АНАЛИЗ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК: ПОСТАНОВКА ПРОБЛЕМЫ

А. Н. Фролова[1], А. Е. Пащенко[2], Т. В. Тулупьева[3], А. Л. Тулупьев[4]

[1,2,3,4]Санкт-Петербургский институт информатики и автоматизации РАН

[1,2,3,4]СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

[1]<just_4_fan@mail.ru>, [2]<aep@iias.spb.su>, [3]<tvt@iias.spb.su>, [4]<alt@iias.spb.su>

<http://tulupyev.spb.ru>

УДК 004.056.5 + 159.9 + 35.083.8

Фролова А. Н., Пащенко А. Е., Тулупьева Т. В., Тулупьев А. Л. **Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы** // Труды СПИИРАН. Вып. 6. — СПб.: Наука, 2008.

Аннотация. *В статье показана актуальность проблемы, представлена классификация социоинженерных атак, предложен возможный подход к оцениванию индекса защищенности информационной системы с точки зрения человеческого фактора, представляющий собой адаптацию методов, применяемых при анализе защищенности программно-аппаратного обеспечения компьютерных сетей.* — Библ. 9 назв.

UDC 004.056.5 + 159.9 + 35.083.8

Frolova A. N., Paschenko A. E., Tulupyeva T. V, Tulupyev A. L. **An Analysis of information systems Security in the Context of Socio-engineering Attacks: Position Statement** // SPIIRAS Proceedings. Issue 6. — SPb.: Nauka, 2008.

Abstract. *The paper states the problem of social engineering attacks, outlines their classification, presents a possible approach to estimation of an index of security of System from the point of view of the human factor. The suggested approach is based on adaptation of the methods applied to the analysis of security of hardware-software complex of computer networks.* — Bibl. 9 items.

1. Введение

Потребность в безопасности является одной из основных потребностей человека [8]. Люди охраняют свою собственную жизнь, а также оберегают свое жилище, имущество, деньги и прочие материальные ценности. Учитывая высокий уровень информатизации современного общества, проблема обеспечения информационной безопасности становится все более актуальной. Статистика преступлений в данной области продолжает неуклонно расти, несмотря на разработку и внедрение новейших технологий защиты информации [4]. Специалисты научились бороться со злоумышленниками, которые атакуют информационные системы извне, то есть применяющими хакерские методы. Но данные методы защиты информации оказываются совершенно неэффективными, если угроза безопасности находится внутри самой информационной системы и исходит от сотрудников, которые пользуются ресурсами данной системы. При реализации такой угрозы принято говорить о «человеческом факторе», которым умело пользуются преступники нового поколения, так называемые *социоинженеры*. Согласно [1], четверть внешних угроз информационной безопасности, по мнению респондентов, составляют приемы социальной инженерии. Полагая указанную долю угроз весьма существенной, в данной статье авторы концентрируются на безопасности информационной системы лишь в аспекте человеческого фактора. В Российской Федерации в силу сложившихся традиций

данному аспекту безопасности уделяется слишком мало внимания. Этому способствует, в частности, уверенность ряда ответственных за безопасность сотрудников, что любая утечка информации вызвана лишь несовершенством технической составляющей системы безопасности. Актуальность данной проблемы обусловлена еще и тем, что российские компании выходят на международный рынок, а это значит, что им придется столкнуться с теми проблемами, которые существуют в мировом масштабе; при этом необходимо обратить внимание на них сейчас, а не после понесенных убытков. Ключевыми проблемами, ведущими к «выпадению» человеческого фактора из анализа системы угроз, является как отсутствие методов обоснованной оценки самих угроз, так и отсутствие эффективных методов борьбы с ними. Цель данной статьи — показать, что одним из подходов, обеспечивающих анализ защищенности информационных систем от социоинженерных атак, может стать адаптация хорошо разработанных методов, используемых в смежных областях знания.

2. Определение социоинженерных атак

Считается, что термин «социальная инженерия» («social engineering») был введен впервые в 1922 году Р. Паундом в его работе «Введение в философию права» [3]. Понятие применялось для обозначения комплекса специфических знаний, которые позволяют управлять процессами создания, модернизации и воспроизведения некой искусственно созданной реальности. В отечественной литературе термин появляется в начале 1970-х годов в работах по критике западной социологии и социальной психологии. Однако в публикациях отечественных исследователей чаще используется аналогичный по смыслу термин «социоинженерная деятельность» [3].

Современное понимание термина «социальная инженерия» состоит в том, что он представляет набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации или для создания условий, при которых, используя халатное отношение пользователей публичной или корпоративной сети к политикам безопасности, последними нарушаются устоявшиеся правила и политики в области информационной безопасности [1]. Действия социального инженера называется социоинженерной атакой.

