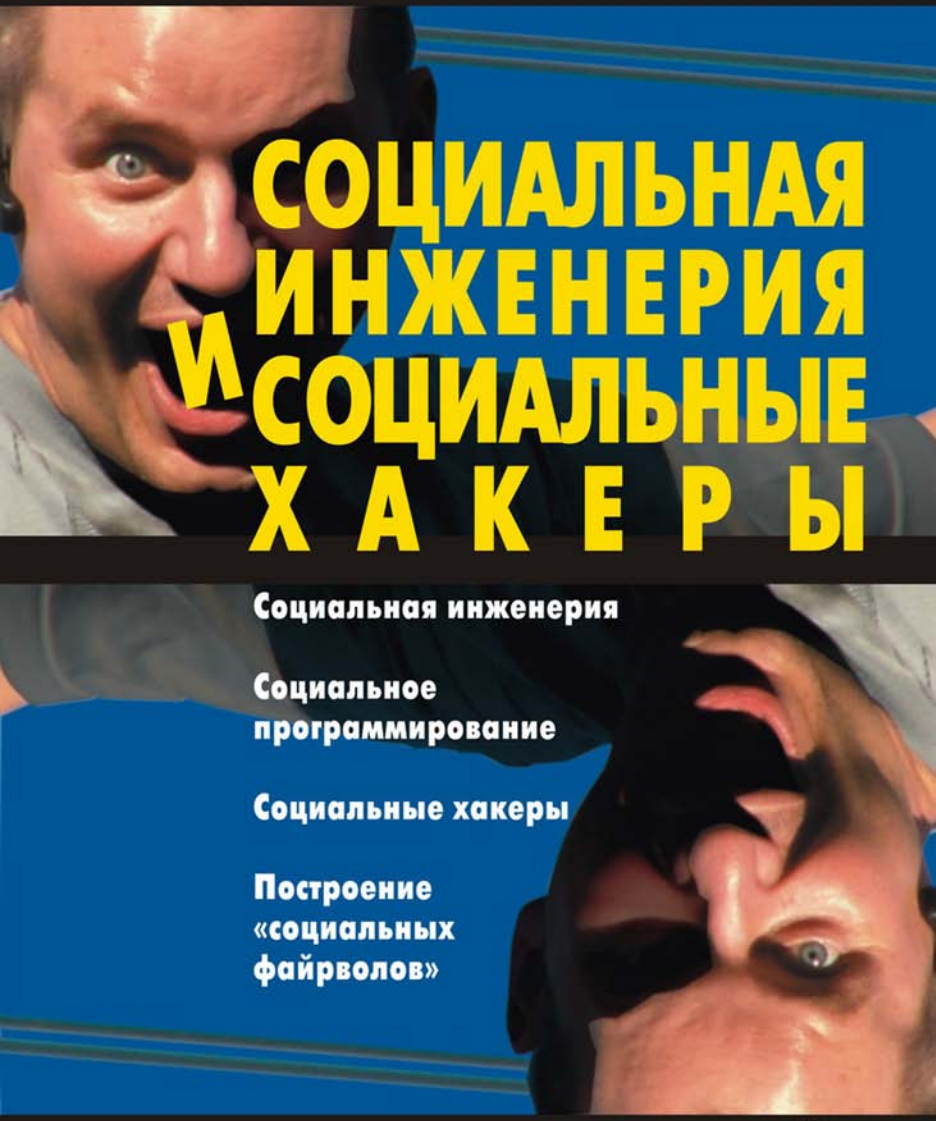
МАКСИМ КУЗНЕЦОВ
ИГОРЬ СИМДЯНОВ



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И СОЦИАЛЬНЫЕ ХАКЕРЫ

Социальная инженерия

Социальное программирование

Социальные хакеры

Построение «социальных файрволов»

bhv

Максим Кузнецов
Игорь Симдянов

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И СОЦИАЛЬНЫЕ ХАКЕРЫ

Санкт-Петербург
«БХВ-Петербург»
2007

УДК 681.3.06
ББК 32.973.26-018.2
К89

Кузнецов, М. В.

К89 Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007. — 368 с.: ил.

ISBN 5-94157-929-2

Прием, когда хакер атакует не компьютер, а человека, работающего с компьютером, называется социальной инженерией. Социальные хакеры — это люди, которые знают, как можно "взломать человека", запрограммировав его на совершение нужных действий.

В книге описан арсенал основных средств современного социального хакера (трансактный анализ, нейролингвистическое программирование), рассмотрены и подробно разобраны многочисленные примеры социального программирования (науки, изучающей программирование поведения человека) и способы защиты от социального хакерства. Книга будет полезна IT-специалистам, сотрудникам служб безопасности предприятий, психологам, изучающим социальную инженерию и социальное программирование, а также пользователям ПК, поскольку именно они часто выбираются социальными хакерами в качестве наиболее удобных мишеней.

