**Психология на службе хакеров**

Владимир Безмалый

Как бы вы ни изощрялись в технических решениях, помните, что главная угроза безопасности вашей сети всегда будет исходить от ваших же пользователей.

Для атаки вашей организации хакеры, использующие приемы социальной инженерии, эксплуатируют доверчивость, лень, хорошие манеры, энтузиазм вашего персонала и многое-многое другое. Трудно защититься от нападения этого типа, адресаты могут не понять, что они были обмануты, или не признавать этого.

Хакер в данном случае пытается убедить ваших сотрудников выдать информацию, которая даст возможность ему использовать ваши системные ресурсы. Традиционно этот подход известен как мошенничество. Многие маленькие и средние компании полагают, что хакерские нападения — проблема для больших корпораций или банков, ведь это сулит большую финансовую выгоду, чем нападение на маленькие компании. Такой подход, возможно, был справедлив в прошлом, однако теперь хакеры атакуют все общество. Преступники могут захватить компанию, атакуя фонды или ресурсы, но они также могут использовать вашу компанию как площадку для нападения на другие компании.

Чтобы защищать персонал от таких атак, вы должны знать, какое нападение ожидать, его возможные цели, потенциальные потери. Тогда вы сможете усилить политику безопасности, включив в нее защиту от подобных атак.

Социальная инженерия — совокупность подходов в прикладных социальных науках, ориентированных на:

\* изменение поведения и установок людей;

\* решение социальных проблем;

\* адаптацию социальных институтов к изменяющимся условиям;

\* сохранение социальной активности.

Глоссарий.ру

В отношении информационной безопасности социальная инженерш) позволяет организовывать и описывать прежде всего угрозы нетехнического

**Угрозы социальной инженерии и защищенность**

Как утверждается в опубликованном на сайте Microsoft руководстве по защите от угроз, связанных с воздействием социальной инженерии [1], на сегодня существует пять основных путей проникновения злоумышленников, использующих мошеннические методы: воздействие через Internet, телефон, анализ мусора, личные подходы, реверсивная социальная инженерия.

**Воздействие через Internet**

Персонал использует информацию и отвечает на внешние и внутренние запросы по электронным каналам. Это дает возможность хакерам подобраться к сотрудникам, используя относительную анонимность Internet. Вы часто слышите об атаках, использующих электронную почту, всплывающие приложения, и атаках, использующих системы мгновенной передачи сообщений, «троянские» вирусы, саморазмножающиеся вирусы или вредоносное ПО, которое повреждает или компрометирует компьютерные ресурсы. От большинства подобных нападений можно уберечься с помощью антивирусной защиты. Однако злоумышленник, использующий методы социальной инженерии, убеждает сотрудника выдать необходимую ему информацию с помощью правдоподобного психологического трюка вместо того, чтобы заразить компьютер вредоносным ПО путем прямого нападения. Такая атака сможет подготовить почву для вредоносного ПО. Поэтому вы должны советовать персоналу, как лучше всего идентифицировать интерактивные нападения, которые используют социальную инженерию, и избежать их.

**Угрозы с использованием электронной почты**

Использование электронной почты как инструмента социальной инженерии стало обычным за прошлое десятилетие. По данным отчета Anti-Phishing Work Group (APWG), в месяц обнаруживается более 20 тыс. фишинговых рассылок и около 30 тыс. новых фишерских Web-сайтов [2].

В первом полугодии 2006 года фишеры отправили 157 тыс. уникальных писем, что на 81% больше по сравнению со вторым полугодием 2005 года, сообщается в отчете по угрозам Internet-безопасности, подготовленном компанией Symantec [3]. Авторы отчета подчеркивают, что каждое такое письмо может быть отправлено сотням тысяч Internet-пользователей. По мнению экспертов APWG, такой рост стал возможен благодаря появлению наборов утилит, которые позволяют в короткие сроки создать фишинг-сайт.

Много сотрудников получают десятки и даже сотни электронных писем каждый день от деловых и частных корреспондентов. Большой объем электронной почты мешает уделять внимание каждому сообщению. Этим-то и пользуются злоумышленники .

Фишинг (phlshlng) — технология Internet-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. (см. рис. 1).

Если посмотреть внимательно, то можно найти два различия между письмом и результатом:

текст в почте заявляет, что сайт безопасен, используя протокол HTTPS, однако на экране показано, что сайт фактически использует HTTP.

