ЕСТЬ РЕШЕНИЕ

История одного расследования

– А подать сюда Ляпкина-Тяпкина!
Н.В. Гоголь

НЕКОТОРОЕ ВРЕМЯ НАЗАД МНЕ ПРЕДСТАВИЛСЯ СЛУЧАЙ проконсультировать одну российскую компанию так называемого «среднего бизнеса». В силу естественного желания выглядеть лучше представители компании периодически изучают отзывы о своем предприятии на различных интернет-сайтах. В ходе мониторинга на известном сайте с отзывами о местах работы был замечен резко отрицательный отзыв о деятельности компании. Автор отзыва, под псевдонимом «Обобранный», писал, что компания «загнила и превратилась в семейный трест по прихватизации».

Собственно говоря, подобные отзывы не редкость, на них следует реагировать PR-менеджеру – специалисту по связям с общественностью. Однако в данном случае была указана информация о серьезных проблемах в компании. В комментарии к собственному отзыву «Обобранный» написал, что «боссы бабло не платят, зато можно за хорошие бабки сплавить конкурс. Ребята из фирмы «Б» заплатят – вот жулики и в шоколаде». Между тем два месяца назад компания на самом деле проиграла конкурс на обслуживание крупного нефтяного холдинга. Той самой фирме «Б» отошел подряд на несколько десятков миллионов рублей. Сопоставив факты, PR-менеджер передал имеющуюся

ИГОРЬ СОБЕЦКИЙ,
заведующий кафедрой экономической безопасности Учебного центра «Информзащита»

у него информацию в службу безопасности компании.

Ранее служба безопасности компании уже провела расследование по факту проигранного конкурса. Было установлено, что предложения выигравшей конкурс фирмы «Б» отличались от заявок компании всего на несколько процентов. Иными словами, при подготовке своей заявки на конкурс фирма «Б» имела исчерпывающую информацию об условиях, предложенных компанией. Однако расследование зашло в тупик, установить конкретных лиц, причастных к утечке информации, не представилось возможным. Теперь же перед начальником службы безопасности компании встала задача выяснить личность «Обобранного» и уточнить, какой информацией тот располагает.

К сожалению, администрация сайта не пошла на контакт со службой безопасности компании и отказалась предоставить имеющуюся информацию по логину «Обобранного», в частности IP-адрес, с которого было размещено сообщение. Таким образом, служба безопасности располагала только псевдонимом и временем размещения отзыва – 13 часов 38 мин., 14 апреля. Поскольку фигурант мог работать и в IT-подразделении компании, начальник службы безопасности под легендированным предлогом – якобы в целях аудита текущего состояния информационной безопасности – привлек к расследованию стороннего консультанта, заведомо не подпадающего под подозрение. Для выяснения личности «Обобранного» были приняты следующие меры.

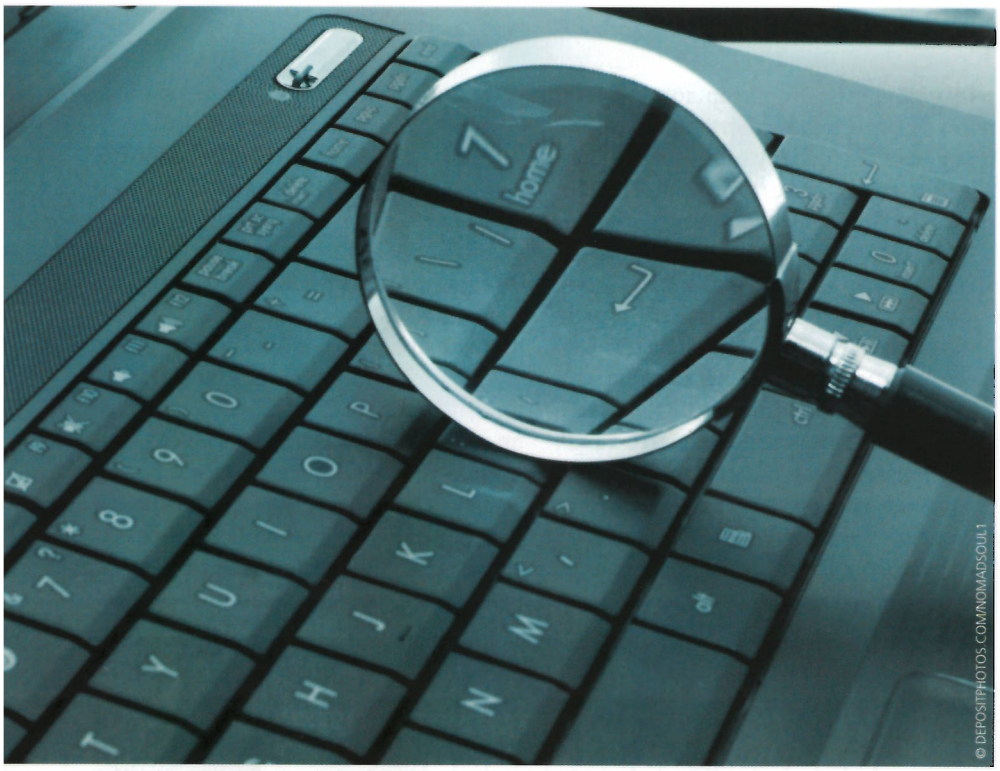
Первое. Просмотр и анализ лог-файлов корпоративного межсетевого экрана на предмет выявления обращений к сайту с отзывами. Данная мера оказалась безрезультатной, с рабочих мест никто из персонала компании в момент размещения отзыва к сайту не обращался. Однако отрицательный результат важен не только в науке, но и на практике. Поскольку отзыв был размещен в рабочий день в дневное время, его автор должен был либо использовать доступ к анонимному прокси-серверу или частный канал для выхода в сеть Интернет, либо отсутствовать в это время на работе.

