Forbes RUSSIA .RU

Внимание, за вами следят!

Как сделать, чтобы политика информационной безопасности работала на вашу компанию, а не против

Надежда Померанцева | 10 февраля 2010 10:44

Система проверки исходящей информации — Что грозит «инсайдеру» — Почему сотрудники соглашаются на перлюстрацию — Сколько стоит информационная безопасность — Защищая информацию, сохраняйте здравый смысл

Директор по развитию «ЭКОПСИ Консалтинг» Григорий Крамской впервые столкнулся с кражей информации, когда работал в небольшой сервисной фирме. Один из линейных менеджеров решил подзаработать на продаже базы данных конкуренту. Злоумышленник под выдуманным предлогом попросил знакомого из IT-отдела открыть ему доступ к базе и возможность скачать ее на внешний носитель. Несколько недель инсайдер вел переписку через корпоративный мейл с потенциальным покупателем — компанией-конкурентом — и в конечном счете договорился о сделке. Информация ушла за несколько десятков тысяч долларов — «гонорар» покупатель должен был перевести на зарплатную карту сотрудника.

«Парадоксально, но в письмах с рабочего ящика они обсуждали не только сумму, но и способ оплаты, — рассказывает Крамской. — Редкая безалаберность с обеих сторон: служба безопасности не отследила кражу, а сотрудник даже не удалил переписку!» Вскрылось все случайно. Коллега «айтишника», который был в сговоре с вором, случайно проговорился, что у одного из менеджеров появилась возможность скачать базу. Это заинтересовало руководство, которое подобных полномочий сотруднику не давало. Решили на всякий случай проверить переписку, причем делали это на глазах у вора. Афера обнаружилась, и последовал жесткий разговор, по результатам которого деньги за базу компания забрала себе, а сотрудник уволился. «Компания-покупатель факт получения базы отрицала, хотя были документальные свидетельства», — замечает Крамской.

По его словам, мораль этой истории применима к практике многих российских компаний: только потеряв часть важной информации (в данном случае клиентской базы), менеджмент начинает относиться внимательнее к деятельности сотрудников и, главное, читать их письма. Первый и самый трудный вопрос встает перед владельцем бизнеса: как защитить информацию, не устраивая концлагерь и не нарушая закон?

Система проверки исходящей информации

Специалисты по защите данных разделяют процесс обеспечения интернет-безопасности в офисе на две составляющие: контроль исходящей информации и слежка за сотрудниками в целях поддержания дисциплины. Если первая функция чаще всего находится в ведении службы безопасности, то второй занимаются HR-отделы.

«Ни у кого нет сомнения, что информация стоит денег и ее необходимо защищать, — утверждает исполнительный директор IT-компании Trafica Владимир Андриенков. — Вопрос, как ты ее защищаешь». Компания Андриенкова занимается установкой «интеллектуальной системы» Monitorium, которая включает в

себя специальный сервер и софт для контроля за исходящим интернет-трафиком. Под «трафиком» подразумевается не только отправка писем через рабочую почту, но и анализ исходящих данных через интернет-коммуникаторы ICQ и Skype.

Правда, в функционал подобных систем не входит анализ действий сотрудника — например, скачивает он данные на флеш-карту или нет. «Во всех приличных западных компаниях хорошим тоном считается отсутствие в компьютере выходов для скачивания информации — USB-портов и других копирующих устройств. Даже чтобы распечатать документ, на это нужно иметь полномочия», — комментирует Андриенков.

Сегодня на российском рынке работают три крупные компании-разработчика систем защиты информации. Старейшие игроки — InfoWatch (входит в ГК «Лаборатория Касперского») и «Инфосистемы Джет». Оборот рынка по защите информации за 2009 год он оценивал не менее чем в $1,3 млн. А стоимость средней системы мониторинга колеблется от $3500 до $100 000 в зависимости от объема исходящего трафика.

Интеллектуальные системы, похожие на те, что устанавливает Trafica, работают по двум функциям — блокировке и мониторингу. Например, если компании важно, чтобы за пределы офиса не просачивалась информация о клиентах, которая содержится в определенных файлах, можно поставить эти документы или информацию о клиентах на блокировку. После чего эти файлы невозможно отправить с офисного компьютера: система заблокирует сообщение автоматически.