название компании в почте — Contoso, но ссылка указывает на компанию Comtoso.

Благодаря такому камуфляжу электронная почта кажется более правдоподобной. Каждое фишинг-письмо маскируется под запрос о пользовательской информации, который якобы должен облегчить пользователю установку обновления или обеспечить дополнительное обслуживание (см. рис. 2).

В июле 2006 года появилась новая разновидность фишинга, тут же получившая название вишинг (vishing). В сообщениях этого типа содержится просьба позвонить на определенный городской номер. При этом потенциальная жертва слышит сообщение, в котором ее просят сообщить свои конфиденциальные данные. Владельцев такого номера найти непросто, так как с развитием IP-телефонии звонок на городской номер может быть автоматически перенаправлен в любую точку земного шара на виртуальный номер.

Согласно информации Secure Computing [4], мошенники конфигурируют режим автонабора, который набирает номера в определенном регионе, и при ответе на звонок происходит следующее:

• автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру немедленно;

• когда по этому номеру перезванивают, на другом конце провода отвечает типично компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона;

• как только номер введен, вишер становится обладателем всей необходимой информации (номер телефона, полное имя, адрес);

• затем, используя этот звонок, можно собрать и дополнительную информацию: PIN-код, срок действия карты, дата рождения, номер банковского счета и т.п.

Пока серьезных инцидентов такого рода еще не отмечено. Но только пока...

В сети, однако, существует еще более серьезная угроза — фарминг (pharming) — перенаправление жертвы по ложному адресу [5]. Этот механизм имеет много общего со стандартным вирусным заражением. Жертва открывает почтовое послание или посещает некий Web-сервер, на котором выполняется исполнимый скрипт-вирус, при этом искажается файл hosts. В результате пользователь попадает на один из ложных сайтов. Механизмов защиты от фарминга на сегодня просто не существует.

Большинство мер защиты основаны на том, чтобы не пропустить неправомочных пользователей. Однако злоумышленник может обойти много защитных средств, если отправит в компанию через ссылку «троянца», саморазмножающийся червь или вирус. Гиперссылка может также привести на сайт, использующий всплывающие окна (приложения), чтобы предложить помощь или информацию.

Чтобы более эффективно сопротивляться хакерским нападениям, использующим социальную инженерию, надо осторожно относиться к поступающей электронной почте. Необходимо включить в политику безопасности руководство, которое охватывает вопросы ее использования: вложений и гиперссылок в сообщениях; запросов о персонале или информации компании изнутри компании; запросов о персонале или информации компании извне. Эти рекомендации нужно дополнить примерами фишинговых нападений.

**Всплывающие приложения и диалоговые окна**

Многие сотрудники просматривают Internet с личными целями. Это чревато опасностью контакта со злоумышленниками, использующими социальную инженерию. Хотя злоумышленники могут не иметь цель напасть именно на вашу компанию, но они могут использовать ее персонал для получения доступа к ресурсам. Чаще всего преследуется цель внедрить почтовый сервер в пределах вашей компьютерной сети, через которую затем начать фишинг или иные почтовые нападения на другие компании или физических лиц.

На рис. 3 показана страница, на которой гиперссылка, как кажется пользователю, связывается с безопасным сайтом управления учетными записями, однако строка состояния показывает, что пользователь перенаправлен на хакерский сайт. В зависимости от браузера, который используется, хакер может подавить или переформатировать информацию строки состояния.

Два простейших метода соблазнить пользователя перейти по ссылке в диалоговом окне — прислать предупреждение о проблеме, которое выглядит как отображение реалистической операционной системы или прикладного сообщения об ошибках или как предложение дополнительных услуг, например, бесплатной загрузки, которая якобы заставит компьютер пользователя работать быстрее.

Защита пользователей от всплывающих приложений, использующих социальную инженерию, состоит прежде всего в понимании ситуации. Блокировку всплывающих окон и автоматические загрузки можно обойти.

Гораздо правильнее убедить пользователей в том, что они не должны нажимать ссылки на всплывающих окнах, не посоветовавшись с персоналом поддержки. Однако при этом сотрудники должны быть уверены в том, что специалисты поддержки не будут легкомысленно относиться к просьбам о помощи, если пользователь просматривает Internet. Эти доверительные отношения можно предусмотреть в вашей политике безопасности по работе в Internet.