Для широкого круга читателей

УДК 681.3.06
ББК 32.973.26-018.2

ISBN 5-94157-929-2

Оглавление

Введение

Для кого и о чем эта книга

Предметом книги является рассмотрение основных методов социальной инженерии — по мнению многих исследователей одного из основных инструментов хакеров XXI века. По своей сути, это книга о роли человеческого фактора в защите информации. О человеческом факторе в программировании выходило несколько хороших книг, одна из них, книга Ларри Константина, так и называется "Человеческий фактор в программировании". Это, пожалуй, единственная книга на данную тему, переведенная на русский язык. Вот что пишет автор в предисловии к этой книге: "Хорошее программное обеспечение создается людьми. Так же как и плохое. Именно поэтому основная тема этой книги — не аппаратное и не программное обеспечение, а человеческий фактор в программировании (peopleware)". Несмотря на то, что книга Л. Константина скорее по психологии, чем по программированию, первое издание книги было признано классическим трудом в области информационных технологий.

Информация тоже защищается людьми, и основные носители информации — тоже люди, со своим обычным набором комплексов, слабостей и предрассудков, на которых можно играть и на которых играют. Тому, как это делают и как от этого защититься, и посвящена данная книга. Исторически так сложилось, что хакерство с использованием человеческого фактора называют *"со-*

циальной инженерией", поэтому наша книга так и называется "Социальная инженерия и социальные хакеры".

Защититься от социальных хакеров можно только зная их методы работы. Наша цель, как авторов книги, — ознакомить читателей с этими методами, чтобы лишить социальных хакеров их главного козыря: неискушенности их жертв в вопросах мошенничества и методах скрытого управления человеком. Мы также надеемся, что изучение материала книги будет полезным для читателей не только в профессиональном, но и в жизненном плане. Ведь изучение тех разделов психологии, о которых мы будем говорить в этой книге, позволит вам взглянуть на окружающую действительность глазами психолога. Поверьте, это большое удовольствие и большая экономия нервов, сил и времени.

Авторы предлагаемой книги пришли к социальному программированию и основным его концепциям, с одной стороны (и большей частью), через программирование, связанное с защитой информации, а с другой — через одно из направлений нашей профессиональной деятельности, связанное с проектированием и установкой средств защиты информации от несанкционированного доступа, систем охранной сигнализации, систем контроля доступа и т. д. Анализируя причины и методы взлома ПО или каналы утечки информации из различных структур, мы пришли к очень интересному выводу о том, что примерно в восьмидесяти (!) процентах причина этого — человеческий фактор сам по себе или умелое манипулирование оным. Хотя это наше открытие, безусловно, не ново. Потрясающий эксперимент провели английские исследователи. Не мудрствуя лукаво, они разослали сотрудникам одной крупной корпорации письма якобы от системного администратора их компании с просьбой предоставить свои пароли, поскольку намечается плановая проверка оборудования. На это письмо ответило 75% сотрудников компании, вложив в письмо свой пароль. Как говорится, комментарии излишни. Не нужно думать, что это просто люди такие глупые попались. Вовсе нет. Как мы увидим дальше, человеческие поступки тоже вполне неплохо программируются. И дело здесь не в умственном развитии людей, которые попадаются на подобные удочки. Просто есть другие люди, которые очень неплохо владеют языком программирования человеческих поступков.

Сейчас интерес к социальной инженерии очень высок. Это можно заметить по многим признакам. К примеру, пару лет назад по запросу "социальная инженерия" в поисковой системе Google было только 2 ссылки. Теперь же их сотни… Известный хакер К. Митник, использующий для взломов методы социальной инженерии, выступает с лекциями в гостинице "Редиссон-Славянская" для топ-менеджеров крупных IT-компаний и специалистов служб безопасности корпораций... По социальной инженерии стали устраивать конференции, в ряде университетов собираются вводить курсы лекций на эту тему…