Если же компания хочет не блокировать, а отслеживать, кто и как часто отправляет те или иные документы, систему можно запрограммировать на мониторинг. Сообщение, содержащее ключевые слова, будет отправлено, но данные (отправитель, дата и текст письма) появятся на экране сотрудника службы безопасности или HR-отдела. Российские компании предпочитают использовать отечественные системы, потому что импортные работают с английским языком. «Настраивать на мониторинг англоязычную систему для работы в российской компании дорого, к тому же непредсказуем результат», — считает Владимир Андриенков.

Пока основные клиенты защитников информации — сырьевые компании, банки и транснациональные корпорации — крупный бизнес. В Trafica подчеркивают, что не настраивают систему на чтение корреспонденции, скорее она нужна для отслеживания перемещения конкретных документов.

Что грозит «инсайдеру»

Если с помощью мониторинга удается поймать вора, возникает другой вопрос: что с ним делать? Дело в том, что уволить инсайдера не так просто. Даже при убедительных доказательствах его вины. Работодателю надо начать беспокоиться об этом заранее, до совершения нарушений: установить режим коммерческой тайны (он прописан в законе «О коммерческой тайне»), а потом утвердить специальные положения, где содержится список сведений и документов, которые подпадают под понятие тайны и не подлежат передаче третьим лицам. Затем следует ознакомить персонал с этим положением под роспись, говорит юрист Московской коллегии адвокатов «Легис-групп» Максим Домбровицкий.

Важно, чтобы на все носители, которые могут содержать конфиденциальную информацию, и на сами документы был нанесен гриф «конфиденциально, коммерческая тайна ООО такого-то». «Если произошло нарушение коммерческой тайны, компания вправе начать собственную внутреннюю проверку и обратиться за помощью в милицию, — предупреждает Домбровицкий. — Тогда инсайдеру может грозить и уголовная ответственность, предусмотренная статьей 183 УК РФ».

Почему сотрудники соглашаются на перлюстрацию

HR-менеджер Елена из федеральной телекомпании ненавидит свою работу. В ее должностные обязанности входит слежка за сотрудниками. С начала кризиса компания сокращает расходы на персонал, чистка рядов не прекращается. «Чтобы уволить сотрудника, нужны веские основания: когда все очевидные нарушители сокращены и выбирать не из кого, мы придумываем повод и начинаем тотальный контроль сотрудника, — рассказывает Лена. — Например, делаем «фотографию рабочего времени».

Технология такова: сотруднику вручается опросный лист самоконтроля с множеством граф, в котором сотрудник обязан расписать каждые 10 минут своего рабочего дня. Одновременно с этим в службу технического контроля приходит запрос на распечатку всех операций с компьютера «объекта». Человек, который заполнял лист, не подозревал о том, что за ним следят. Далее «самоконтроль» и распечатка от IT-службы сравнивались, и обязательно находилась какая-то погрешность, например в виде незафиксированного захода на «Одноклассники.ру». Сотрудника обвиняли во лжи и предлагали либо уволить «по плохой статье», либо написать заявление по собственному желанию.

По словам Елены, с моральной точки зрения заниматься такими вещами ужасно противно — HR-дирекцию прозвали «отделом по борьбе с персоналом». Но от судебного иска со стороны обиженных ее телекомпания застрахована — в случае разбирательства данные перлюстрации покажут, что виноват сам истец.

Ухищрения, которые была вынуждена применять Елена, чисто русские. В компаниях, устроенных по западному типу, вопросы информационной безопасности регламентируются либо трудовым контрактом, либо правилами внутреннего трудового распорядка (ПВТР). В этих документах досконально прописаны как список запрещенных действий (например, посещение социальных сетей), так и возможная перлюстрация.

Интересно, что большинство опрошенных Forbes менеджеров не видят в чтении их писем начальством ничего зазорного.

