ББК С832.3

Павлова Ю.В., Быкова А.В.

Социальная инженерия: основные методы воздействия социальных хакеров

В современном мире информация принимает все большее значение, и способы ее защиты становятся одним из важнейших насущных вопросов каждого человека. Компьютерные системы являются общеизвестным местом хранения данных. Технический прогресс движется вперед, разрабатываются тысячи способов защиты информации, подразумевающих под собой аппаратное и программное обеспечение. Однако, основное внимание следует уделять не этим элементам защиты, а роли человеческого фактора в этом вопросе. Анализируя причины и методы взлома программного обеспечения или каналы утечки информации из различных структур, исследователи пришли к выводу о том, что примерно в 80% причина этого - человеческий фактор сам по себе или умелое манипулирование им.

Информация защищается людьми и основные носители информации-люди, с обычным набором комплексов, слабостей, на которых играют, достигая свои цели, социальные хакеры. Защититься от них можно только зная их методы работы.

У системы две составляющие и основных путей ее взлома соответственно два. Первый путь, когда "взламывается компьютер" - технический. А *социальной инженерией* называется то, когда, взламывается компьютерная система, по второму пути, и атакуется человек, который работает с компьютером.

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. Можно поставить самые совершенные системы защиты, и все равно бдительность нельзя терять ни на минуту, потому что в схеме обеспечения безопасности есть одно очень ненадежное звено – человек.

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. 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.

Фишинг на сегодняшний день является одним из самых распространенных видов социальной инженерии. По сути фишинг это выведывание информации для доступа к банковским счетам доверчивых пользователей. Он распространен в тех странах, где пользуются популярностью услуги интернетбанкинга. Чаще всего "фишеры" используют поддельные электронные письма, якобы присылаемые банком, с просьбой подтвердить пароль или уведомление о переводе крупной суммы денег.

Суть фишинга сводится к следующему. Злоумышленник заставляет пользователя предоставить ему какую-либо секретную информацию: информацию о банковских счетах, кредитных картах и т. д. Самое важное в том, что жертва совершает все эти действия абсолютно добровольно, – фишеры хорошие психологи и действуют четко.

Выделяют три основных вида фишинга:

1)почтовый;

2)онлайновый;

3)комбинированный.

Суть *почтового фишинга* в том, что жертве отправляется электронное письмо, в котором содержится просьба выслать те или иные конфиденциальные данные. К примеру, от имени интернет-провайдера с похожего (или идентичного) почтового адреса отправляется письмо, в котором написано, что по провайдеру нужно узнать логин и пароль для доступа в Интернет указанного пользователя, так как сам провайдер по тем или иным техническим причинам (например, база "рухнула") этого сделать не может.

Онлайновый фишинг заключается в том, что мошенники один в один копируют какой-либо из известных сайтов, причем для него выбирается очень похожее доменное имя (или то же самое, только в другой зоне), и создается идентичный дизайн. Данный вид фишинга иногда еще называют *имитацией бренда.*

Комбинированный фишинг является объединением двух предыдущих видов фишинга. Его появление вызвано тем, что почтовый и онлайновый фишинг уже достаточно устарели, да и пользователи стали грамотнее в части информационной безопасности. Поэтому фишеры придумали другую тактику. Так же как в онлайновом фишинге создается поддельный сайт, а потом как в почтовом фишинге пользователям отсылаются письма с просьбой зайти на этот сайт.

Это достаточно сильный психологический ход, благодаря которому комбинированный фишинг сразу же получил огромное распространение. Дело в том, что посетители стали настороженнее, и уже немногие просто так скажут свои пароли (хотя и такие встречаются). А в комбинированном фишинге эта настороженность как раз и снимается, благодаря тому, что в письме пользователя не просят сообщать какие-либо конфиденциальные

данные, а просто просят зайти на сайт. Пользователю просто предлагается зайти на какой-либо сайт, и самому проделать все необходимые операции.

Естественно, законодательства всех стран оказались неприспособленными к этому новому виду мошенничества.

В России первый зарегистрированный случай фишинга датируется маем 2004 года, когда клиенты Сити-банка получили по электронной почте письма с просьбой зайти на сайт банка (лжесайт, естественно) и подтвердить номер своей карты и ПИН-код.

Следует рассмотреть известные способы борьбы с фишингом.

