КАК В КОМПАНИЯХ СЛЕДЯТ ЗА СОТРУДНИКАМИ 16

ПО КОМУ УДАРИТ БОРЬБА ГОСУДАРСТВА С ПОСРЕДНИКАМИ 26

Экономический еженедельник издательского дома «Коммерсантъ» Выходит по понедельникам Индекс 73100

Коммерсантъ | dengi.kommersant.ru | №47 [754] 30.11 – 06.12.2009

ДЕНЬГИ

НЕСУЩИЕ ВМЕСТЕ

НА ЧЕМ ДЕРЖИТСЯ СИСТЕМА ХИЩЕНИЙ В РОССИИ

4 601865 000042 090

№47 (754) 30.11–06.12.2009
КОММЕРСАНТЪ ДЕНЬГИ

Слежка в рабочем порядке

МАРИЯ ГЛУШЕНКОВА

ЕСЛИ ВЫ, НАХОДЯСЬ В ОФИСЕ, НАПИСАЛИ ДРУГУ С ЛИЧНОГО ЭЛЕКТРОННОГО АДРЕСА ЧТО-ТО НЕПРИЯТНОЕ О СВОЕМ НАЧАЛЬНИКЕ, А ПОТОМ ВАС НЕОЖИДАННО УВОЛИЛИ, НЕ УДИВЛЯЙТЕСЬ. СОВРЕМЕННЫЕ СИСТЕМЫ СЛЕЖЕНИЯ, УСТАНОВЛЕННЫЕ ВО МНОГИХ КОРПОРАЦИЯХ, ПОЗВОЛЯЮТ УЗНАТЬ О ВАШИХ ДЕЙСТВИЯХ НА РАБОЧЕМ МЕСТЕ БУКВАЛЬНО ВСЕ — ВПЛОТЬ ДО ТОГО, КАКУЮ КНОПКУ НА КЛАВИАТУРЕ ВЫ СЕЙЧАС НАЖИМАЕТЕ. ТАКАЯ СЛЕЖКА АБСОЛЮТНО НЕЗАКОННА, ОДНАКО БОЛЕЕ ПОЛОВИНЫ КРУПНЫХ РОССИЙСКИХ КОМПАНИЙ ПРИЗНАЮТСЯ В ЭЛЕКТРОННОМ КОНТРОЛЕ ДЕЙСТВИЙ СОТРУДНИКОВ.

ОКО ЗА ОКОМ В 2006 году в США компания Hewlett-Packard оказалась втянутой в неприятную историю. Председателя совета директоров HP Патрицию Данн обвиняли в том, что она использовала незаконные методы выявления утечки конфиденциальной информации и организовала слежку за другими руководителями компании и журналистами известных информационных агентств. К расследованию были подключены министерство юстиции Калифорнии, Комиссия по ценным бумагам США и ФБР.

Чтобы замять шпионский скандал и избежать массы гражданских исков, HP была вынуждена заплатить $14,5 млн отступных. Львиная доля этой суммы — $13,5 млн — была направлена на формирование специального фонда, из средств которого должны были финансироваться расследования в сфере нарушений прав граждан на неприкосновенность частной жизни.

И это неудивительно. Только официальная статистика по перлюстрации уже может стать причиной для нервного срыва. Дальше всех продвинулись американцы: в том же году, когда HP расплачивалась за нездоровый интерес своего топ-менеджера, в США были приняты поправки в федеральное законодательство, в соответствии с которыми все компании обязали хранить архивы электронных писем, журналы переписки систем мгновенных сообщений, веб-чатов и прочую документацию своих сотрудников. Еще раньше, в 2003 году, компании большинства штатов обязали оповещать контролирующие органы о случаях утечки инсайдерской информации.

