ШПИОНСКИЕ СТРАСТИ В ЛОКАЛЬНЫХ СЕТЯХ: СТЕГАНОГРАФИЯ НЕ ПРОЙДЕТ!

Проблема информационной безопасности сродни проблеме брони и снаряда. На каждый цифровой замок найдется своя цифровая отмычка. Но максимально усложнить жизнь информационным взломщикам можно. Надо только понять, откуда ждать атаки

Текст **РОМАН ГОРБАНЬ,** менеджер группы «Форензик» КПМГ в России и СНГ

Министр-администратор

Зачастую руководители компании имеют общее представление о том, каким образом контролируются IT-ресурсы. Решения принимают квалифицированные IT-менеджеры, которые при этом руководствуются не только безопасностью, но и тем, насколько удобно сотрудникам их отдела использовать внутреннюю информационную инфраструктуру. Это приводит к тому, что все компьютеры организации оказываются крайне уязвимы со стороны практически всего IT-персонала, включая самых младших сотрудников. Многие из руководителей были бы шокированы, узнав, что у любого айтишника есть прямой доступ к локальным дискам их компьютера, на которых хранятся клиентские базы, договора, финансовая и другая конфиденциальная информация. Мало радости доставит вам также новость о том, что через систему удаленного доступа виден экран вашего компьютера и можно полностью контролировать все, что на нем происходит. Известны случаи, когда на всех компьютерах компании был установлен один и тот же довольно примитивный пароль локального администратора, который в течение нескольких минут подбирается с помощью специального программного

обеспечения. Таким образом, доступ к любому компьютеру организации может получить не только IT-специалист, но и любой другой сотрудник, финансово мотивированный со стороны третьих лиц.

В ходе одного из расследований мы столкнулись с массовым затиранием файлов – способом, применяющимся в случаях, когда пользователь очень не хочет, чтобы удаленную информацию смогли восстановить. Косвенные следы тогда указывали на то, что удаленная информация могла быть полезна для расследования. Мы подозревали, что виновными могут оказаться системные администраторы, и провели анализ предварительно сделанных копий жестких дисков их компьютеров и файл-серверов организации. После нескольких интервью с IT-специалистами и сотрудниками компании, в которой произошел инцидент, нам удалось реконструировать цепочку событий. Сопоставив временные метки удаленных файлов, а также проанализировав журналы событий, время установки программ и другие факты с уже известными данными, нам удалось выйти на виновных в инциденте. Примечательно, что в той компании каждый из сотрудников IT-отдела имел полный набор полномочий. Мы также выявили программу для удаленного мониторинга действий пользователя, установленную на всех компьютерах сотрудников. Данная программа не была согласована со штаб-квартирой, а использовалась в личных целях. Согласно исследованию, проведенному КПМГ с января 2005 по сентябрь 2008 года, 280 млн человек во всем мире подверглись краже информации. В 25% случаев это произошло в результате утери или хищения компьютеров; 80% инцидентов повлекли за собой утечку персональных данных; 51% краж был совершен инсайдерами; 46% украденной информации не было защищено какими-либо средствами.

Сорвать банк

Мало кто задумывается о рисках, сопряженных с интернет-банкингом. Все больше людей пользуется этой услугой, признавая ее удобство, оперативность и, что немаловажно, безопасность. Действительно, интернет-сессии между клиентом и сайтом банка всегда надежно защищены ключом, сгенерированным только на один сеанс; взломать такой шифр практически невозможно. Но и тут хакеры используют особую методику. На компьютер пользователя по беспроводной сети интернет-кафе (обычно в крупных аэропортах) совершается атака, в результате которой настройки соединения подменяются таким образом, что компьютер жертвы начинает использовать в качестве сервера компьютер злоумышленника, причем для пользователя это может выглядеть, как обрыв связи: ничего подозрительного. Пользователь повторно пытается зайти на сайт своего банка, что ему удается. С компьютера хакера он загружает поддельный сертификат для защищенного соединения, после чего получает предупреждение, говорящее о том, что подлинность данного сертификата не может быть подтверждена. Подавляющее большинство людей тем не менее жмут на кнопку «Продолжить». Введенные затем логин и пароль сохраняются на компьютере злоумышленника. Чем он и воспользуется, пока жертва

Фото: РИА-Новости, архивы пресс-служб

будет совершать авиаперелет – отрезанная на несколько часов от всех средств коммуникации.
Думаете, тут нужна квалификация компьютерного гения? Ничего подобного. Подробные инструкции по такого рода взломам с демонстрационными картинками и видеороликами лежат на общедоступных сайтах в Интернете.

