**Социальная инженерия**

Кевин Митник – в прошлом хакер, взломавший информационные системы крупнейших компаний мира, а ныне консультант по информационной безопасности, учредитель компании Mitnick Security Consulting. Автор книг «Искусство обмана» и «Искусство вторжения».

Сегодня человеческий фактор в информационной безопасности играет гораздо более важную роль, чем 20 лет назад, когда Интернет не был коммерческим и его пользователями были лишь специалисты. Многие компании, которые думают, что проблему информационной безопасности можно решить просто с помощью аппаратных и программных средств, сильно заблуждаются. Технологии безопасности, которым мы привыкли доверять, – межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и другие – малоэффективны в противостоянии хакерам, использующим методы социальной инженерии. Необходима мощная работа с персоналом, обучение сотрудников применению политики безопасности и техникам противостояния социоинженерам – только тогда ваша система безопасности будет комплексной.

**Непрямая атака**

Представьте ситуацию: крупный московский офисный центр. Вы входите в лифт и видите на полу компакт-диск с логотипом известной компании и наклейкой: «Строго конфиденциально. Заработная плата сотрудников за 2005 год». Самая естественная человеческая реакция – взять этот диск, отнести в свой офис и вставить в CD-ROM своего рабочего компьютера. Предположим, вы так и сделали. На диске – файл со знакомой иконкой MS Excel. Вы пытаетесь его открыть, но вместо столбиков цифр и фамилий видите лишь сообщение операционной системы: «ошибка, файл поврежден». В этот момент на ваш компьютер, помимо вашей воли и вашего ведома, загружается вредоносная программа. В лучшем случае это «троянец», отслеживающий, какие клавиши вы нажимаете и какие совершаете операции, и передающий эту информацию по мгновенно налаженному каналу связи на чужой компьютер. В худшем варианте – вирус, который в считанные мгновения разрушит вашу информационную систему и распространится по локальной сети, пожирая всю корпоративную информационную систему. Вы ведь подключены к локальной сети, правда?

Это типичный пример социальной инженерии – нарушения информационной безопасности компании с помощью воздействия на человека. Есть много способов манипулировать людьми, и любопытство – только один из мотивов, которые можно использовать.

Почему злоумышленники прибегают к социальной инженерии?

Это проще, чем взломать техническую систему безопасности.

Такие атаки не вычислить с помощью технических средств защиты информации.

Это недорого.

Риск – чисто номинальный.

Работает для любой операционной системы.

Эффективно практически на 100%.

База для социоинженера

Первый этап любой атаки – исследование. Используя официальную отчетность компании-жертвы, ее заявки на патенты, сообщения о ней в прессе, рекламные буклеты этой фирмы и, конечно же, корпоративный сайт, хакер пытается получить максимум информации об организации и ее сотрудниках. В ход идет даже содержимое мусорных корзин, если его удается раздобыть. Социоинженер выясняет, кто в компании имеет доступ к интересующим его материалам, кто в каком подразделении работает и где это подразделение расположено, какое программное обеспечение установлено на корпоративных компьютерах... Словом, все, что только можно.

Хакер всегда стремится выдать себя за того, кто имеет право на доступ к интересующим его данным и кому эти данные действительно нужны по долгу службы. Для этого он должен свободно ориентироваться в терминологии, владеть профессиональным жаргоном, знать внутренние порядки компании-жертвы. Затем следует разработка плана атаки: предстоит изобрести предлог или схему обмана, которые помогут построить доверительные отношения с нужным сотрудником. Если атака прошла успешно и работник организации ничего не заподозрил, хакер, скорее всего, не ограничится одним вторжением, а вернется и будет дальше пользоваться возникшим доверием.

Ошибка резидента (пример из фильма «Дневной дозор»): главный герой (Антон Городецкий), успешно сымитировав личность представителя вражеского стана, пытается проникнуть в этот самый стан. Проходя мимо охранника, он небрежно бросает ему: «Привет, Витек!» - ориентируясь на бейдж с именем стража, приколотый к его пиджаку. Разоблачение следует немедленно: пиджак на охраннике – чужой.

Самые распространенные методы атак:

Выяснение, передача или несанкционированная смена паролей

Создание учетных записей (с правами пользователя или администратора)

Запуск вредоносного программного обеспечения (например, «троянца»)

Выяснение телефонных номеров или иных способов удаленного доступа к корпоративной информационной системе

Фишинг (электронное мошенничество)

Несанкционированное добавление дополнительных прав и возможностей зарегистрированным пользователям системы

Передача или распространение конфиденциальной информации.