Однако у многих лекций и опубликованных статей, с которыми ознакомились авторы, есть несколько серьезных недостатков. Во-первых, не объясняется психологическая подоплека применяемых приемов. Авторы статей просто говорят: "Это делается так-то". А почему именно так — никто не объясняет. В лучшем случае приводятся фразы: "в основе этого приема лежат принципы нейролингвистического программирования", что, правда, запутывает еще больше. Иногда еще говорят, что "для того, чтобы не стать жертвой социальных хакеров, нужно развивать в себе психологическое чутье". О том, куда за этим самым чутьем сходить и где его приобрести, тоже ничего не говорится. И, наконец, третий и, пожалуй, самый серьезный недостаток публикуемых в настоящее время статей по социальной инженерии состоит в том, что большинство примеров, которые в них приводятся — надуманные ("киношные"), которые в реальной жизни не сработают. Читатель, изучая этот пример, понимает, что если к нему заявится такой хакер, он его непременно раскусит. Что правда: такого, — раскусит. Но когда к нему приходит настоящий, — он выкладывает ему самые сокровенные секреты. Предлагаемая книга призвана, с одной стороны, устранить эти недостатки и дать читателю реальный психологический минимум, который лежит в основе "социального хакерства". С другой стороны, в книге много реальных, а не выдуманных примеров, что тоже поможет читателю в освоении материала, и покажет основные приемы, которыми действуют социальные хакеры. Прочитав эту книгу, читатели будут в немалой степени защищены от подобных манипуляций. И еще одно небольшое замечание. Во многих местах книга написана в стиле учебника по социальной инженерии. Таким образом, мы нередко писали так, как если бы обучали читателей методам социальной инженерии. Это не из-за того, что нам

хотелось научить читателей методам мошенничества, а потому, что очень часто, для того чтобы распознать манипулятора, нужно знать, как он действует, вжиться в эту роль… Не для того, чтобы кого-то "охмурить", а только для того, чтобы суметь предвидеть опасность и предсказать дальнейшие действия.

Книга будет в одинаковой степени полезна представителям трех видов профессий: IT-специалистам, сотрудникам служб безопасности предприятий и психологам, изучающих социальную инженерию. В первую очередь, книга будет интересна IT-специалистам, причем самого широкого круга профессий: программистам, системным и сетевым администраторам, специалистам по компьютерной безопасности и т. д. Хотя бы потому, что за кражу ценной информации из "недр компьютера" спрашивают именно с IT-специалистов. И именно им в первую очередь приходится "расхлебывать" последствия такой кражи. Нередко на плечи IT-специалистов ложится и выяснение причин утечки информации. В силу этого многие зарубежные университеты уже вводят для специалистов по компьютерной безопасности курс лекций по основам социальной психологии. Книга будет интересна также и "рядовым" пользователям ПК, поскольку именно они наиболее часто выбираются социальными хакерами в качестве наиболее удобных мишеней.

Психологам книга будет интересна по причине того, что в ней впервые изложены основные принципы социальной инженерии и показано, на каких психологических концепциях она базируется. Сотрудникам служб безопасности она полезна по причине того, что за несанкционированное проникновение на объект отвечают именно они, а такие проникновения очень часто строятся на использовании "человеческого фактора".

Читатели книги смогут задать любой вопрос, посвященный методам социального программирования, на специальном форуме на сайте авторов.

Благодарности

Авторы выражают признательность сотрудникам издательства "БХВ-Петербург", благодаря которым наша рукопись увидела свет.

ЧАСТЬ I

Что такое социальная инженерия и кто такие социальные хакеры

В первой части обсуждаются основные концепции социальной инженерии и социального хакерства. Первая глава, как обычно, — это введение в обсуждаемый вопрос, а во второй главе приведены различные примеры использования методов социальной инженерии.

Глава 1.	Социальная инженерия — один из основных инструментов хакеров XXI века
Глава 2.	Примеры взломов с помощью методов социальной инженерии
Глава 3.	Примеры социального программирования
Глава 4.	Построение социальных файрволов
Глава 5.	Психологические аспекты подготовки социальных хакеров

ГЛАВА 1

Социальная инженерия — один из основных инструментов хакеров XXI века

...В начале февраля 2005 года многие специалисты по информационной безопасности нашей страны ждали выступления К. Митника, известного хакера, который должен был рассказать о том, какую опасность представляет собой социальная инженерия, и какими методами пользуются социальные инженеры (которых мы в дальнейшем будем называть социальными хакерами). Увы, ожидания не очень-то оправдались: Митник рассказал лишь об основных положениях социальной инженерии. И много говорил о том, что методы социальной инженерии используют преступники всего мира для получения самой различной засекреченной информации. По мнению многих участников встречи, слушать было интересно, т. к. человек действительно очень обаятельный, но никаких особых тайн раскрыто не было.

Примечание

Кевин Митник — известный хакер, которому противостояли лучшие эксперты по защите информации из ФБР, и осужденный в 90-х годах правосудием США за проникновение во многие правительственные и корпоративные секретные базы. По мнению многих экспертов, Митник не обладал ни значительной технической базой, ни большими познаниями в программировании. Зато он обладал искусством общения по телефону в целях получения нуж-

ной информации и того, что сейчас называют "социальной инженерией".

То же самое можно сказать и о его книгах — никаких особенных откровений там нет. Мы совершенно не исключаем, что Митник это все прекрасно знает, более того, мы даже в этом почти уверены, только, к сожалению, он ничего из того, что действительно знает, не рассказывает. Ни в своих выступлениях, ни в книгах.