Симпатические чернила

Наибольшую обеспокоенность по поводу сохранности конфиденциальной информации испытывают банки. Они не используют беспроводные сети, внедряют строгий контроль за всем потоком информации. Как правило, у корпоративных пользователей сильно ограничен доступ к Интернету и введен контроль за электронными письмами, уходящими на внешние адреса. Телефонные переговоры записываются, регламентировано подключение внешних USB-устройств. Казалось бы, украсть информацию изнутри практически невозможно.
Однако и здесь есть возможность обмануть службу безопасности. Злоумышленник, например, может воспользоваться стеганографией, разместив файл любого формата (включая doc, xls, ppt, zip и другие) внутри изображения или аудиозаписи таким образом, что это оказывается незаметно для человеческого восприятия. Так, невинная фотография, озаглавленная «Как я провел отпуск.jpg», может содержать в себе до сотен килобайтов конфиденциальной информации. Ни одна программа не способна на 100% определить наличие или отсутствие стеганографии в том или ином файле. А их в течение дня пользователи отправляют тысячами.

Жизнь без проводов и секретов

Беспроводные технологии, безусловно, облегчают нашу жизнь. Ушли в прошлое кабель локальной сети, провода от принтера, колонок и фотокамеры – теперь они все подключены к маленькому и удобному wi-fi роутеру. Однако весь трафик в зоне публичного Интернета легко считывается. Захваченные пакеты затем реконструируются, после чего можно видеть полученные и отправленные письма, вебстраницы, открытые пользователем.
Архаичные проводные сети, именуемые на компьютерном сленге «веревками», избавляют от такого рода проблем. Но и «веревки» можно взломать. В фальш-потолке или полу между протянутыми проводами устанавливают скрытый роутер. Из внедренного роутера вытягивается другой, уже нигде не задокументированный кабель. Свободный конец этого кабеля можно соединить с модемом и вывести в коммутируемую телефонную сеть либо «поднять» скрытую wi-fi сеть прямо на роутере – теперь в корпоративную сеть можно входить откуда угодно. Такой вид доступа организуют для себя системные администраторы. С одной стороны, это удобно для выхода «на работу» из дома. С другой – если системный администратор попадет под сокращение, он сможет на постоянной основе удаленно забирать конфиденциальные файлы и продавать их третьим лицам.
На одном из проектов специалистами КПМГ был обнаружен как раз такой сценарий доступа в сеть. Скрытый кабель вел напрямую в конкурирующую организацию, сидящую этажом выше.

СЕО-УРОК №13

Не позволяйте системным администраторам превращать IT-отдел в неподконтрольную территорию. IT-безопасность требует комплексных решений.

Рейдеры во сне и наяву

При возникновении угрозы насильственного захвата компании нанимают профессионалов по борьбе с рейдерством, обращаются к юристам и местным властям.
Однако все эти усилия по сохранению бизнеса могут быть нейтрализованы действиями инсайдеров, сливающих информацию о готовящихся мерах рейдерам, позволяя им быть всегда на шаг впереди. Согласно различным исследованиям, в том числе проведенным компанией «КПМГ», около 50% случаев воровства информации, уходящей за пределы организации, совершается именно инсайдерами. Вычислить и уличить предателя среди лояльных сотрудников порой крайне сложно. Не устанавливать же за каждым сотрудником слежку!

ДИРЕКТОР ПО ПРОДАЖАМ КОМПАНИИ «ФОРС ЦЕНТР РАЗРАБОТКИ» АЛЕКСЕЙ ЛАПИРОВ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СВЕТЕ НОВОГО ФЕДЕРАЛЬНОГО ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