Европа в вопросе контроля эпистолярной деятельности офисных работников тоже старается не отставать. На рассмотрении Европейской комиссии сейчас находится новый закон (предполагается, что он будет принят к 2011 го-

НА ЧЕРНОМ РОССИЙСКОМ РЫНКЕ ПО-ПРЕЖНЕМУ МОЖНО КУПИТЬ ПРАКТИЧЕСКИ ЛЮБУЮ БАЗУ ДАННЫХ — НИ ЗАКОНЫ, НИ НОВЕЙШИЕ IT-РАЗРАБОТКИ У НАС ПОКА НЕ ЗАЩИЩАЮТ НИ ЧАСТНУЮ ЖИЗНЬ, НИ БИЗНЕС

ду), обязывающий все коммерческие компании, агентства и организации сообщать потребителям о фактах утечки или утери конфиденциальных данных клиентов. Логично предположить, что для того, чтобы знать об утечке, ее нужно сначала как минимум зафиксировать. Простейший способ добиться этого — все та же перлюстрация. В Финляндии в этом году уже был принят закон, позволяющий работодателям отслеживать идентификационные данные электронной переписки своих сотрудников.

Интересно, что противники финского законопроекта, прозванного Lex Nokia за то, что в его разработке участвовали представители известного производителя мобильных телефонов, напирали в парламенте на неприкосновенность частной жизни финских граждан, но ничего поделать не смогли. Аргументация Nokia оказалась сильнее: поговаривали, что компания, постоянно страдавшая от утечек инсайда конкурентам, попросту пригрозила властям вывести свою штаб-квартиру из Финляндии, спровоцировав тем самым потерю 16 тыс. рабочих мест.

России пока далеко до таких ужасов: узаконивать внутрикорпоративный шпионаж пока никто не решается. Хотя неофициально мы неплохо успели продвинуться в этом вопросе. Согласно опросу рекрутингового портала superjob.ru, на фирмах, где трудится свыше 5 тыс. человек, в 52% случаев работодатели подтверждают существование IT-контроля за подчиненными. В секторе малого и среднего бизнеса на каждом третьем предприятии из тех, чей штат не превышает 50 человек, вся электронная корреспонденция сотрудников, включая почту, мессенджеры и Skype, сегодня отслеживается.

«Однажды на работе, когда я писала e-mail клиенту, мне позвонил начальник и стал отчитывать по поводу неправильно расставленных приоритетов в письме,— возмущается менеджер небольшой фирмы, торгующей стройматериалами, Елена Молчанова.— При этом видеть мой монитор начальник никак не мог и давал мне указания, сидя у себя в кабинете. То, что меня так цинично контролируют, стало для меня настоящим открытием. Если бы я знала об этом, никогда бы не стала пользоваться рабочим ящиком в личных целях, что до того случая было для меня абсолютно естественным».

Отметим, что поведение начальника Елены — довольно редкий случай. Мало кто из работодателей так откровенно демонстрирует сотрудникам, что за ними следят. Однако это вовсе не значит, что слежки не существует. Системы анализа трудового веб-трафика, выпускаемые крупнейшими мировыми поставщиками решений по безопасности, либо уже содержат возможность создания внутренней системы всеобъемлющего контроля, незаметного для объекта, либо требуют минимальной модернизации. Например, покупка простейшего keylogger — шпиона, которым и пользовался начальник Елены,— не ударит по карману даже малого предпринимателя: всего-то $400. Для более крупных предприятий и более сложных систем контроля расценки выше, но тоже отнюдь не заоблачные. «Системы защиты предприятий от утечек данных (DLP-системы — Data Leakage Prevention) для крупных компаний — от 500 пользователей — стоят от $100 тыс. в зависимости от количества рабочих станций (компьютеров) и прочих факторов»,— говорит PR-директор компании InfoWatch Игорь Царев. За что же предприятия платят эти деньги?

КОНТРОЛЬНАЯ РАБОТА Еще в 2005 году в США компании 3ami и BridgeHead Software разрекламировали свою разработку — систему MAS (Monitoring, Auditing & Security), которая позволяла следить за каждым нажатием клавиши на компьютерах сотрудников. MAS могла контролировать, записывать и сохранять все действия компьютера, не допуская при этом внешнего вмешательства в уже сохраненный файл. Система отслеживала все действия с файлами — устанавливала факт их отправки, копирования, записи на другие носители, распечатки или удаления. Полученные с помощью MAS данные официально могли быть использованы в качестве доказательств преступлений в судах США.

