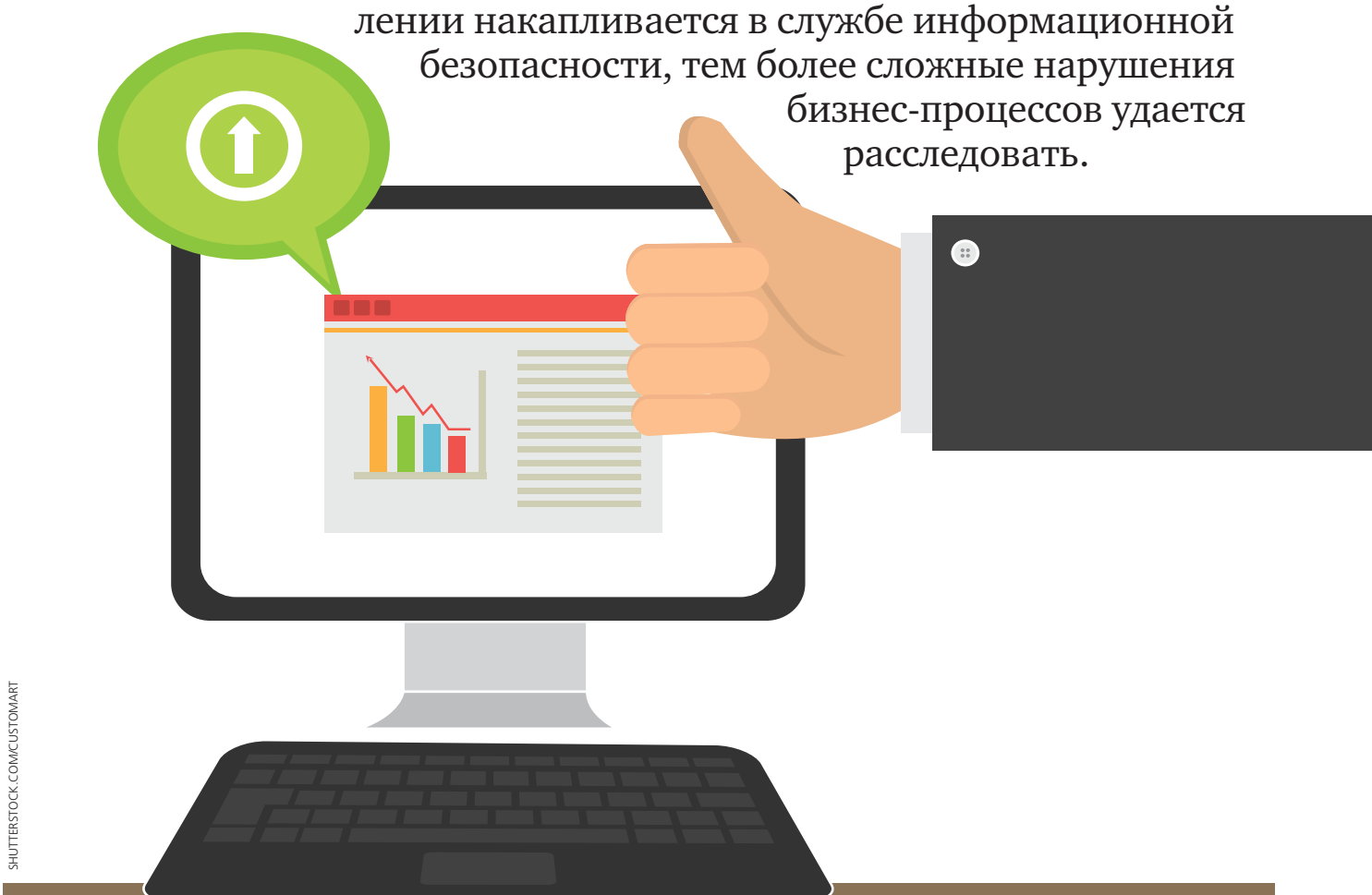
ГАЛИНА РЯБОВА,
руководитель направления Solar Dozor компании Solar Security

Применение DLP для расследования мошенничества с дебиторской задолженностью

Традиционно программные комплексы для борьбы с утечками информации (Data Loss Prevention) успешно применяются для контроля распространения конфиденциальных данных и анализа коммуникаций сотрудников компании. И чем больше опыта в этом направлении накапливается в службе информационной безопасности, тем более сложные нарушения бизнес-процессов удается расследовать.



