упустить незначительную на первый взгляд деталь, которая могла бы помочь предотвратить нарушение. Описанные технологии позволяют упростить работу службы ИБ, заблаговременно сузив круг внимания до тех сотрудников, которые должны находиться под особым контролем, а значит, плавно перейти от расследований инцидентов к их предотвращению на ранней стадии, то есть до того, как компании будет нанесен ущерб. ●