Повторная проверка лог-файлов межсетевого экрана установила, что в период размещения отзыва никто из работников компании к известным анонимным серверам не обращался. А вот анализ лог-файлов СКУД компании позволил установить, что в момент размещения отзыва за пределами офиса компании находились 349 человек – все-таки это было время обеденного перерыва, – из которых в течение всего дня по различным причинам не появлялись на рабочем месте 29 человек.

Второе. Было сделано обоснованное предположение, что кратковременная отлучка работника из офиса компании специально для размещения компрометирующего отзыва маловероятна. Это дало возможность сосредоточиться на тех 29 работниках, которые отсутствовали полный рабочий день. С помощью специалиста по кадровой работе из их трудовых книжек была получена информация о местах предыдущей работы. Затем были изучены отзывы на сайте о 28 предприятиях. Оказалось, что «Обобранный» разместил отзыв о фирме «В» – там руководитель якобы «кидает народ на бабло» и «разводит стукачей, как Сталин». По полученным от специалиста по кадровой работе сведениям, в фирме «В» ранее работал системный администратор Алексей Д. Таким образом, было установлено что Алесей Д. и есть «Обобранный» и именно он может располагать информацией о злоупотреблениях при подготовке предложений на конкурс.

Третье. К сожалению, полученная информация не давала возможности прямо потребовать у Алексея Д. поделиться имеющимися у него сведениями со службой безопасности компании. С высокой вероятностью Алексей Д. мог отказаться от сотрудничества в силу надуманной «обиды» на компанию. Поскольку он не совершил никакого преступления – размещение подобной информации о своем работодателе порицаемо лишь с чисто этической точки зрения – никаких рычагов давления у службы безопасности не было. Принудительные же методы получения информации, увы, запрещены законодательством нашей страны. Поэтому была подготовлена «случайная» встреча Алексея Д. с «журналистом», якобы представляющим известную скандальную газету «Г». «Журналист» сообщил, что планирует написать большую разоблачительную статью о корпоративном мошенничестве, и прямо предложил Д. продать имеющийся у него компромат.

Поскольку фигурант мог работать и в IT-подразделении компании, начальник службы безопасности под легендированным предлогом – якобы в целях аудита текущего состояния информационной безопасности – привлек к расследованию стороннего консультанта



Статья 183

Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну...

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, – наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

Оказалось, что Д. прямо на работе периодически подрабатывает частными заказами по ремонту и настройке компьютеров для других работников компании

Предложение нашло благодарный отклик у Д., и за сравнительно небольшое вознаграждение тот поделился своими секретами. Оказалось, что Д. прямо на работе периодически подрабатывает частными заказами по ремонту и настройке компьютеров для других работников компании. Зная об этом, к нему обратился заместитель начальника отдела маркетинга компании Дмитрий Х. И попросил починить его ноутбук. На ноутбуке Д. нашел логин и пароль Дмитрия Х. к его электронной почте и из любопытства ознакомился с его частной перепиской. В переписке была полная история передачи Дмитрием Х. конфиденциальной информации своей подруге, работающей в отделе маркетинга фирмы «Б». Эту переписку Алексей Д. сохранил у себя «на всякий случай» и позже продал «журналисту». В дополнение Д. сообщил о незначительных злоупотреблениях еще двоих менеджеров среднего звена компании.

Несмотря на то что в действиях Дмитрия Х. отчетливо прослеживался состав уголовного преступления, предусмотренного статьей 183 УК РФ, по репутационным соображениям руководство компании решило не давать делу официального хода. В компании грянула организационно-штатная реформа, в результате которой и Дмитрий Х., и двое его коллег-ловкачей остались за бортом компании. Официальных обвинений им никто не предъявлял.

Предприимчивый Алексей Д. продолжает трудиться системным администратором. Оргштатные изменения счастливо прошли мимо IT-отдела, а его знакомый «журналист» уже пообещал выкупить по сходной цене любой компромат, который тот сумеет найти.

А какова мораль этой статьи? Увы, морали тут давно уже не осталось. Автор лишь продемонстрировал на рядовом примере, как можно достичь положительного результата расследования инцидентов информационной безопасности даже при самых скудных исходных данных. ●

[1] В этом месте указывалось название вполне реальной организации – основного конкурента компании.
[2] Система контроля и управления доступом, позволяет контролировать передвижения сотрудников по офису компании.
[3] Двое работников пришли в компанию с одного и того же места работы.
[4] За откровенность Алексей Д. получил 150 долларов и автомобильный компрессор.
[5] В этом случае гонорар был куда больше – Дмитрию Х. досталось целых 400 долларов, вкупе с благосклонностью подруги.
[6] Один из них устроил в компанию на работу свою приятельницу, а другая выписала подчиненным фиктивную премию и присвоила ее.