Примечание

Что, наверное, в общем-то, и неудивительно, т. к. ФБР взялось тогда за него очень плотно, показав, кто в доме хозяин, и нервы ему подергали изрядно. Было и множество объяснений, и запрет на работу с ЭВМ в течение нескольких лет, и тюремное заключение. Не стоит удивляться тому, что после таких перипетий он стал весьма законопослушным человеком, и не будет не то какие-то секретные базы похищать, но даже и о не секретных вещах станет говорить с большой осторожностью.

В результате таких недоговорок социальная инженерия представляется этаким шаманством для избранных, что не так. Более того, есть еще один важный момент. Во многих описаниях атак пропускаются целые абзацы, если не страницы. Это мы вот к чему. Если взять конкретно схемы некоторых, наиболее интересных атак, и попытаться их воспроизвести согласно написанному, то, скорее всего, ничего не выйдет. Потому что многие схемы К. Митника напоминают примерно такой диалог.

— Вася, дай пароль, пожалуйста!

— Да на! Жалко мне, что ли для хорошего человека.

Разбор же этой "атаки" напоминает примерно следующее: "Вася дал социальному хакеру, потому что он с рождения не умел говорить "Нет!" незнакомым людям. Поэтому основной метод противодействия социальным инженерам — это научиться говорить "Нет"". ...Может быть, эта рекомендация и подходит для Америки, но, боюсь, что не для России, где большинство скорее не умеют говорить "Да", а "Нет" у всех получается весьма неплохо. Действительно, есть тип людей, которые органически не могут отказать другому человеку, но, во-первых, таких людей немного, а всех остальных нужно к такому состоянию подводить. А о том, как подводить, не сказано ни слова.

Примечание

О психологической типологии и о том, как эти знания использовать в социальной инженерии, мы подробно поговорим в *приложении 2*.

Вот примерно это и имеется в виду, когда мы говорим, что у Митника нередко пропускаются целые абзацы. Можно допустить, что первая фраза могла иметь место в начале, а вторая — в конце разговора. Но между ними было еще очень многое и самое интересное. Потому что, чтобы все было так просто, нужно человека погрузить либо в глубокий гипноз, либо вколоть ему "сыворотку правды". Но даже если это так и было, то об этом тоже нужно писать.

В жизни же происходит, как правило, по-другому. И пароли говорят, и базы выносят, не потому что не просто "нет" ответить не могут, а потому что "нет" отвечать бывает, ...очень не хочется. А для того, чтобы человеку, который владеет какой-то серьезной информацией, очень сложно было ответить "нет", нужно его подвести к такому состоянию. Проследив за ним, скажем, в течение недельки. Вдруг что интересное обнаружиться? Может он сам "засланный казачок" или по вечерам на конкурентов подрабатывает, а может дело то вообще серьезнее обстоит: по вечерам он подрабатывает не на конкурентов, а ходит в публичный дом ...для людей с нетрадиционной сексуальной ориентацией, и, будучи для всех прочих примерным семьянином, очень не хочет, чтобы об этом кто-то узнал. Вот имея примерно такую информацию, к нему же можно смело подходить и говорить:

— Вася, а ну скажи-ка мне все пароли, которые знаешь. И доступ мне в свою сеть открой, чтобы я время попусту не терял.

И вот в этом случае уже очень многие Васи ответят:

— Да на, пожалуйста. И пароли дам и доступ открою. Жалко мне, что ли для хорошего человека...

На языке разведчиков это называется "вербовка". И если вдруг в вашей организации все куда-то исчезает, все пароли кому-то известны, подумайте о том, не сел ли кто "на хвост" кому-то из ваших сотрудников. Вычислить того, на кого сели, и тех, кто сел, обычно бывает не сложно. Умные сотрудники служб безопасно-

сти, кстати, прежде чем доверять людям ключевые посты, обычно очень сильно его проверяют на предмет, скажем так, слабых сторон кандидата на должность. И следят за ним, и тесты всякие умные устраивают, чтобы знать, что за человек работать пришел.

...Это вступление написано не для того, чтобы покритиковать К. Митника — каждого из нас есть за что покритиковать — а для того, чтобы показать, что в социальной инженерии не все так просто, как это иногда преподносится, и относиться к этому вопросу нужно серьезно и вдумчиво. Теперь, после этого вступления, как говорится, давайте начнем.

Компьютерная система, которую взламывает хакер, не существует сама по себе. Она всегда содержит в себе еще одну составляющую: человека. Образно выражаясь, компьютерную систему можно представить следующей простой схемой (рис. 1.1).

