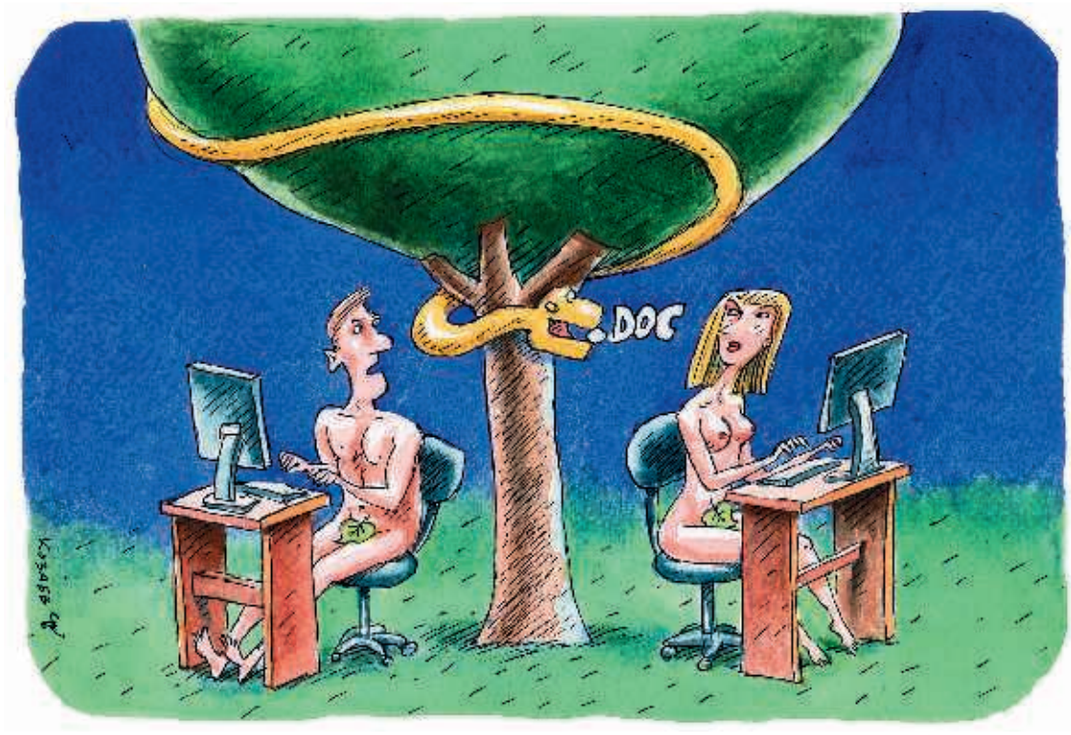
Находка для шпиона



Как в век тотальной информатизации уберечь важные данные от утечки на сторону?

Елена Покатаева

ПОД КОЛПАКОМ

Интернет — это технологическая подножка всему человечеству. Такая мысль непременно придет в голову, если внимательно читать ежедневные сообщения о вирусах, мошенниках и шпионах. Ведь они гораздо вольготнее чувствуют себя на просторах Сети, чем благонамеренные бизнес-пользователи, зарабатывающие свою трудовую корпоративную копеечку с использованием сетевых коммуникаций. Создается ощущение, что опасность утраты конфиденциальных данных выходит из-под контроля — слишком много новых возможных каналов утечек добавляется в ходе технологического совершенствования компьютерных и коммуникационных систем. Можно ли вообще обуздать эти процессы?

«На рынке предлагаются типовые решения защиты от утечек данных, но их эффективность не будет высока, — поясняет Ольга Горшкова, представитель компании InfoWatch. — В каждой компании есть своя специфическая информация, которую также нужно защищать». Кстати, определить, что нуждается в защите, не такая простая задачка, как может показаться на первый взгляд. Скажем, не вызывает сомнений необходимость защиты интеллектуальной собственности, если деятельность компании связана, например, с научными исследованиями. Если же речь идет о внутренней информации, с которой работает компания, возможны варианты. «Если вам понятно, какие ваши данные представляют ценность, нужно ответить на следующий вопрос: для кого это ценно?» — рассуждает Валерий Боронин, руководитель лаборатории защиты информации от внутренних угроз «Лаборатории Касперского». «Большая часть информации, являющейся для нас конфиденциальной, не может быть эффективно использована сторонними лазутчиками, — рассказывает Георгий Дзагуров, генеральный директор компании Penny Lane Realty. — Пусть даже вы узнали, что через нас продается некий дом, но без нашей поддержки эта информация вам ничего не даст». Так что правильно определить источник интереса к вашим данным — первейший шаг в деле их защиты.