Например, в трудовом контракте директора по маркетингу Coinstar Money Transfer в странах Восточной Европы и СНГ Натальи Катиной есть необычные пункты. «По контракту я должна вести список контактов, фиксировать адреса электронной почты, которые являются собственностью компании точно так же, как и мой рабочий адрес и телефон, — объясняет Катина. — Я отдаю себе отчет в том, что не имею права удалять из почты сообщения не личного характера, и в случае, если я покину компанию, они останутся работодателю, ведь они относятся к деловой документации». По ее словам, в Coinstar перлюстрации нет, но даже если кто-то будет читать, работники не станут считать это вмешательством в личную жизнь или ущемлением прав.

Однако ни ICQ, ни Skype в ее офисе не заблокированы — наоборот, эти приложения используются как средство связи в решении рабочих вопросов. «У нас не стоит блоков вообще ни на что, — рассказывает Катина. — Даже если предположить, что у нас поставят блок на те же «Одноклассники», то не считаю это ущемлением прав. Лично я никогда не висела в социальных сетях».

Сколько стоит информационная безопасность

Наиболее жестко защищают информацию банки. В финансовых учреждениях безопасность регламентируется международным стандартом ISO 27001. Как рассказал Forbes руководитель службы информационной безопасности «Банк24.ру» Андрей Ерин, банк обязан проводить с этой целью более сотни процедур во всех сферах деятельности компании. «Различные типы «асек» у нас доступны только ограниченному кругу лиц — только тем, кому они нужны, — говорит Ерин. — Социальные сети только у

службы безопасности, устройства для копирования информации у большинства сотрудников закрыты, посещения сайтов логируются, а фамилии наиболее активных «серферов» выкладываются на всеобщее обозрение». Последнее не шутка. По понедельникам служба информационной безопасности рассылает сводку «Top-10 Интернет» — кто на каких сайтах сидел.

По словам Ерина, действия сотрудников в сети контролируются не только на уровне отдельных приложений, но и программой тотального контроля (путем снятия скриншотов). При необходимости эти записи используются при расследовании инцидентов комиссией из сотрудников отдела информационной безопасности, внутренней безопасности и службы внутреннего контроля. «Когда мы выстраивали свою систему управления информационной безопасности, то исходили из уровня реальных угроз в действующих процессах банка, поэтому все политики информационной безопасности живые и работающие», — утверждает Ерин.

По его словам, два сотрудника уже уволены по причине нарушения политики информационной безопасности. Причину увольнения Ерин не конкретизирует, говорит, что «эти уязвимые места в системе мы уже закрыли». Несмотря на то что уволившиеся ушли «по собственному желанию», остальные работники знают истинную причину, так как инциденты подробно обсуждались на внутрикорпоративном форуме.

Для защиты информации банки и другие компании используют специальное ПО, помогающее вовремя засечь саботажника на рабочем месте. Например, функционал системы Realite, разработанной казанской SMI Labs и московской Digital Zone, включает в себя мониторинг сетевого трафика, скриншоты с экранов компьютеров, мониторинг используемых приложений, фиксацию клавиатурного ввода и т. п. Диапазон продаж широк — компании, имеющие от 20 до 2000 рабочих мест. Внедрение слежки стоит от 400 рублей за рабочее место.

Защищая информацию, сохраняйте здравый смысл

Выстраивая информационную защиту, важно помнить, что она может быть эффективна только тогда, когда ее нельзя обойти. Бизнес-тренер Илья Богин вспоминает, как, работая в отделе персонала крупной пищевой компании, столкнулся с запретом на посещение социальных сетей («Мой Круг» и др.). Между тем соцсети служили ему инструментом поиска новых сотрудников. Переговоры с IT-отделом не помогли — компьютерщики не открыли доступ. «Тогда я потратил несколько часов, чтобы через другой прокси-сервер не только зайти на необходимые мне сайты, но и заодно открыть «Одноклассники» и другие ресурсы, доступ к которым был заблокирован, кстати, установил и ICQ», — смеется Богин.

После этого он сделал скриншот рабочего стола и отправил его «айтишникам» с вопросом, для чего нужны ограничения, если их все равно можно обойти. «Они посмеялись, конечно, и только развели руками — мол, таковы правила», — вспоминает Богин.

Темы: **информационная безопасность**, **информация**, **перлюстрация**