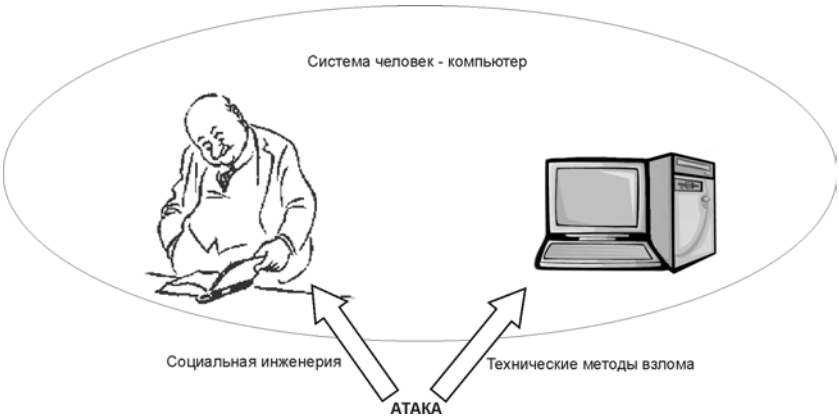


Рис. 1.1. Основные варианты взлома компьютерной системы (человек — с карикатуры Х. Бидструпа)

Задача хакера состоит в том, чтобы взломать компьютерную систему. Поскольку, как мы видим, у этой системы две составляющие, то и основных путей ее взлома соответственно два. Первый путь, когда "взламывается компьютер", мы назовем техническим. А *социальной инженерией* называется то, когда, взламывая компьютерную систему, вы идете по второму пути и атакуете человека, который работает с компьютером. Простой пример. Допус-

тим, вам нужно украсть пароль. Вы можете взломать компьютер жертвы и узнать пароль. Это первый путь. А пойдя по второму пути, вы этот же самый пароль можете узнать, попросту спросив пароль у человека. Многие говорят, если правильно спросить.

По мнению многих специалистов, самую большую угрозу информационной безопасности, как крупных компаний, так и обычных пользователей, в следующие десятилетия будут представлять все более совершенствующиеся методы социальной инженерии, применяемые для взлома существующих средств защиты. Хотя бы потому, что применение социальной инженерии не требует значительных финансовых вложений и досконального знания компьютерных технологий. Так, к примеру, Рич Могулл, глава отдела информационной безопасности корпорации Gartner, говорит о том, что "социальная инженерия представляет из себя более серьезную угрозу, чем обычный взлом сетей. Исследования показывают, что людям присущи некоторые поведенческие наклонности, которые можно использовать для осторожного манипулирования. Многие из самых вредоносных взломов систем безопасности происходят и будут происходить благодаря социальной инженерии, а не электронному взлому. Следующее десятилетие социальная инженерия сама по себе будет представлять самую высокую угрозу информационной безопасности". Солидарен с ним и Роб Форсайт, управляющий директор одного из региональных подразделений антивирусной компании Sophos, который привел пример "о новом циничном виде мошенничества, направленного на безработных жителей Австралии. Потенциальная жертва получает по электронной почте письмо, якобы отправленное банком Credit Suisse, в котором говорится о свободной вакансии. Получателя просят зайти на сайт, представляющий собой почти точную копию настоящего корпоративного сайта Credit Suisse, но в поддельной версии представлена форма для заполнения заявления о приеме на работу. А за то, чтобы рассмотрели заявление, "банк" просил пусть символические, но деньги, которые требовалось перевести на такой-то счет. Когда же деньги перевели весьма много человек, сумма получилась уже не столь символическая. Фальшивый сайт сделан столь мастерски, что экспертам потребовалось время, чтобы убедиться, что это под-

делка. Стоит признать, что злоумышленники применили довольно хитрую комбинацию технологий. Их цель — самые нуждающиеся члены общества, т. е. те, кто ищет работу. Это как раз те люди, которые могут поддаться на такого рода провокацию", — говорится в словах Форсайта. Энрике Салем, вице-президента компании Symantec, вообще считает, что такие традиционные угрозы, как вирусы и спам, — это "проблемы вчерашнего дня", хотя компании обязательно должны защищаться и от них. Проблемой сегодняшнего дня Салем называет фишинг с использованием методов социальной инженерии.

Примечание

Подробно о фишинге — в *главе 2*.

Почему же многие исследователи считают, что социальная инженерия станет одним из основных инструментов хакеров XXI века? Ответ прост. Потому что технические системы защиты будут все больше и больше совершенствоваться, а люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами, и будут самым слабым звеном в цепочке безопасности. Вы можете поставить самые совершенные системы защиты, и все равно бдительность нельзя терять ни на минуту, потому что в вашей схеме обеспечения безопасности есть одно очень ненадежное звено — человек. Настроить человеческий *брандмауэр*, иначе говоря *файрвол* (firewall), — это самое сложное и неблагодарное дело. К хорошо настроенной технике вы можете не подходить месяцами. Человеческий брандмауэр нужно подстраивать постоянно. Здесь как никогда актуально звучит главный девиз всех экспертов по безопасности: "Безопасность — это процесс, а не результат". Очень простой и часто встречающийся пример. Пусть вы директор, и у вас очень хороший сотрудник, который, по вашему мнению, ну уж никогда ничего никому не продаст и никого не продаст. В следующем месяце вы понизили ему зарплату, скажем, по тем или иным причинам. Пусть даже эти причины весьма объективны. И ситуация резко изменилась: теперь за ним глаз да глаз, потому что он места себе не находит от обиды, он уже вас убить готов, что уж тут говорить о каких-то внутрикорпоративных секретах.