Однако чувствительной для компании может оказаться вообще любая информация, способная негативно повлиять на ее имидж. «Если сотрудники обсуждают в Сети через ICQ, интернет-чаты и форумы решения руководства или подробности происходящей в компании реорганизации, считать это утечкой конфиденциальной информации или нет? — размышляет Ольга Горшкова. — Я считаю, что, безусловно, да, поскольку это может сказаться на бизнесе компании». Но сотрудники, которые таким образом выдают важную информацию, обычно делают это без специальной цели, разве что из чувства обиды на руководство, закручивающее гайки. Более того, эксперты говорят, что более 70 процентов всех инцидентов в сфере информационной безопасности связано с внутренними угрозами, то есть действиями сотрудников. Причем, по оценкам аналитиков компании Gartner, 80—90 процентов всей слитой из компании информации — это непреднамеренные утечки, проще говоря, результат халатности или безалаберности. Оценки российских специалистов несколько иные: согласно отчету InfoWatch, в I полугодии 2010 года соотношение случайных и умышленных утечек данных из компаний примерно равное. Но работать с разными типами утечек нужно по-разному.

Готовы ли вы ограничить коммуникации сотрудников, чтобы пресечь утечки данных?

Георгий Дзагуров, генеральный директор компании Penny Lane Realty

Наша конфиденциальная информация реально полезна только ближайшим конкурентам, а их мы знаем наперечет, это порядочные люди. Я видел фирмы, где ни в Интернет из офиса не выйдешь, ни копию файла не сделаешь — это паранойя и недоверие к собственной команде. Оплачиваемые услуги инсайдеров для меня опасны именно потерей сплоченности команды. При недоверии мы предпочитаем прощаться с человеком, чтобы не разрушалась атмосфера взаимного доверия.

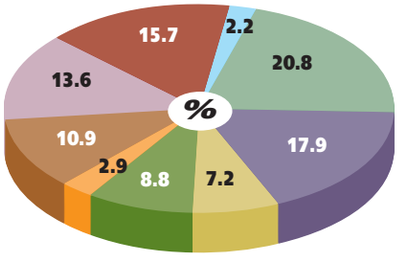
Андрей Гриценко, начальник службы информационной безопасности банка «Возрождение»

В большинстве случаев должностные обязанности сотрудников не предполагают использование сети Интернет, ICQ, съемных носителей информации и мобильных устройств. Ограничение доступа сотрудников к этим возможностям никак не сказывается на качестве исполнения служебных обязанностей, но в то же время позволяет существенно снизить операционные риски, в том числе значительно уменьшить риски утечки конфиденциальных данных из банка.

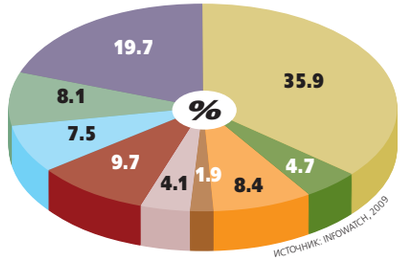
Валерий Боронин, руководитель лаборатории защиты информации от внутренних угроз «Лаборатории Касперского»

Принимаемые меры должны быть адекватны рискам, а безопасность обратно пропорциональна удобству. Правило 80:20 применимо и здесь — часто есть возможность значительно снизить большую часть рисков с помощью недорогих и не требовательных к ресурсам мер. Каждый следующий шаг, как правило, становится все более дорогим и ресурсоемким, поэтому баланс определяется в зависимости от задач и выделяемых средств.

Основные каналы умышленных утечек, %



Основные каналы случайных утечек, %



- Мобильный компьютер (ноутбук, КПК)
- Мобильный носитель (флэш-накопитель, CD, DVD и т. д.)
- Настольный компьютер, сервер, НЖМД
- Интернет
- Бумажный документ
- Архивный носитель
- Электронная почта
- Другой
- Не установлено

ИСТОЧНИК: INFOWATCH, 2009

Если поиск заказчиков и расследование случаев заказного инсайда — скорее задача правоохранительных органов, то неумышленные утечки — это сфера ответственности самой компании, так сказать, тест на пригодность к жизни в информационном обществе. Профессионалы выделяют несколько типов инсайдеров: «бестолковые» (выносящие информацию из офиса на диске ноутбука, чтобы поработать с ней дома, но вместо этого оставляющие ноутбук на столике в кафе), «жертвы социальной инженерии» (дублирующие конфиденциальную информацию на почтовый ящик мошенника), «обиженные» (стремящиеся скомпрометировать работодателя любым способом), «нелояльные» (мечтающие сменить место работы, прихватив с собой корпоративные ноу-хау), а также специально внедренные инсайдеры, передающие бизнес-информацию, например, недобросовестным участникам фондового рынка. Самое неприятное, что весь арсенал технических средств по защите корпоративных данных от несанкционированного доступа извне в данной ситуации оказывается бесполезен, ведь инсайдеры имеют к ней вполне легальный доступ изнутри. Для таких ситуаций используются технические решения класса DLP (Data Leak/Loss Prevention — предотвращение утечек данных).

В основе их работы лежит простая и старая как мир идея непрерывного наблюдения, проще говоря, слежки за тем, что происходит с данными в корпоративной информационной системе: какие данные передают пользователи по электронной почте, факсу, ICQ? Какие документы распечатывают на принтере? Какие сайты Интернета посещают? Это непростая программная система, которая умеет не только собирать данные, но и распознавать подозрительную активность пользователя (например, ту, которая предшествует «сливу» сведений), а также составлять аналитические отчеты по различным информационным срезам. Если в организации есть настоящий шпион, он себя проявит, и тогда архив запротоколированных действий станет основой расследования.