Злоумышленник использует особые методы обмана и маскировки, провоцирующие жертву-сотрудника, который обладает определенными полномочиями, на разглашение служебной информации или на действия, которые помогут злоумышленнику в достижении его цели. Как правило, целью социоинженера является получение доступа к компьютерным системам и сетям предприятия с последующим доступом к конфиденциальным данным [2].

3. Классификация сценариев социоинженерных атак

Принято разделять приемы прямой социальной инженерии (ПСИ) и приемы обратной социальной инженерии (ОСИ).

Прямая социальная инженерия предполагает выход злоумышленника непосредственно на интересующую его или его заказчика организацию и последующее проведение социоинженерной атаки. Для успешной атаки тщательно изучается круг лиц, имеющих доступ к интересующей злоумышленников ин-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

формации. Затем применяются уже известные и отработанные социо-инженерные приемы [1].

Второй прием принято называть обратной социальной инженерией (reverse social engineering). Основное отличие данного метода — это создание ситуации, при которой жертва, сталкиваясь с проблемой, сама просит помощи социо-инженера [2]. Этому, как правило, предшествует мелкая диверсия, в ходе которой хакер-инженер инициирует неполадку в работе компьютера, подключенного к сети. План атаки должен быть достаточно точным, поскольку, с одной стороны, вызываемые затруднения должны представляться пользователю безнадежными с точки зрения устранения их своими силами, а с другой, он не должен рассказать о случившемся коллегам и ответственным лицам, а должен попытаться устранить проблему сам. Для решения проблемы пользователь должен обратиться к социоинженеру, который будет находиться в списке ICQ контактов, либо к «хорошему знакомому» кого-то из сотрудников, либо в «центр компьютерной скорой помощи». Главное, чтобы решение проблемы было быстрым, дешевым и, казалось, безопасным. Атакующий, который может заставить жертву позвонить ему, будет располагать высоким уровнем доверия с ее стороны: «если я позвоню кому-нибудь, кто, как мне кажется, из технической поддержки, то я не буду просить его подтвердить свою личность» [2].

4. Обзор основных методов и приемов социальной инженерии

Самый верный, но отнюдь не самый простой прием — выяснение пароля либо возможность создания административной учетной записи. Как правило, в организациях, уделяющих достаточное внимание просвещению своих сотрудников в области информационной безопасности, вероятность реализации этого способа атаки довольно низка [1].

Однако наиболее популярными среди социоинженеров способами работы с легальными пользователями сетей являются разные формы «фишинга» (от английского «fishing» — рыбалка). С помощью фишинга — рассылки сообщений, вызывающих полное доверие пользователей сети, выполняется загрузка и запуск вредоносного программного обеспечения (malicious software или malware). Как правило, это — «троянские» программы и вирусы. Они содержат код, который приводит к невозможности пользоваться как отдельными файлами, так и системой в целом или создается для получения доступа к информации с данного компьютера и сети, к которой он подключен. Данные программы инсталлируются на персональный компьютер в ходе посещения различных страниц в Интернете или, например, открытия приложения, прикрепленного к вполне безобидному с виду «письму друга», присланному на электронную почту (метод silent install) [5].

Запуск программ-шпионов (spyware), троянов, обманная подтасовка псевдоссылок на сайты-обладатели брендового имени (brand hijackers), перехват информации (pharming) и другие действия активно используются социо-инженерами. При этом формы, задачи и масштабы такой деятельности могут быть абсолютно разными — от продажи данных статистики посещения рекламных сайтов (маркетинговая информация, отражающая спрос на товары) до мощной конкурентной разведки с последующей реализацией стратегического плана по усилению или ослаблению конкурентных преимуществ различных участников рынка [1].

5. Предлагаемый подход к анализу защищенности информационной системы от социоинженерных атак

Перед представлением подхода необходимо дать первичное описание модели, в рамках которой мы находимся и действуем. Рассмотрим цепочку *социоинженер – сотрудник – руководство – информация*. Если планируется социоинженерная атака на коммерческую организацию, то первым звеном цепочки является атакующая сторона или в данном случае социоинженер, который хочет получить информацию конфиденциального характера. Сотрудник (жертва атакующей стороны) является «проводником», через который социоинженер может получить нужную ему информацию. Руководство компании является хранителем информации и стороной, которая заинтересована в сохранении конфиденциальной информации. И наконец, информация — это то, что социоинженер стремится получить.