**Мгновенная передача сообщений**

Мгновенная передача сообщений (Instant Messaging, IM) — относительно новое средство коммуникации. Непосредственность и дружелюбный интерфейс IM-систем делают его идеальным средством для нападений, использующих социальную инженерию, ведь пользователи расценивают данную службу как телефон и не связывают ее с потенциальными угрозами ПО. Основные атаки, использующие IM, это гиперссылки на вредоносное ПО и его рассылка.

Злоумышленник (на рис. 4 он выделен красным цветом) исполняет роль известного пользователя и посылает электронную почту или 1М-сообщение, исходя из того, что получатели примут их за сообщения от кого-то, кого они знают. Большинство IM-средств доступа допускает идентификацию пользователей, основанную на адресе электронной почты, что дает возможность хакеру послать приглашения контакта IM другим людям в организации.

Нужно включить IM-безопасность в политику безопасности. Для этого необходимо установить следующие пять правил:

• выбрать единственную IM-платформу и утвердить ее в качестве стандарта;

• определить параметры настройки безопасности развертывания;

• рекомендовать пользователю не использовать настройки по умолчанию;

• установить стандарты пароля;

• обеспечить руководство по использованию.

**Угрозы при использовании телефонной связи**

Телефон предполагает уникальный способ нападения. В настоящее время взлом телефонной связи по IP-протоколу (Voice over IP, VoIP) является главной угрозой. VoIP-имитация становится таким же широко распространенным явлением, как электронная почта и 1М-имитация.

Есть три главных типа атак, направленных на офисные АТС, во время которых:

• просят информацию, обычно имитируя законного пользователя, чтобы обратиться к телефонной системе непосредственно или получить удаленный доступ к компьютерным системам;

• получают доступ к «свободному» использованию телефона;

• получают доступ к системе коммуникаций.

Эти методики получили название фрикинга (phreaking). Самый обычный прием хакера — имитация роли телефонного инженера (см. рис. 5).

Запросы об информации или доступе по телефону — малорискованная форма нападения. Если адресат начинает что-то подозревать или отказывается исполнять запрос, хакер может просто положить трубку. Но такие нападения более сложны, чем атака хакера, просто звонящего в компанию и интересующегося пользовательским идентификатором и паролем. Обычно используется сценарий, когда просят или предлагают справку прежде, чем почти машинально происходит запрос о личной или деловой информации.

Внутренняя телефонная система организации — самая важная часть защиты, которую вы должны оговорить в политике безопасности.

**Служба поддержки**

Иногда энтузиазм сотрудников технической поддержки заставляет их забыть о необходимости выполнять процедуру безопасности. Если же службе поддержки предписывают строгие стандарты безопасности, требуя проверки правомерности запроса пользователя, то появляются помехи в работе. Персонал, чувствующий, что ИТ-отдел не обеспечивает их немедленным обслуживанием, склонен жаловаться и доказывать, что их запросы важнее, чем вопросы безопасности.

Служба поддержки должна балансировать между безопасностью и деловой эффективностью, а политика и процедуры безопасности должны способствовать этому. Требование аутентификации обратившегося за помощью не является избыточным, поскольку каждый сотрудник знает свои данные. Но это не дает гарантии безопасности, потому что хакер также может их знать. Труднее защитить аналитика службы поддержки против внутреннего взлома. У внутреннего хакера больше исходных данных для имитации легитимного обращения. Процедуры защиты должны обеспечить двойную роль в этой ситуации:

• аналитик службы поддержки должен иметь гарантии аудита всех действий, сервисная служба должна вести журнал всех действий так, чтобы быстро исправить или ограничить любой ущерб в случае атаки.

• аналитик службы поддержки должен иметь структурированную процедуру обработки запросов пользователей.

Аудит всех процедур — самый ценный инструмент в предотвращении инцидента и последующем его расследовании.

**Анализ мусора**

Мусор — источник информации для хакеров. Деловые бумажные отходы неоценимы для тех, кто использует социальную инженерию.

Плохо, когда в компании нет правил управления отходами включая цифровые носители информации, (на этих отходах можно найти все виды данных). В этом случае политика безопасности компании должна содержать положение об управлении их жизненным циклом, в том числе процедуры разрушения или стирания.