Глубина и детальность планируемых «оперативно-разыскных мероприятий» определяет сложность и стоимость DLP-проекта. «Шкалы для измерения действия человеческого фактора не придумано, — говорит Валерий Боронин. — Однако историю инцидентов и статистику по каждому пользователю можно и нужно учитывать. Поэтому каждая организация сама описывает допустимые и недопустимые модели поведения пользователей». Нужно определить, какая информация является конфиденциальной, как, где и кем она порождается, кому и к какой информации можно давать доступ, и — самое главное — детально прописать, каким образом каждый сотрудник может распоряжаться этим доступом. А еще нужно уметь привязывать личность нарушителя к его «электронной версии» (IP-адресу, учетной записи, адресу электронной почты), чтобы избежать ошибочных обвинений.

> *«80—90 процентов всей «слитой» из компании информации — это непреднамеренные утечки, проще говоря, результат халатности или безалаберности»*

Но вот каково добропорядочным сотрудникам сознавать, что все манипуляции их пальцев с клавиатурой и мышью отслеживаются и записываются? Похоже, придется смириться с тем, что именно такой оказывается плата за легкость и удобство электронных коммуникаций. А руководству и HR-отделам компаний придется потрудиться — не только разработать внутреннюю политику информационной безопасности, но и донести эту информацию до всех сотрудников. И не просто получить подпись под документом, а добиться того, чтобы сотрудники поняли, как именно следует обращаться с корпоративными данными: о чем не следует болтать по телефону и в социальных сетях, как составлять электронные письма. И даже что делать с ненужными распечатками документов! Исследование InfoWatch выявило занятный факт: 20 процентов неумышленных утечек в I полугодии пришлось на бумажные документы, без всякого злого умысла выброшенные в корзины для бумаг.

Стало быть, DLP-проект — это совместное детище корпоративного менеджмента, IT-подразделения, службы безопасности, отдела кадров. Думается, организовать слаженную работу этих четырех подразделений — это задачка почище настройки технического решения и написания томов регламентов. К тому же она, можно сказать, бесконечна, ведь технологии развиваются, появляются новые каналы связи и новые методы обработки инсайдеров. К счастью, эта бесконечная жизнь делится на четкие циклы: обновление политики безопасности — мониторинг — анализ инцидентов. Как говорят специалисты, если DLP-система построена качественно, после ее запуска в промышленную эксплуатацию количество инцидентов с нарушением безопасности снижается на 50 процентов. Но до нуля не дойдет никогда — человеческий фактор не позволит. ■

КОНФИДЕНЦИАЛЬНО

Красный коридор

Андрей Казачков,
заместитель директора департамента безопасности «Роснанотех»

Основная информация, с которой работает госкорпорация «Роснанотех», — портфель инвестиционных проектов, который нужно надежно защищать от посторонних глаз. Причем руководству было очевидно — основной источник угроз находится внутри компании: как правило, это работник, имеющий доступ к конфиденциальной информации, который пытается — случайно или намеренно — передать чувствительную для компании информацию вовне. Первый проект защиты мы реализовали самостоятельно — в виде контроля (и при необходимости блокирования) записи данных на флэш-накопители. Причем это была «умная» система — она умела различать, разрешена или нет конкретная операция конкретному работнику. Однако люди привыкли пользоваться и другими электронными каналами связи. Как взять под контроль все их многообразие? Из разнообразных DLP-решений мы выбрали, опираясь на исследования международных аналитиков, систему компании Symantec, а затем интегратора — компанию КРОК. От интегратора требовалась разработка всех регламентов защиты от утечек, включая классификацию конфиденциальной информации (где находится, кто владеет), описание процессов обращения с информацией и предотвращения утечек. Это самая сложная и кропотливая часть проекта, которая заняла около полугода. Но именно она обеспечивает перекрытие всех возможных каналов утечки, позволяя в дальнейшем наращивать функциональность: как только добавляется новый способ связи, настраиваются процессы, и запускается новый цикл мониторинга защиты.

DLP-проект требует финансовых вложений: от десятков до сотен тысяч долларов. Причем стоимость технического решения сравнима со стоимостью организационной части. Но эта овчинка стоит выделки. Ведь теоретически создать недорогую и предельно безопасную систему возможно — просто перекрыть сотрудникам все электронные каналы общения. Но для нас такое решение неприемлемо: бизнес-процессы утратят необходимую гибкость, поскольку сотрудники будут не столько работать над проектами, сколько получать разрешения на отправку электронной почты, факса, выход в Интернет. DLP-система должна быть не только безопасной, но и удобной для работы сотрудников, ведь ее главная задача — защищать компанию от неумышленных утечек. Значит, делать это надо с максимальным тактом и уважением к работникам. А для поимки настоящих шпионов есть другие системы.