Дьяченко Алексей, 016 группа

Социальная инженерия

При создании системы безопасности (СБ) предприятия необходим комплексный подход. Объектом защиты должна быть вся система обработки информации. На этапе технического проектирования системы защиты должна быть произведена классификация информации, проанализирована ее ценность и на основе этого определена разумная степень защиты для каждого класса информации. Выработанная таким образом политика безопасности должна учитывать законодательные, организационные, технологические и технические меры защиты, то есть представлять собой последовательное изложение целей, задач, принципов и способов защиты Информационной Системы. В RFC 2196 приводится определение: "Политика безопасности – это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации". При реализации ПБ выделяется техническая часть и организационная (именно она описана в RFC). Значение четких правил недооценивают, хотя они являются самой дешевой частью СБ. Кроме того, без них использование программно-аппаратных средств защиты просто бессмысленно. Наличие надежных технических средств и правильный выбор режима их использования еще не гарантируют владельцу защищенность его информационной системы. Немаловажную роль играет правильность их использования. Поскольку даже самые стойкие шифры при неправильном их использовании существенно теряют качества, то конфиденциальность передаваемой информации во многом зависит от того, какие ошибки допускает ее владелец при использовании криптографической защиты. А то, что все пользователи допускают ошибки – неизбежно и является непреложным и важным фактом. Человек – неотъемлемая часть любой СБ, поэтому необходимо учитывать атаки, направленные на него.

Социальной инженерией (СИ) принято называть атаки на систему безопасности, объектом которых является человек. Классическим примером – звонок по телефону с целью получить пароль. Но чаще всего под этим термином подразумевают любые способы психологического воздействия на людей для введения их в заблуждение. Это основная часть атак СИ, включающая в себя множество различных тактик, нагнетание напряжения, выдача за другое лицо, отвлечение внимания. Современный человек склонен к сотрудничеству, готов ответить скорее "да", чем "нет", обычно не отказывает в просьбе о мелкой помощи и заводит разговор с посторонним. Грамотно сыграв на чувствах, злоумышленник заставляет людей делать то, что ему нужно. Чаще всего злоумышленники используют страх, любопытство, жадность, превосходство, великодушие и жалость.

Страх. Самый распространненый психокомплекс человека. Большинство, не задумываясь, выполняют то, что от них требуют, услышав слова "начальник", "шеф" или "директор". Боязнь потерять работу, показаться невежливым, некомпетентным используется злоумышленниками в своих целях.

Любопытство. Заполняя регистрационные формы, чтобы посмотреть "самое, самое …", объект атаки и не подозревает, что они были созданы специально, что бы он ввел

свои данные. Так как часто пользователь не утруждает себя запоминанием различных паролей, то, получив от него пароль, злоумышленник получает доступ ко всем его аккаунтам.

Жадность. Пример отличной СИ на почве жадности описан в книге Сидни Шелдона "Интриганка". Мошенница зашла в ювелирный магазин и, представившись женой расточительного миллиардера, приобрела первый попавшийся крупный бриллиант за $150.000. Через пару дней она вернулась, восхищенная покупкой, и поинтересовалась, нет ли еще одного, столь же крупного камня. Когда продавец объяснил, что продал ей очень редкий бриллиант и будет трудно отыскать подобный, аферистка заверила, что она готова заплатить $500.000, если только найдется еще один такой же. После долгих и безрезультатных поисков, продавец отчаялся, но тут по объявлению позвонила безутешная вдова, у которой – о чудо – оказался очень похожая драгоценность. "После смерти Джона у меня остались долги на сумму $300.000, а еще вот этот бабушкин бриллиант. Я согласна его продать, но только за $300.000. Мне нужны деньги, чтобы погасить долг". Прикинув, что все равно выигрывает 200 тысяч, ювелир купил камень. Стоит ли говорить, что это был тот же самый бриллиант, который он продал парой недель ранее и мошенницу он больше не видел.