Мы предлагаем рассмотреть подход к анализу защищенности информационной системы от социоинженерных атак, который будет являться адаптацией модели автоматизированного анализа защищенности программно-аппаратного комплекса информационной системы, предложенной М. В. Степашкиным в его диссертационной работе [7]. Для анализа защищенности система формирует модель сети на основе графов, где вершинами являются локальные компьютеры, а связи между вершинами соответствуют связям между компьютерами. После этого для каждого компьютера описывается его конфигурация, включающая сведения о версии установленной операционной системы, а также о других программных продуктах и их настройках. Из существующих публичных баз данных уязвимостей, насчитывающих сотни тысяч элементов, извлекаются для тестирования в данной конкретной информационной системе те уязвимости, которые в ней возможны. После этого производится анализ, какие действия или цепочки действий могут привести к успешной атаке злоумышленников, то есть к получению ими доступа к какой-либо части информации в системе. После анализа защищенности предпринимаются действия, которые позволят предотвратить какое-то число атак на систему.

Подобная модель может быть использована и в рамках изучения социоинженерных атак. Остаются применимыми алгоритмы, на которых основан анализ защищенности, изменения должны коснуться баз данных уязвимостей, а также модели структуры информационной системы. Вместо базы данных возможных атак на некую программно-аппаратную составляющую информационной системы может быть составлена база данных возможных социоинженерных атак, а вместо базы данных уязвимостей программно-аппаратных компонентов — база данных уязвимостей сотрудников. Безусловно, в некоторой степени такие базы данных уже разработаны социоинженерами, ведь, совершая атаку, они используют знания о психологических уязвимостях жертвы и составляют наиболее эффективные сценарии атакующих действий для конкретного сотрудника, обладающего данными уязвимостями.

Самым сложным этапом реализации данного подхода является составление базы данных уязвимостей индивидов. Такие уязвимости сильнейшим образом связаны с их потребностями. Именно потребности мотивируют человека совершать те или иные действия.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Потребности давно изучаются в психологии, разработаны несколько классификаций [8], и эти знания могут быть использованы для составления базы данных по уязвимостям сотрудников. Существует множество различных теорий потребностей человека, но наиболее распространенной, широко используемой и применимой к данному случаю является пирамида потребностей по А. Маслоу [9]. А. Маслоу выделил пять иерархических уровней потребностей:

1) Физиологические потребности (потребности в воде, пище, сексуальные потребности и т. п.);
2) Потребности в безопасности и уверенности в будущем (потребности в физической и социальной безопасности, защите, стабильности);
3) Социальные потребности (потребности в общении, любви, принадлежность к группе и т. п.);
4) Потребности в уважении и признании (потребности в оценке другими, в престиже, уважении, признании профессиональной компетентности, привлекательности и т. п.);
5) Потребности в самовыражении и саморазвитии.

Иерархия потребностей позволяет понять, что уровни актуальных потребностей сотрудников могут различаться. Знание иерархии потребностей помогает социоинженеру в первую очередь определить, какой уровень иерархии является для данного сотрудника наиболее актуальным, а значит, какой способ воздействия, мотивации для него можно выбрать. Данная концепция помогает воздействующему агенту определить последовательность воздействия на сотрудника, учитывать не только физиологические потребности, но и потребности более высоких уровней. Для какого-то сотрудника необходимо и достаточно материального мотивирования, а кому-то необходимо ощущать свою важность и получать нужные ему знаки внимания. Более того, данная теория подчеркивает динамичность потребностей и объясняет, что нельзя рассчитывать, что мотивация, которая сработала один раз, будет эффективно работать все время.

После того как определено, какого рода информация должна содержаться в базе данных уязвимостей сотрудников, для успешного анализа защищенности необходимо предложить способы ее сбора. При этом главными условиями при выборе этих способов должны служить критерии полноты и достоверности получаемых при их использовании сведений; также данные методы сбора должны быть в определенной степени универсальными для сбора информации о всех сотрудниках.

Первый и самый очевидный способ — это спросить самого человека о его потребностях. Но зачастую человек сам не осознает свои реальные потребности и уж точно не готов делиться такой личной информацией с руководством компании. В данном случае процесс сбора информации, а также выявление взаимосвязей является очень дорогостоящим и априорно субъективным. Кроме того, необходимо каким-то образом автоматизировать процесс сбора данных.

В качестве возможной альтернативы непосредственному опросу предлагается использовать программные приложения для скрытого тестирования, например в виде игры. Одним из ее этапов может стать определение материальной потребности сотрудника, где ему будет предложено в какой-то ситуации принять решение, которое позволит судить о том, насколько уязвим человек в такой потребности, как например «деньги». Следует также отметить, что искажения, которые может внести игровая ситуация, не являются непреодолимыми: они элиминируются, если человек окажется в надлежащим образом подготовленной игровой обстановке. Возможно внедрение и других программных сис-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

тем, главное, чтобы они позволяли либо в автоматическом режиме, либо без затрат существенных сил и средств осуществить сбор данных о выраженности различных потребностей всех сотрудников.