SHUTTERSTOCK.COM/CUSTOMART

Одним из таких примеров могут служить всевозможные мошеннические схемы с участием контрагентов, например безосновательное увеличение кредитной линии, лоббирование интересов. При этом важно понимать, что в одних случаях сотрудник вашей компании может выступать как наивная жертва, а в других – как активный соучастник преступления против организации.

В первую категорию очень часто попадают молодые специалисты, которые дорожат выстроенными отношениями и могут идти на поводу у более опытных и злонамеренных коллег по рынку. Помочь избежать подобных ситуаций поможет сравнительный анализ формальных историй работы с клиентом и реальной переписки с ним. Ведь очень часто на бумаге картина, описанная человеком, выглядит идеально, в действительности компания-контрагент не перестает получать товар, а ее кредитная линия продолжает расти. Кроме того, в реальной переписке могут быть интересные детали, которые для опытного безопасника являются «красными флажками» возможного мошенничества, но которые не заметит ни один менеджер.

Гораздо страшнее, когда ВАШ сотрудник умышленно продвигает интересы своих сообщников, ведь в таких случаях злоумышленник будет стараться всеми способами скрыть реальные причины своих действий. Когда речь идет об умышленном сговоре сотрудника с контрагентом, всегда есть причина такого поведения. Наиболее частыми основаниями становятся:

- Ценное вознаграждение (откат, дорогие подарки и т. д.).
- Поддержание прочных социальных связей (помощь родственникам, друзьям).
- Постоянно действующие мошеннические схемы.

Тем не менее всех злоумышленников всегда объединяет один тревожный признак зарождающейся угрозы – их коммуникации приобретают более неформальную окраску. Сотрудники меньше переписываются по корпоративной электронной почте, а все больше через личную почту, мессенджеры или социальные сети. Таким образом, в поле зрения руководителя попадает только заметная невооруженным глазом деловая активность – заметки о регулярных контактах, зарегистрированные в CRM, и отчеты о проделанной работе. Но в таких критичных вопросах всегда важно иметь альтернативный взгляд на бизнес-процесс, понимать, насколько он прозрачен, нет ли теневой стороны отношений между компаниями.

Узнать, как реально обстоят дела в отношениях между представителями двух организаций, поможет анализ рабочих и неформальных коммуникаций сотрудников с применением DLP-системы.

Всех злоумышленников всегда объединяет один тревожный признак зарождающейся угрозы – их коммуникации приобретают более неформальную окраску

Специалист службы ИБ, имея в своем арсенале такое решение, сможет без труда заметить нарушения и неявные признаки обмана со стороны контрагента, быстро провести расследование и собрать доказательства. Давайте рассмотрим один из примеров, который недавно произошел с нашим клиентом.

Случай из практики

Не так давно к нам обратился клиент «М» – крупная оптово-розничная компания в сегменте FMCG, с просьбой помочь провести достаточно необычное расследование. У руководителя отдела сбыта закрались подозрения в том, что причина дебиторской задолженности у ряда клиентов – лоббирование их интересов в ущерб компании.

Для справки: дебиторская задолженность (англ. Accounts receivable (A/R)) – сумма долгов, причитающихся предприятию, фирме, компании со стороны других предприятий, фирм, компаний, а также граждан, являющихся их должниками, дебиторами[1], что соответствует как международным, так и российским стандартам бухгалтерского учета.