Превосходство. Конечно, никто не кидается на банальное "слабо" демонстрировать свою компетенцию. Но в горячке спора на профессиональную тему, желая "пустить пыль" в глаза собеседнику или просто хвастая собственной осведомленностью, сотрудник может сообщить злоумышленнику важные сведения.

Великодушие и жалость. Здесь злоумышленник дает жертве почувствовать свою значимость, обращается за помощью. Когда к сотруднику обращается красивая девушка и, протягивая дискету, спрашивает, как распечатать файл, то в 9 случаев из 10 он вставит эту дискету в компьютер и получит целый "букет" троянов, которые, активизируясь, начинают красть пароли, финансовые отчеты и другую конфиденциальную информацию.

Это не исчерпывает список чувств, на которых может сыграть социальный инженер. Радость и гнев, зависть и подозрительность, обычная лень – все может быть использовано мошенниками.

Для атак с помощью СИ не требуется специальных технических средств и знаний. Для связи с жертвой злоумышленники пользуются телефоном, электронной почтой, общением через Интернет в реальном времени или встречей в реальной жизни. Чаще всего используется телефон, так как он позволяет, сохраняя анонимность, поддерживать с собеседником постоянный контакт. Непосредственный контакт не оставляет жертве времени обдумать ситуацию, решение приходится принимать мгновенно, под натиском гнущего свою линию злоумышленника. Разговор по Интернету в "реальном" времени дает злоумышленнику другие возможности воздействия на жертву. Множество авантюр совершается через ICQ. Разговорив собеседника, мошенник узнает о структуре организации, именах и прозвищах сотрудников, принятых мерах для обеспечения безопасности. Полученные сведения используются потом при телефонных звонках, чтобы сойти "за своего".

Для получения необходимой информации злоумышленнику часто достаточно просто пройтись по офису атакуемой фирмы. Представившись журналистом или смешавшись с группой сотрудников в "час пик", злоумышленник попадает в здание, где может записать вирус в оставленный включенным компьютер, посмотреть написанные "для памяти" на бумажках пароли. Полезную информацию злоумышленник способен получить

из мусорных корзин. Старые телефонные книги содержат данные о структуре организации, об именах и телефонах сотрудников, записки данные о текущем положении дел в компании, помогают завоевать доверие. Инструкции и документы показывают уровень системы безопасности компании, ее сильные и слабые стороны. Информация на вышедших из строя и отремонтированных жестких дисках помогает при атаках на существующую систему.

Обратной социальной инженерией (ОСИ) называется ситуация когда СИ применяется "наоборот". Объект атаки, попав в заранее подготовленную ловушку, обращается за помощью к злоумышленнику. Хакер полностью контролирует ситуацию, ему не нужно завоевывать доверие пользователя, жертва сама расскажет ему все необходимое. Предупрежденный и подготовленный к атакам СИ пользователь беззащитен перед обратной СИ.

Атака с помощью ОСИ состоит из трех частей:

1. Диверсия. Готовится ловушка для пользователя. В систему вносятся мелкие неполадки, легко устранимые, но сразу бросающиеся в глаза. Например, меняется цвет фона.
2. Реклама. Жертве сообщается, что злоумышленник может решить проблему. Например, заменяется телефон службы техподдержки.
3. Помощь. Общение с пользователем, в ходе которого стороны решают проблемы друг друга. Хакер помогает пользователю, а пользователь – хакеру.

Атаки ОСИ требуют большой предварительной подготовки, которая не всегда может быть проведена, но в случае успеха злоумышленник получает больше ценной информации от сотрудников.

Кроме атак с помощью СИ человека можно запутать, отвлечь внимание. Это называется Human Denial of Service, дословно – человеческий отказ в обслуживании. Например, посылая мусор на 80 порт, сконцентрировать внимание администратора на этой атаке, проводя параллельно атаку настоящую атаку на систему. Шаблоны и стереотипы, вбитые в голову сотрудникам системы безопасности, тоже относятся к HDoS.