Ваши сотрудники должны понимать: выбрасывание носителя в корзину для отходов не есть его уничтожение. Анализ мусора нельзя считать правонарушением, поэтому вы должны быть уверены, что персонал знает, как выбрасывать ненужные материалы. Необходимо разработать процедуры уничтожения мусора и разместить отходы внутри защищаемого периметра, чтобы они были недоступны.

Политика безопасности часто не принимает во внимание эту проблему, поскольку предполагается, как правило, что любой, кто получает доступ к ресурсам компании, должен заслуживать доверия.

Одна из самых эффективных мер при работе с мусором — классификация данных. Вы назначаете различные категории информации и определяете, как персонал должен с ними обращаться.

**Личностные подходы**

Для хакера самый простой путь получения информации — попросить об этом непосредственно. Такой прием может показаться грубым, но это основа мошенничества. В руководстве Microsoft [1] особо выделяется четыре его разновидности:

• Запугивание. Обычно используется имитация полномочий, чтобы принудить адресата исполнить запрос.

• Убеждение. Как правило, при этом используется лесть.

• Использование доверительных отношений. Этот подход требует длительного периода вхождения в доверие к адресату.

• Помощь. Хакер предлагает адресату помощь, в рамках которой необходимо обнародовать личную информацию.

Нападения путем предложения «помощи» могут быть минимизированы, если вы имеете эффективную службу сервисной поддержки. Обращения к неформальному помощнику — часто результат потери доверия к ее услугам. Для предотвращения таких атак необходимо:

• определить в вашей политике безопасности, что служба поддержки — единственное место, куда нужно сообщать о проблемах;

• гарантировать, что служба поддержки имеет стандартизованный процесс реагирования в пределах установленного уровня обслуживания;

• проверять выполнение сервисных работ регулярно, чтобы удостовериться, что пользователи получают ИТ-услуги адекватного уровня.

Нельзя недооценивать важность службы поддержки в обеспечении защиты первого уровня против нападений социальной инженерии.

Услуги ИТ должны отвечать следующим правилам:

• каждое действие технической поддержки должно быть запланировано;

• подрядчики и внутренний персонал, которые осуществляют локальное обслуживание или инсталляцию, должны иметь документы, идентифицирующие личность;

• при проведении работ пользователь должен перезвонить в отдел поддержки, чтобы сообщить время прибытия инженера поддержки и время его ухода.

• каждая работа должна иметь наряд, подписываемый пользователем.

• пользователь никогда не должен обращаться к информации или регистрации на компьютере, чтобы обеспечить доступ инженера (если инженер не имеет достаточных прав доступа, чтобы завершить задачу, он должен войти в контакт с сервисной службой).

**Защита помещений**

Подавляющее число больших компаний используют инфраструктуры защиты помещений. Компании среднего размера могут быть менее осведомлены о правилах контроля посетителей. Ситуация, в которой посторонний человек следует за кем-то, проходя в офис, является очень простым примером нападения с использованием социальной инженерии. Этот прием нельзя осуществить в большой компании, где каждый человек должен использовать электронный пропуск для прохода через турникет, или в маленькой компании, где каждый знает каждого. Однако это очень просто осуществить в компании с тысячей служащих, которые практически не знают друг друга.

Компания должна организовать вход таким образом, чтобы посетители проходили непосредственно мимо охранника, предъявляя свои пропуска или регистрируясь. Недопустимо скопление посетителей перед охранником, которое может затруднить его работу.

**Реверсивная социальная инженерия**

Реверсивная социальная инженерия описывает ситуацию, в которой адресат из числа персонала предлагает хакеру информацию, которую он хочет продать. Такой сценарий осуществляется все чаще. Защита от реверсивной социальной разработки — самая трудная задача.

**Список литературы**

1. How to Protect Insiders from Social Engineering Threats. Midsize Business Security Guidance. Microsoft, 2006. www.microsqft.com

2. APWG Phishing Trends Activity Report for December 2006, http://www.antiphishing.org/reports/ap wg\_ report\_december\_2006.pdf

3. Symantec Internet Security Threat Report. Trends for January 06-June 06. Volume X, Published September 2006. www.symantec.com

4. Secure Computing SecureNews September 2006, http:// www. securecomputing. com/pdf/ SecureNewsSeptember2006.pdf

5. Zulfikar Ramzan. Drive-By Pharming: How Clicking on a Link Can Cost You Dearly, www.symantec.com

Журнал «Директор информационной службы», март 2007