В результате анализа собранной информации логично разделить сотрудников на несколько групп. Деление может производиться на основе степени выраженности отдельных потребностей, или распределение по группам будет осуществляться с учетом сочетания степени выраженности сразу нескольких потребностей. Основываясь на информации о количественном и качественном составе групп, можно разрабатывать инструкции по политике безопасности для каждой конкретной группы людей, а также проводить специально адаптированные тренинги, в которых бы были правильно расставлены акценты по стилю преподнесения и характеру предоставляемой информации.

Комплекс представленных мер будет способствовать снижению числа успешных социоинженерных атак. Следует отметить, что нельзя рассчитывать на то, что, проведя одноразовое обучение и объяснив, какие последствия может повлечь за собой то или иной действие, мы раз и навсегда решим данную проблему. Через какое-то время внутренние психологические установки человека ослабевают, что влечет за собой изменение отношения к ограничениям, ряд из которых становится выполнять необязательно, а также ведет к неисполнению различного рода инструкций. При этом, как правило, сотрудники не в состоянии оценить масштаб возможного вреда, что приводит к негативным последствиям [6]. Из вышесказанного следует, что профилактическая работа — не одноразовая интервенция, а постоянный и сложный процесс, требующий мониторинга.

Предлагаемый нами подход к анализу защищенности информационной системы, включающий в себя анализ возможных уязвимостей сотрудников, а также предлагающий действия для уменьшения вероятности осуществления успешных атак социоинженеров, может послужить основой для введения системы индексов защищенности информационных комплексов с точки зрения человеческого фактора. Данная система будет базироваться на разработанной классификации:

а) виды возможных атак, угроз, целей, объектов, субъектов;
б) причины и мотивации, по которым персонал не смог противодействовать атакам;
в) виды приемов обнаружения и пресечения социоинженерных атак;
г) виды приемов предотвращения (профилактики) атак, включая совершенствование инструкций по безопасности (где главный упор следует делать на простоту и понятность) и разработку перечня необходимых тренингов, направленных на разъяснение возможных угроз и способов противодействия им.

После создания данной классификации станет возможна обоснованная оценка вклада различных аспектов «человеческого фактора» в итоговую оценку, характеризующую защищенность системы.

6. Заключение

В данной статье была показана актуальность проблемы защиты информационных систем от социоинженерных атак, дано определение, описаны основные направления социоинженерной деятельности, возможные сценарии нападения, приведены примеры используемых приемов и методов, а также предложен возможный подход для построения индекса защищенности системы с точки

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

зрения человеческого фактора. Выработанная концепция родственна уже разработанному подходу к анализу защищенности программно-аппаратного комплекса информационных систем, основными задачами является адаптация и формирование баз данных возможных социоинженерных атак и уязвимостей сотрудников.

Литература

1. *Бычек В., Ершова Е.* Социальная инженерия в интеллектуальной битве «добра» и «зла» [Электронный ресурс] / Защита информации. Инсайд, 2006. №6. // <http://www.aladdin.ru/press-center/publications/publication11475.php> (по состоянию на 04.02.2008).
2. *Митник К. Д., Саймон В. Л.* Искусство обмана. М.: Компания АйТи, 2004. 360 с.
3. *Резник Ю. М.* Социальная инженерия: Предметная область и границы применения // Социс, 1994. №2.
4. *Орлов С.* Щит и меч для корпоративных клиентов [Электронный ресурс] / LAN. 2005. №3 // <http://www.osp.ru/lan/2005/03/140240/> (по состоянию на 04.02.2008).
5. «Банда неуловимых» хакеров из России стала головной болью для служб безопасности мировых банков [Электронный ресурс] // NEWSru.com 15.03.2007 <http://www.newsru.com/world/15mar2007/banda.html> (по состоянию на 04.02.2008).
6. Актуальность проблем обеспечения внутренней информационной безопасности [Электронный ресурс] // Kommersant.ru 23.10.2006 <http://www.aferizm.ru/bb/it/bb_it_aktyalno_infbez.htm> (по состоянию на 04.02.2008).
7. *Степашкин М. В.* Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак : Дис… канд. техн. наук: СПб.: СПИИРАН, 2002. С. 196.
8. *Хьелл Л., Зиглер Д.* Теории личности (Основные положения, исследования и применение). СПб.: Питер Пресс, 1997.
9. *Молл Е. Г.* Менеджмент: организационное поведение. М.: Финансы и статистика, 2000. 160 с.