Типовой защиты от СИ не существует и не может существовать. Среди злоумышленников попадаются талантливые люди, не уступающие "великому комбинатору" Остапу Бендеру. Самые лучшие технические механизмы не могут защитить от такой атаки. Любые технические средства, какими бы прозрачными и удобными они ни были, всегда мешают пользователям в работе, а различные тонкости известны, как правило, лишь специалистам и непонятны пользователям этих средств. Снизить вероятность успеха атак с использованием СИ может правильно построенная политика безопасности. ПБ отвечает на два вопроса: "Что защищать?" и "От кого защищать?".

Обычно все угрозы делятся на внутренние и внешние. Против внешних угроз используются технические средства (фаерволы, антивирусы, системы обнаружения вторжения, почтовые фильтры). Эксплуатация этих средств входит в задачи IT отдела. Против внутренних угроз используются организационные средства, составление которых находится в компетенции руководства. При составлении таких правил необходимо:

1. Определить потери от несанкционированного доступа к информации, определить информацию, доступ к которой должен быть ограничен.

2. Учесть требования существующих стандартов при работе с защищаемыми данными.
3. Создавать защиту адекватную угрозе. Слишком много защиты так же плохо, как и слишком мало. Использование излишних систем защиты неоправданно затруднит работу и приведет к потерям.
4. Привлекать сотрудников к разработке правил. Никому не нравятся требования "спущенные" сверху.
5. Проводить тренировки. Это не только способ сообщить сотрудникам об изменениях в ПБ, но и узнать о работе существующей ПБ. На примерах, возникающих при эксплуатации, оценить недостатки используемой ПБ.
6. Документировать правила. Каждый сотрудник должен быть с ними ознакомлен и, как минимум, ежегодно обновлять свои знания. Любой новый работник обязан изучить правила и подтвердить, что с правилами ознакомлен.
7. Установить систему штрафов и неукоснительно ей следовать. Каждое наказание должно быть четко аргументированным и оправданным.
8. Постоянно обновлять ПБ с учетом современных технических средств. Мошенники используют неграмотность жертв в области безопасности. Защищать нужно не только пароли, но и другую критическую информацию об организации. Атаки СИ выявляют уязвимые места в ПБ, которые не могут быть обнаружены другими способами.

При использовании только организационных мер обеспечения информационной безопасности разрабатываются инструкции и предписания для перекладывания ответственности с людей, придумывающих такие документы, на конкретных исполнителей. Требования таких документов без соответствующего технического обеспечения затрудняют деятельность организации и, как правило, не выполняются. При практическом внедрении политики безопасности необходимо:

1. Создать отдел, обеспечивающий разработку правил работы с системой обработки информации, определяющий права сотрудников по доступу к ресурсам этой системы, осуществляющий административную поддержку технических средств защиты информации (настройка конфигурации, оперативное реагирование на поступающие сигналы о нарушениях, анализ зафиксированных нарушений);
2. Разработать технологию по выполнению политики безопасности рассматривающую порядок взаимодействия различных подразделений организации при ее выполнении.

Создавая отдел информационной безопасности, необходимо принять во внимание, что эксплуатация средств защиты требует небольшого количества сотрудников. Основные затраты происходят на этапе создания политики безопасности, когда необходимы знания квалифицированных специалистов, потребность в которых после ее внедрения отпадает. Кроме того, система безопасности должна разрабатываться в сжатые сроки, чтобы не отстать от развития системы обработки информации предприятия. Поэтом лучшим выходом является обращение к сторонним специалистам, имеющим опыт в проведении подобных работ.

Ссылки:

Составление ПБ:

http://www.computerworld.com/securitytopics/security/story/0,10801,85583,00.html?SKC=security-85583

Социальная инженерия:

http://www.securitylab.ru/30696.html
http://www.citforum.ru/security/articles/soc_eng/

Обратная социальная инженерия:

http://bukin-ms.viv.ru/cont/hacker/37.html

Организационные меры обеспечения защиты информации

http://www.infosec.ru/press/pub/p13.html