Поскольку суть фишинга состоит в получении паролей и банковских сведений, необходимых для доступа к электронным счетам пользователей, одним из выходов в этой ситуации будет использование *генераторов одноразовых паролей*, позволяющее обойти этот вид мошенничества. Генератор одноразовых паролей на вид напоминает обычный небольшой карманный калькулятор. Когда пользователь заходит на сайт банка, для того чтобы получить доступ к своему счету, ему необходимо ввести показанную генератором последовательность символов. Банк применяет тот же алгоритм для создания пароля. Доступ предоставляется только в том случае, когда оба пароля совпадают. Такой пароль нельзя украсть по той простой причине, что доступ по нему можно получить только один раз. Минусы использования такой системы состоят в дополнительных расходах для клиентов. Еще один способ - *мобильное подтверждение.* Суть этого приема в том, что доступ к карте осуществляется только после того, как пользователь отправит со своего мобильного телефона**,** номер которого он сообщил банку, какое-либо сообщение. *Еще один метод борьбы - это хеширование паролей конкретного веб-сайта.* Хеширование паролей предотвращает кражу конфиденциальных данных путем добавления к паролю информации, специфичной для того сайта, где предполагается применить пароль. Пользователь просто вводит в специальной форме свой пароль, а браузер преобразует его и добавляет необходимую информацию. Суть в том, что веб - сайту, на котором пользователь вводит пароль, этот пароль в чистом виде не сообщается, на сайт приходит уже хешированный пароль. Таким образом, даже если пользователь и введет свой пароль на фальшивом сайте, то хакеры его применить не смогут. На настоящем же сайте применяется та же схема хеширования, что и у владельца карты.

Более опасным видом мошенничества, чем фишинг, является так называемый ***фарминг.*** Фарминг заключается в изменении адресов так, чтобы страницы, которые посещает пользователь, были не оригинальными страницами, скажем, банков, а фишинг - страницами.

Поскольку суть фарминга сводится к автоматическому перенаправлению пользователей на фальшивые сайты, фарминг гораздо более опасен, чем фишинг, так как в отличие от последнего новый метод хищения данных не требует отсылки писем потенциальным жертвам и соответственно их ответа на них. Это, естественно, более изощренный, хотя и технически намного

более сложный метод мошенничества, чем фишинг. Но зато при фарминге у пользователя практически нет причин проявлять свою недоверчивость: писем никто не присылал, на сайт никто заходить не просил. Пользователь сам по своему желанию решил зайти на сайт банка, и зашел. Только не на оригинальный, а на поддельный сайт.

Следует обратить внимание на еще один важный момент. Очень часто, когда речь заходит о безопасности предприятия, в том числе, когда дело касается социальной инженерии, защита идет только от внешней угрозы, совершенно игнорируется то, что опасность может подкрасться изнутри. Пока идет поиск, атаки снаружи, атака происходит изнутри за счет собственных сотрудников. Конечно, немалая часть сотрудников - честные и порядочные люди, но... люди есть люди, а у людей есть пороки.

Согласно статистике процент честных людей равен 30. 50% готовы нарушить закон в том случае, если они будут уверенны в своей безнаказанности. Оставшиеся же 20% готовы нарушить закон при любых условиях.

Мотивы краж могут быть самыми разными - от недовольств зарплатой, до чисто клептоманического стиля поведения. Рассмотрение этого вопроса с точки зрения инженерии представляет интерес потому, что именно на тех пороках и играют, как правило, социальные хакеры.

Чтобы не допустить того, чтобы организация стала добычей социальных инженеров социальных хакеров, следует ***наблюдать за сотрудниками на всех стадиях их развития в организации.*** Любой сотрудник в организации всегда проходит три стадии развития:

1) устройство на работу;
2) этап работы;
3) увольнение.

При приеме сотрудника на работу необходимо собрать о нем как можно больше сведений, с целью прогноза того, как он поведет себя в той или иной ситуации. Как правило, такую проверку проще всего сделать с помощью стандартных психологических тестов, которые сейчас приведены практически на любом сайте по психологии. Основная проблема в соблюдении этого правила состоит в том, что за сотрудником, если и наблюдают, то только в период его устройства на работу. В лучшем случае – в период его работы на предприятии. И практически никто не проводит работу с увольняющимися сотрудниками, хотя они и представляют основную угрозу для безопасности предприятия. Во-первых, потому что нередко сотрудники увольняются, затаив, по объективным или субъективным причинам, злость на свое, уже почти бывшее руководство. А от злости и до мести недалеко. Во-вторых, сотрудников могут вынудить к увольнению конкуренты, попросив его уволиться не одного, а вместе с клиентской базой. И не допустить этого – основная задача службы безопасности предприятия или тех, кто выполняет ее функции.

Еще одним методом похищения секретной информации является способность социальных хакеров использовать такой человеческий фактор,

как невнимательность, беспечность сотрудников организации. В некоторых фирмах, наряду с мощной технической защитой, царит почти полная «демократия». Важные документы могут быть разбросаны прямо на столе невнимательного сотрудника, и чаще всего этот сотрудник оставляет кабинет незапертым, когда выходит. Любая уборщица будет иметь доступ к такой информации.

Еще один интересный социоинженерный канал утечки информации - это различные выставки, презентации и т.д. Представитель компании, который стоит у стенда, из самых лучших побуждений, из-за того, чтобы всем понравиться, нередко выдает самые сокровенные секреты компании, которые ему известны и отвечает на любые вопросы.

Подводя итог, можно сказать, что проблема использования методов социальной инженерии действительно существует и игнорировать ее нельзя. Помимо технической защиты, следует изучать рекомендуемую психологами практическую информацию, для того, чтобы научиться распознавать социальных хакеров и защищаться от них.