Замечу также, что для того, чтобы заниматься обеспечением безопасности, особенно в части настройки "человеческих файрволов", нужно обладать устойчивой нервной и психической системой. Почему, вы поймете из следующей прекрасной фразы А. Эйнштейна, которую мы, вслед за Кевином Митником, не можем не повторить: "Можно быть уверенным только в двух вещах: существовании вселенной и человеческой глупости, и я не совсем уверен насчет первой".

Основная схема воздействия в социальной инженерии

Все атаки социальных хакеров укладываются в одну достаточно простую схему (рис. 1.2).

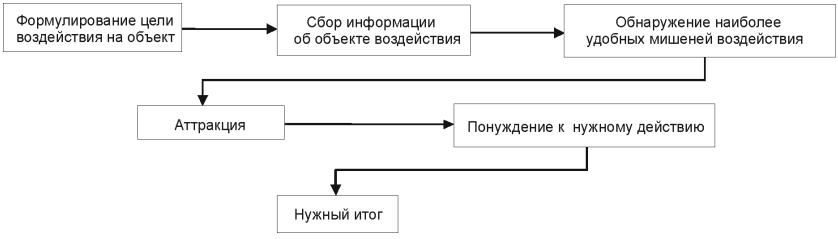


Рис. 1.2. Основная схема воздействия в социальной инженерии

Примечание

Эта схема носит название *схема Шейнова*. В общем виде она приведена в книге белорусского психолога и социолога В. П. Шейнова, долгое время занимавшегося психологией мошенничества. В немного измененном нами виде эта схема подходит и для социальной инженерии.

Итак, сначала всегда формулируется цель воздействия на тот или иной объект.

Примечание

Под "объектом" здесь и далее мы будем иметь в виду жертву, на которую нацелена социоинженерная атака.

Затем собирается информация об объекте, с целью обнаружения наиболее удобных *мишеней воздействия*. После этого наступает этап, который психологи называют *аттракцией*. Аттракция (от лат. *attrahere* — привлекать, притягивать) — это создание нужных условий для воздействия социоинженера на объект. Принуждение к нужному для социального хакера действию обычно достигается выполнением предыдущих этапов, т. е. после того, как достигнута аттракция, жертва сама делает нужные социоинженеру действия. Однако в ряде случаев этот этап приобретает самостоятельную значимость, к примеру, тогда, когда принуждение к действию выполняется путем введения в транс, психологического давления и т. д.

Вслед за В. П. Шейновым, проиллюстрируем данную схему на примере рыбной ловли. Мишень воздействия в данном случае — потребность рыбы в пище. Приманкой служит червяк, кусок хлеба, блесна и т. д. А аттракция — это создание условий, необходимых для успешной рыбной ловли: выбор нужного места ловли, создание тишины, выбор нужной насадки, прикорм рыбы. Принуждение к действию, это, допустим, рывки удилищем, благодаря которым червяк или другая насадка дергается и рыба понимает, что пища может и уйти и надо действовать активнее. Ну а с итогом все понятно.

Другой пример: подкуп сотрудника. Здесь мишень — потребность сотрудника предприятия в деньгах. О том, что он в них нуждается и что с большой вероятностью "примет предложение", узнается на этапе сбора информации. Аттракцией может быть, к примеру, создание таких условий, при которых сотрудник будет в деньгах очень нуждаться.

> ***Примечание***
>
> Эти условия часто создаются умышленно. Банальный пример — ехал сотрудник на машине и "слегка попал в аварию", после которой и машину надо ремонтировать, и тому джипу, в который он врезался, деньги заплатить. Количество таких "дорожных подстав" сейчас выросло неимоверно, и исполнителей найти не сложно.

Теперь кратко остановимся на таком популярном виде преступлений, как *кража баз данных*.

Примечание

Кража баз данных — это одна из основных областей применения социальной инженерии. Разговор о кражах баз данных мы продолжим также и в *главе 2*.

Каких только баз сейчас не найдешь: и базы МГТС, и базы Центробанка, и базы Пенсионного фонда, и базы БТИ, и базы МВД с ГИБДД, и базы по прописке... В настоящий момент эксперты спорят о том, к какому виду преступлений относить кражу клиентских баз данных. С одной стороны, данный вид преступлений, вроде бы, по мнению многих экспертов, относится к преступлениям в области IT. Те, кто так считают, исходят из того простого положения, что базы данных хранятся на жестких дисках серверов, и, значит, если их украли, то это преступление в IT. Но с другой стороны, это не совсем так, потому что большинство краж совершаются с использованием методов социальной инженерии.