Сегодня такое решение совершенно стандартно. Локальная сеть компании программируется на индексацию и сохранение на сервере всех входящих и исходящих e-mail независимо от того, удалялись они или нет. В случае необходимости активируется заданная система поиска, которая, в частности, может быть ограничена перепиской двух конкретных сотрудников за определенный период времени или названием проекта, который держится фирмой в секрете от широкой общественности. Известна история, которую любят рассказывать потенциальным заказчикам IT-продавцы решений по безопасности, когда через час после установки в сети крупной компании программы MAILsweeper, позволяющей блокировать прием и отправку сообщений с «опасными» словами, поиск выдал письмо сотрудника, в котором тот передавал конкурентам секретную документацию, подготовленную фирмой к грядущему тендеру.

Бывает, систему настраивают на ограничение доступа сотрудников на различные форумы и блог-сообщества, где логично предполагается и непреднамеренный слив. К примеру, согласно результатам исследования фирмы Proofpoint, опубликованным британским интернет-таблоидом The Register, 18% американских корпораций в этом году понесли ущерб от сообщений своих сотрудников в блогах, 17% поймали работников на сливе информации через социальные сети. Впрочем, e-mail в этом смысле лидирует: по данным Proofpoint, в 2009 году утечка информации через электронную почту была зафиксирована в 43% компаний. Размер убытков, понесенных от кражи конфиденциальных данных корпорациями по всему миру, по разным оценкам, в прошлом году составил $550 — 600 млрд.

«Сумма потерь поражает воображение,— замечает генеральный директор компании „Информзащита“ Владимир Гайкович.— Но, если честно, я еще не слышал ни об одном банкротстве компании из-за какой-либо утечки. Это, на мой взгляд, говорит о том, что большинство цифр, называемых в прессе, отражают не реальный, а потенциальный ущерб при са-

ЖЖИВОЕ МНЕНИЕ

LiVEJOURNAL www.livejournal.com

Как вы относитесь к слежке компаний за сотрудниками?

Мнения блогеров публикуются в рамках совместного проекта журнала «Деньги» и Livejournal.com.

Turrel_hanna

Прошу прощения, но что значит «личная жизнь» на рабочем месте? Нет, я понимаю, есть срочные вопросы, которые иногда нужно решать в телефонном режиме: болезнь ребенка, смерть родственника, прочее. Но нельзя посвящать этому большую часть рабочего дня, а потом обижаться на работодателя, что тот призывает к дисциплине и читает e-mails. Кстати, в правилах пользования корпоративной связью есть пункт о том, что работодатель имеет доступ к электронной почте и internet logs.

slidingcms

Среднестатистические работодатели по обоюдному согласию с работниками играют в одну и ту же игру. Правила этой игры не меняются в России десятилетиями. Работодатель платит за человека на рабочем месте, а не за быстрый и качественный результат. Сотрудники искусственно затягивают текущие задачи, так как за досрочное их решение они получат отнюдь не премии, а новые нагрузки. Пока нет мотивации быстро делать работу, слежка (но только для уличения сотрудника в безделье) — вещь подлая и неоправданная.

Umab_c_pex

Право на неприкосновенность личной жизни на практике имеют начальник 1-го отдела плюс директорат. А остальные сотрудники обычно проходят по категории «Да знаешь, сколько таких сейчас на улице?! Только свистни — сотнями набегут!».

Elena_1918

В некоторых компаниях с целью слежки за сотрудниками заставляют писать подробнейшие, чуть ли не поминутные отчеты о работе. Но к этому быстро приспосабливаются и пишут отписки. Начальники таким образом часто просто избавляют себя от необходимости напрямую общаться с подчиненными. Боятся? Не умеют? Не хотят? Лень? На мой взгляд, это говорит об отсутствии нормального оперативного менеджмента в компании.

Cpt_comic

Слежка за сотрудниками в той или иной форме — абсолютно бесполезное занятие. Если компания этим занимается, то она тем самым расписывается в неспособности создать адекватную систему мотиваций для сотрудников. В грамотно выстроенной компании существует такая система, которая будет создавать правильные стимулы для того, чтобы человек сам понимал, как и на что ему тратить свое рабочее время.

От редакции. Мы, конечно, не собираемся шпионить за блогерами: у нас нет ни желания, ни соответствующих средств. Кроме того, у каждого свой график работы. Но отметим, что все комментарии оставлены с 12.00 до 15.30 по московскому времени, то есть в тот период, когда у большинства людей самый разгар рабочего дня.