**Прямая атака**

В «доэлектронную эру» социальной инженерией пользовались злоумышленники, звонившие по телефону. Например, для того чтобы получить доступ к базе абонентов телефонной компании, достаточно было позвонить туда и представиться сотрудником сервисной службы, совершающим плановую проверку, или работником органов власти, уточняющим данные. Главное – выбрать нужный тон. Этот метод действует и сейчас, а современные средства телефонии только облегчают хакерам задачу. Так, с помощью специальной приставки к аппарату звонящий может изменить тембр голоса. А использование офисной мини-АТС помогает замести следы – усложнить определение номера, с которого звонят. Хакер набирает один из телефонов компании и спрашивает у сотрудника его логин и пароль, представляясь системным администратором. Если это крупная организация, где не все сотрудники знают друг друга, велика вероятность того, что пользователь сообщит социоинженеру интересующие его данные.

Невероятно, но факт: в ходе специального исследования 7 из 10 офисных сотрудниц лондонского вокзала Ватерлоо назвали свои логин и пароль незнакомцу в обмен на шоколадку!

С распространением компьютеров возможности социальной инженерии расширились. Теперь для атаки можно использовать электронную почту или ICQ. Иногда даже не нужно подделывать стиль того, от чьего имени пишешь, и сотрудник все равно ничего не заподозрит. Например, человеку приходит «письмо от начальства»: «Прошу направить мне копию базы данных по клиентам Северного Федерального округа в формате MS Excel в срок до 15.00 сегодня, 5 марта». Он, конечно же, направит – и прости-прощай секретные данные. Или «письмо от системного администратора»: «Уважаемые коллеги! В связи с обновлением версии системы совместной работы ваш логин и пароль изменен. Ваш новый логин и пароль – во вложенном файле». На самом же деле вложение содержит вирус, выводящий из строя операционную систему. Последнее – реальный пример из недавней практики московской компании «Тауэр».

Бреши в информационной системе – сотрудники обычно:

считают, что корпоративная система безопасности непогрешима, и теряют бдительность

легко верят полученной информации, независимо от ее источника

считают соблюдение корпоративной политики безопасности пустой тратой времени и сил

недооценивают значимость информации, которой владеют

искренне хотят помочь каждому, кто об этом просит

не осознают пагубных последствий своих действий.

**Ключик к каждому**

В различных странах люди по-разному подвержены социоинженерному воздействию. Россияне – не самая доверчивая нация, а вот жители США и Японии очень внушаемы. В каждой стране есть свои культурные особенности, которые должен учитывать социоинженер. Например, на западе прекрасно работает «норма взаимности»: если человеку сделать что-то приятное, он будет чувствовать себя обязанным и при первой же возможности постарается отплатить добром. В Испании атака успешнее всего пройдет, если использовать личное доверие, завязать с жертвой приятельские отношения. А немец скорее поддастся на уловки хакера, если сыграть на его приверженности к корпоративному порядку.

Независимо от национальности, наиболее уязвимы для атак социоинженеров новые сотрудники. Как правило, им еще не успели рассказать о всех существующих корпоративных правилах, они не изучили регламентов информационной безопасности. Новички еще не знают всех своих коллег, особенно лично. К тому же, им свойственна повышенная доверчивость и готовность помочь, дабы зарекомендовать себя как активных и отзывчивых членов команды, на которых можно положиться. Они вряд ли будут интересоваться правами доступа социального инженера, который выдает себя за другого сотрудника, особенно вышестоящего.

Возможно, вас атакуют, если ваш собеседник:

проявляет к вам повышенный интерес, преувеличенное внимание и заботу

отказывается дать вам свои координаты

обращается к вам со странной или необычной просьбой

пытается втереться к вам в доверие или льстит вам

говорит с вами подчеркнуто начальственным тоном.

Даже самые бдительные сотрудники не всегда могут распознать социальную инженерию. Да они и не должны действовать как детектор лжи. Ключевой фактор успеха – обучение. Политики безопасности должны войти в плоть и кровь каждого, кто работает в компании. И, разумеется, прежде чем втолковывать сотрудникам суть этих политик, нужно их разработать.

Светлана Шишкова, E-xecutive