Кто и каким способом ворует базы данных? Если в ответ на этот вопрос вы услышите, что их воруют хакеры, взламывая корпоративные серверы государственных органов и крупных компаний — не верьте этому. Это не так. Все гораздо проще и прозаичнее. Воруют их обыкновенные люди, не пользуясь, в большинстве случаев, никакими сложными приборами, если таковым не считать обыкновенный накопитель Flash Drive, подключаемый к порту USB.

Как мы уже говорили, примерно в 80 случаях из 100 информацию воруют не по техническому каналу, а по социальному. Таким образом, это не хакеры сидят ночи напролет и взламывают серверы, а, скажем, обидевшийся системный администратор уволился. Но не один, а вместе со всеми базами данных и всей информацией о предприятии. Или за умеренную плату сотрудник компании сам "сливает" на сторону информацию о компании. Или просто пришел человек со стороны, представился лучшим другом системного администратора, и сел налаживать "глючную" базу данных, потому что лучший друг нынче болен. После его ухода эта база действительно стала работать лучше, но — в другом месте. Если вы считаете, что это очень тривиально и проходит только в маленьких и совсем уж беспечных компаниях, то вы зря так считаете. Совершенно недавно именно так похитили ценную информа-

цию в одной из весьма крупных питерских компаний, работающих в области энергетики. И таких примеров очень много. Тот факт, что основной канал утечки информации — социальный, задачу защиты информации крайне сильно усложняет. Потому что вероятность утечки по техническому каналу в принципе можно свести к нулю. Можно сделать сеть очень защищенной, что никакая атака извне ее "не прошибет". Можно вообще сделать так, что внутренняя сеть учреждения не будет пересекаться с внешней, как это сделано в российских силовых ведомствах, к примеру, где внутренние сети не имеют выхода в Интернет. Кабинеты руководства и все кабинеты, в которых проводятся важные совещания, следует оборудовать средствами защиты от утечки информации. Никто ничего на диктофон не запишет — мы поставили подавители диктофонов. По радиоканалу и каналу побочных электромагнитных излучений никто ничего не прослушает — поставили генератор радиошума. Виброакустический канал тоже перекрыли, невозможен и лазерный съем информации по колебаниям оконного стекла, через вентиляционные шахты тоже никто ничего не услышит. Телефонные линии защитили. ...Итак, все сделали. А информация все равно "сделала ноги". Как, почему? А люди унесли. Без всяких сложных технических манипуляций. В очередной раз сработал тот самый пресловутый и навязший в зубах человеческий фактор, о котором все вроде бы и знают, и о котором все стараются забыть, живя по принципу "пока гром не грянет...". Заметьте: похитить информацию из сетей государственных органов по техническому каналу практически невозможно. А она, тем не менее, похищается. И это является еще одним доказательством того, что, в основном, информацию похищают с использованием людей, а не технических средств. Причем похищают иногда до смешного просто. Мы проводили аудит одного крупного предприятия нефтехимической отрасли на предмет организации в нем защиты информации. И выяснили интересную штуку: доступ к столу секретаря генерального директора могла иметь любая ночная уборщица. И имела, судя по всему. Вот такая демократия царила на этом предприятии. А бумаг на этом столе столько было разбросано, что по ним можно было составить представление почти обо всей нынешней деятельности предприятия и о планах его развития на ближайшие

5 лет. Оговоримся еще раз, что это действительно крупное предприятие, с солидной репутацией и миллионными оборотами. В долларовом эквиваленте, конечно. А защита информации была поставлена... Впрочем, никак она не была поставлена. Еще один интересный социоинженерный канал утечки информации — это различные выставки, презентации и т. д. Представитель компании, который стоит у стенда, из самых лучших побуждений, ради того, чтобы всем понравиться, нередко выдает самые сокровенные секреты компании, которые ему известны, и отвечает на любые вопросы. Я не раз это говорил многим своим знакомым директорам, и один из них в шутку предложил мне подойти к представителю его компании на ближайшей выставке и попытаться таким образом что-нибудь этакое у него выведать. Когда я принес ему диктофонную запись, он, можно, сказать, плакал, потому что одна из фраз звучала примерно так: "А вот недавно наш директор еще ездил в Иран...". Этот способ добычи информации, кстати, используется немалым количеством фирм.

Примечание

Подробнее о том, как выведывается информация на презентациях — в *главе 2*.