О темах предстоящих публикаций «Денег» вы можете узнать по адресу: community.livejournal.com/opinion_ru, там же оставляйте свои комментарии. А приключившиеся с вами истории, которые могли бы стать поводом для наших журналистских расследований, излагайте по адресу: www.kommersant.ru/reply.aspx.

мом плохом стечении обстоятельств. То есть все эти цифры — сублимация страха перед утечками информации. Ни подтвердить, ни опровергнуть их невозможно. Реальные же потери компаний, на мой взгляд, на несколько порядков меньше».

Тем не менее такая статистика заставляет компании тратить немалые деньги на организацию программных систем «обороны». К примеру, в России, согласно оценкам компании «Информзащита», в 2008 году бизнес раскошелился примерно на $220 млн. «В последнее время увеличился спрос на все, что связано с системами управления безопасностью, что легко объяснимо. Качественное управление — это единственный способ повысить эффективность построенной системы безопасности»,— отмечает Владимир Гайкович.

Что это за решения? «Речь идет об интегрированных продуктах для комплексной защиты конфиденциальных данных компании от несанкционированной утечки или разглашения,— поясняет Игорь Царев.— Решение представляет собой программно-аппаратное устройство, которое выполняет мониторинг и фильтрацию данных, передаваемых за пределы компании по электронной почте, через веб- или интернет-пейджеры (ICQ и проч.). Есть решения, которые представляют собой систему криптографической защиты конфиденциальной информации в процессе ее хранения и обработки».

ЗАКОННОЕ БЕЗЗАКОНИЕ До сих пор в разных странах законодатели ломают голову, как примирить нормативную базу, отстаивающую территорию privacy, с законотворчеством, так или иначе эту территорию затрагивающим. Несмотря на драконовские законы, создававшиеся для борьбы с утечкой инсайда, Старый и Новый Свет не забывал укреплять пробелы нормативных баз по части защиты персональных данных: например, в США не так давно был принят закон «О защите персональных медицинских данных». Это действительно только пробелы, поскольку глобально тайна личной жизни и все с ней связанное — письма, телефон, интернет — охранялось всегда и везде на уровне конституции. Такова же ситуация и в России.

«Вопрос личной переписки любого гражданина нашей страны регулируется Конституцией,— поясняет директор правового департамента компании „Нексиа Пачоли" Ирина Баршай.— В соответствии с 23-й статьей Конституции РФ каждый человек имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этих прав возможно только на основании судебного решения, а за их нарушение предусмотрена ответственность вплоть до уголовной».

«Пункт 2 статьи 23 Конституции РФ защищает тайну переписки. Только на основании судебного решения эта тайна может быть нарушена. Для электронной переписки основной закон исключений не делает, упоминая о тайне „иных" сообщений. А за нарушение тайны переписки предусмотрена уголовная ответственность по статье 138 УК РФ,— подтверждает Дмитрий Ширяев, ведущий консультант ООО „ФинЭкспертиза".— Что же касается прихоти или системы безопасности как причин негласного сбора информации, то они одинаково незаконны, так как решение о допуске к частной электронной переписке принимал вовсе не суд. Так что хакер-любитель и начальник службы безопасности крупной корпорации отвечать должны одинаково, последний — даже больше, поскольку точно будет действовать по предварительному сговору с подчиненным — техническим специалистом-исполнителем».

Получается, что контроль за любыми коммуникациями сотрудников — противозаконен, он может быть санкционирован только решением суда. Согласно внутреннему уставу компании, сотрудников могут обязать петь гимн по утрам. Или проходить собеседование с помощью детектора лжи, что, к примеру, практиковалось в «Евросети». Однако контролировать трудовую деятельность своих сотрудников, отслеживая их переписку, работодатель не вправе. Даже если речь идет о сотруднике, с утра до вечера сидящем в «Одноклассниках», уволить его за это будет нельзя. Хотя, конечно, это может стать поводом подобрать другие статьи Трудового кодекса. «Никто не запрещает работодателю контролировать работника в части исполнения последним его трудовых обязанностей,— говорит Ирина Баршай.— Но речь идет о простом контроле, когда работнику выдается письменное задание на день и вечером по пунктам проверяется его исполнение. Таким образом умный работодатель