С 1 января 2010 года будет разрешено использовать только сертифицированные средства защиты информации. На наших глазах формируется новый сегмент рынка – рынок решений по защите персональных данных. Закон коснулся абсолютно всех. Если раньше вопрос обеспечения защиты данных был частным делом компании, то теперь это объект законодательно-правового регулирования.
Различные «самоделки» уйдут в прошлое: предприятия будут обязаны использовать только сертифицированное ПО.
Ведущие мировые производители ПО никогда не пренебрегали вопросами безопасности. К примеру, линейка продуктов *Oracle*, обеспечивающая защиту данных, как раз сертифицирована в соответствии с требованиями закона «О персональных данных». Более того, предвосхищая растущий спрос, компания «ФОРС» совместно с Oracle создала специальное предложение на поставку по доступной цене ПО Oracle, обеспечивающего защиту данных в соответствии со всеми требованиями.
Крайне важно, чтобы поставщики услуг помогали заказчикам и потенциальным клиентам получить как можно более полную информацию как о тех новых требованиях, которым должны отвечать их IT-системы, так и о том, как это все можно реализовать на практике.
Очевидно, что надежно защитить данные при минимальном уровне издержек могут лишь специализированные решения с широкими интеграционными возможностями, охватывающие весь объем задач. Потребуется объединить усилия первого лица компании, IT-директора и руководителя службы безопасности. Внедрение IT-решений должно сочетаться с организационными мероприятиями.
Затраты на защиту данных в разных организациях и отраслях могут существенно различаться. К примеру, в банковской сфере расходы на IT всегда были существенными и уровень информатизации там значительно выше, чем в реальном секторе экономики. Соответственно, скорее всего, речь в данном случае пойдет лишь о доработке существующей системы за счет приобретения специализированных приложений. В тех же компаниях, где финансирование проектов по информационной безопасности осуществлялось по остаточному принципу, придется начинать практически с нуля. Без комплексного предпроектного обследования и составления целостной картины IT-инфраструктуры не обойтись. На этом этапе проводится первичное изучение всех ее элементов, разрабатывается подробное, детально обоснованное коммерческое предложение («ФОРС» использует процессный подход, предполагающий следование логике существующих бизнес-процессов при реализации решения по защите персональных данных).
На этапе аудита информационной безопасности проводится комплексное обследование аппаратных и программных средств, определяются круг задач, «узкие места», составляется подробное их описание.
Следующий шаг – подготовка технического задания, в котором описывается архитектура предлагаемого решения. Только после этого можно приступать к комплексной его реализации.

Можно предложить другой подход. Например, специалисты КПМГ собирают из открытых источников информацию о сотрудниках и анализируют их внешние связи. Становится понятно, кто и каким образом связан с враждебной организацией. На компьютерах неблагонадежных сотрудников могут содержаться следы, подтверждающие их причастность к сотрудничеству с рейдерами: неосторожно отправленное или полученное электронное письмо, опрометчиво распечатанный документ или удаленные файлы.
Если захват еще только-только начался, значит, есть время для выстраивания прочной обороны. Нужно проверить всю IT-инфраструктуру на предмет уязвимости, разграничения прав доступа и места физического размещения данных. Для этого организации нередко арендуют серверы или вывозят собственные в другие страны с подходящим законодательством. Хранящиеся на них данные будет крайне сложно заполучить или похитить. Более простой способ – шифрование данных. Например, использование двойного доступа, когда при вводе разных паролей к одному и тому же зашифрованному носителю пользователю будут доступны разные файлы, причем доказать факт существования второго пароля невозможно.

Совершенно секретно

Изложенные выше методы не обязательно применимы только в случае с рейдерством; некоторые из подходов можно использовать и при расследовании кражи интеллектуальной собственности, злоупотребления рабочими полномочиями и прочих нарушений.
Необходимо уделять внимание всем аспектам IT-безопасности. Можно создать независимую рабочую группу из действующих сотрудников, что позволит им посмотреть по-новому на вещи и выдать свежие идеи. Или нанять консультантов, имеющих опыт работы в данной сфере.
Порой руководителю кажется, что все возможные меры уже испробованы и решения задачи безопасности не существует. Или наоборот: у руководителя присутствует ложная уверенность в том, что все надежно защищено. Оба сценария могут быть опасными. Опыт показывает, что в сфере IT-безопасности нет двух одинаковых проектов: у каждой организации свои потребности.
Какими бы ни были найденные решения, важно, чтобы они не только удовлетворяли требованиям безопасности, но и отвечали нормам законодательства, были одобрены с точки зрения процедур риск-менеджмента, а также учитывали возможность технической поддержки.