...К сожалению, многие люди крайне беспечны, и не хотят заботиться о сохранности информации. Причем часто даже в очень крупных организациях это "не хотение" простирается от самых рядовых сотрудников до генерального директора. И при таком раскладе один системный администратор или начальник службы безопасности, будь они даже полными параноиками, помешанными на защите информации, ситуацию не спасут. Потому что на данный момент, увы, даже те из руководителей, которые понимают, что информацию защищать надо, не всегда осознают еще одну вещь: что защита информации должна быть системной, т. е. проводится по всем возможным каналам утечки. Вы можете сколько угодно защищать компьютерную сеть, но если люди получают низкую зарплату и ненавидят предприятие, на котором они работают, хлеще, чем советский народ гитлеровских оккупантов, то на эту защиту можно даже не тратить денег. Другой пример несистемности можно нередко наблюдать, ожидая приема

у дверей какого-нибудь директора. Очень нередки случаи, когда те, кто конструирует систему безопасности, не учитывают такую вещь: директора имеют свойство говорить громко, иногда срываясь на крик. Двери же в кабинет генерального директора часто настолько звукопроницаемы, что совещающихся в "генеральском" кабинете можно слушать, совершенно не напрягаясь, даже если они говорят шепотом. Как-то я[1] приехал в Москву к одному "близкому к телу" директору проконсультироваться с ним на предмет, что же ожидает дальше нашу отрасль. А у него как раз случилось важное незапланированное совещание, и меня попросили подождать. Посидев 15 минут у его кабинета, я понял, что узнал гораздо больше того, что хотел узнать, и в принципе можно уезжать. Остался только из приличия. Пикантность ситуации в том, что когда дошла очередь до меня, на мои вопросы директор почти не ответил, говоря, что, мол, сам понимаешь, очень конфиденциально, я и сам пока не очень-то в курсе... И так далее. Тем не менее, я его очень горячо и любезно поблагодарил.

...Возвращаясь к базам данных, содержащих конфиденциальные сведения, следует отметить, что после вышенаписанного полностью понятно, кто и как их крадет. Обыкновенные люди их крадут. Очень часто — сами же сотрудники предприятий. Недавно вот осудили таможенника в чине подполковника, который снабжал рынок таможенными базами данных. В соседнем регионе поймали за руку начальника отдела налоговой инспекции, который за умеренную плату сливал данные местным криминальным браткам. И так далее.

Для чего их воруют и кому это нужно? Нужно это многим. От млада до велика. Нужно как рядовым гражданам, так и "финансовым акулам". Если начать с граждан, то не вдаваясь в глубинные рассуждения об особенностях русского менталитета, скажем лишь, что пока в справочных службах наших "телекомов" сидят крикливые и всем недовольные барышни, то даже самому законопослушному и честному человеку гораздо проще для своих

[1] Здесь и далее, когда повествование ведется от первого лица, это означает, что либо приводимые примеры из коллекции одного из авторов, либо излагается личный опыт одного из авторов. — *Прим. авт.*

нервов пойти и купить эту базу номеров телефонов организаций на рынке пиратского ПО, чем позвонить на справочную службу.

Это по понятным причинам нужно всем тем, кто занимается конкурентной разведкой.

Это нужно криминалитету. К примеру, каждый уважающий себя угонщик автомобилей имеет базу ГИБДД. Криминалу также немаловажно знать, не обделяют ли его те, кого он "крышует". Домушники находят себе жертв с помощью баз данных.

Это нужно финансовым гигантам, практикующим практику рейдерских наездов.

> ***Примечание***
>
> *Рейдерские наезды* — это такая практика в новой российской истории, при которой, грубо говоря, большая компания прибирает к рукам те компании, которые меньше с помощью так называемых рейдеров. Допустим, некая большая компания захотела купить какую-то другую компанию, которая поменьше. Для этого она делает заказ рейдерам, — людям, которые построят план захвата компании и его исполнят. Подробно о рейдерах рассказано в *главе 2*.

...Продолжать можно долго. В общем, рынок обширен и спрос на продукцию есть. А спрос всегда рождает предложение. Это один из основных законов экономики. Если есть спрос, обязательно, рано или поздно, дорогое или дешевое, но предложение будет. Каким бы этот спрос не был. Даже если этот спрос очень кощунственный, к примеру, спрос на детские органы. Страшнее спрос сложно придумать. А все равно предложение есть. Что уж тут говорить про какие-то базы данных.

> ***Примечание***
>
> В настоящее время цена вопроса на воровство одной базы данных крупного предприятия составляет около $2000.

Можно ли вообще прекратить воровство баз данных? На государственном уровне это можно сделать, наверное, только ужесточив наказание за данное преступление. Хотелось бы посмотреть на того, кто осмелился бы своровать какую-то базу в советские времена. Правда, "ужесточив", это не совсем тот термин: дело в том, что сейчас базы данных можно красть практически