Дебиторская задолженность в торговле – явление вполне обычное, но, когда суммы долга клиента начинают расти, а сроки оплаты постоянно переносятся, тут уже руководители начинают волноваться не на шутку.

Первым тревожным звоночком становится нехватка собственных оборотных средств, а в самых запущенных случаях, по словам представителя торговой компании «М», приходится брать кредит на выплату заработной платы сотрудникам в условиях возникновения кассового разрыва.

Таким образом, компания сама залезает в долги и платит по нынешним временам достаточно высокие проценты по займу, а в то же время кредитует своих контрагентов совершенно бесплатно.

Осознав всю серьезность происходящего, руководство обратилось в службу безопасности с

Такое программное обеспечение позволяет контролировать коммуникации сотрудников на рабочих местах и обладает богатым функционалом для выявления ранних признаков мошенничества

SHUTTERSTOCK.COM/CUSTOMART

целью проверки деятельности сотрудников, отвечающих за отношения с дебиторами.

Основным инструментом в ходе данного расследования послужила система для борьбы с утечками информации класса Data Loss Prevention – Solar Dozor. Такое программное обеспечение позволяет контролировать коммуникации сотрудников на рабочих местах и обладает богатым функционалом для выявления ранних признаков мошенничества и распутывания сложных схем.

Начинаем расследование

Шаг 1. Свое расследование совместно со службой безопасности компании «М» мы начали с составления списка компаний-должников и подбора адресов их веб-сайтов, которые дали нам список доменов их корпоративной электронной почты (список 1). Таким образом, после определения рисковых активов у нас появилась некая зацепка и ряд гипотез, которые мы в дальнейшем проверили.

Результат: список доменов электронной почты компаний-должников.

Шаг 2. Резонно предположить, что сотрудники компании «М» общаются со своими коллегами из компаний-должников через рабочую электронную почту. Чтобы вытащить все такие коммуникации, мы произвели поиск по архиву коммуникаций за последние полгода. Далее был создан фильтр, который выдал нам всю переписку наших сотрудников с адресами электронной почты из списка 1.

имя@M-company.ru <-> имя @debtcompany.ru

Результат: список менеджеров нашей компании и список контактов в компаниях-должниках.

Шаг 3. Кроме электронной почты, наши менеджеры вполне могут общаться со своими контактерами через веб-почту. Поэтому по всему списку менеджеров ищем переписку с адресами в публичных доменах электронной почты (mail.ru, gmail.com и т. д.).

При этом дополнительно вводим ФИО сотрудников компаний-должников в качестве параметра поиска.

Результат: ветки переписки наших менеджеров с представителями компаний-должников.

Шаг 4. По каждому менеджеру проводим анализ его переписки с сотрудниками должника на предмет наличия неформального общения, перевода разговора в неконтролируемые каналы – «давай по телефону», «лучше при встрече» и т. д., предложения помощи в решении проблем.

Результат: подтвержденные неформальные контакты.

Шаг 5. Проводим тщательный анализ контактов и изменений статусов по дебиторской задолженности конкретных менеджеров и компаний-должников. Особое внимание уделяем фактам постепенного увеличения лимитов отгрузки. На этом этапе появляются подозреваемые, следовательно, проверяем гипотезу о мошенничестве путем анализа переписки по лексике:

- Сговор.
- Лоббирование интересов контрагента в ущерб компании.
- Материальная заинтересованность.
- Сведения о ликвидации контрагента.

Результат: установлены конкретные сотрудники, действующие в интересах контрагентов, накоплена доказательная база для дальнейшего разбора инцидентов с руководителями.

Данное расследование помогло компании «М» выявить недобросовестных сотрудников и ускорить возврат задолженности контрагентами. Результаты проверки были доведены до сведения всех сотрудников организации. Узнав о ведущемся мониторинге, некоторые сотрудники пришли с повинной, признавшись в мелких нарушениях. Заработать хочется многим, но стабильная работа в кризис дороже. ●