УДК 316

Ламинина Ольга Глебовна
кандидат философских наук, доцент, доцент кафедры
информационной аналитики и политических технологий
Московского государственного технического университета
им. Н.Э. Баумана
Olga.Laminina@gmail.com
Olga G. Laminina
candidate of philosophical sciences, associate professor, associate professor
information analytics and political technies
Moscow state technological university
of N. E. Bauman
Olga.Laminina@gmail.com

Возможности социальной инженерии в информационных технологиях

Possibilities of social engineering in information technologies

Аннотация: *Статья посвящена описанию возможностей методов социальной инженерии для манипулирования поведением как индивидуумов, так и групп населения ради получения доступа к конфиденциальной информации. Социальная инженерия использует знания психологии и человеческого фактора. Необходимо быть предельно осторожным, социальные хакеры знают наши слабые места очень хорошо.*

Ключевые слова*: социальная инжинерия, злоумышленник, информация, компьютерные атаки, фрикинг, информационные технологии****.***

Summary: *Article is devoted to the description of opportunities of methods of social engineering for a manipulation by behavior of both individuals, and national groups for the sake of receipt of access to confidential information. The social engineering uses knowledge of psychology and a human factor. It is necessary to be extremely careful, social hackers know our weak points very well.*

Keywords: *social engineering, malefactor, information, computer attacks, freaking, information technologies*

Социальная инженерия (СИ) — относительно молодая наука. Научное обоснование социальной инженерии впервые дал австрийский ученый К.Поппер, который в своих трудах "Нищета историцизма" и "Открытое общество" рассматривал данное направление "как совокупность подходов прикладной социологии, направленных на рациональное изменение социальных систем на основе фундаментальных знаний об обществе и предсказании возможных результатов преобразований.[1]

Социальная инженерия – это целенаправленная деятельность специально подготовленных людей по переустройству (преобразованию) социального мира.[2]

Люди так или иначе пользовались ее техниками испокон веков. Еще в Древней Греции и Риме были востребованы люди, способные ввести собеседника в заблуждение и убедить его в своей правоте. Выступая от имени верхов, такие люди вели дипломатические переговоры и нередко решали сложные проблемы, которые без их вмешательства привели бы к кровопролитию.

Наибольшее развитие социальная инженерия получила в послевоенные годы в США и Великобритании, прежде всего в контексте обеспечения реализации проектов американских и британских спецслужб, в рамках которых новое научное направление в социологии начало приобретать масштабный прикладной характер.[1] Целью социальной инженерии стала разработка технологий манипуляции сознанием людей.

В начале 70-х гг. начинается расцвет фрикинга. Фрикинг — набор технологий позволявший произвести взлом уличных телефонов, а далее с помощью методов СИ получить доступ к управлению телефонными сетями. К концу 70-х фрикеры настолько отработали техники манипулирования неподготовленными операторами, что могли без проблем узнать у них практически все, что хотели.

Самые искусные социальные инженеры всегда действовали экспромтом, полагаясь на своё чутье, благодаря наводящим вопросам, интонации голоса они могли определить комплексы и страхи человека и, мгновенно сориентировавшись, сыграть на них. Таким образом, к каждому находился свой индивидуальный подход.

С появлением компьютеров, многие фрикеры перебрались в компьютерные сети и стали хакерами. Навыки СИ в новой области стали еще полезнее, особенно после появления социальных сетей, и как следствие, возможность манипулировать не одним оператором, а огромными массами пользователей, побуждая их поступать по заранее разработанному сценарию.

И сегодня, когда владение информацией стало активно использоваться в коммерческих целях, важную роль в информационной безопасности играет человеческий фактор.

В данном контексте термин «социальная инженерия» — это использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации, т. е. это совокупность методов, основанных на психологических особенностях людей.

Целью социальной инженерии является побуждение людей совершать определенные действия, которые при обычных условиях они бы никогда не сделали, например, разглашение своей конфиденциальной информации, переходы на неизвестные сайты по сомнительным ссылкам. Вся система социальной инженерии базируется на том факте, что именно человек является самым слабым звеном любой системы информационной безопасности. Именно поэтому, когда злоумышленникам технически получить конфиденциальную

информацию трудно, они воздействуют непосредственно на самое слабое место в системе информационной безопасности — на пользователя.

Методы социальной инженерии способны обойти самые мощные системы информационной безопасности. К тому же использование социальной инженерии для несанкционированного получения информации очень выгодно, т.к.:

- это проще, чем взломать систему информационной безопасности;
- атаки нельзя вычислить с помощью технических средств защиты информации;
- это не требует больших вложений;
- представляет собой минимальный риск;
- работает для любой вычислительной платформы;
- имеет стопроцентный эффект.

Самыми распространенными методами атак являются:

1. Фишинг (англ. fishing — рыбная ловля, выуживание) — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — чаще всего к логинам и паролям, путем подлога сайтов или web страниц.

2. Кви про кво (от лат. Quid pro quo — «то за это»). Данный вид атаки подразумевает звонок злоумышленника в компанию по корпоративному телефону. В большинстве случаев злоумышленник представляется сотрудником технической поддержки, опрашивающим, есть ли какие-нибудь технические проблемы. Под видом их решения, мошенник прелагает сотруднику ввести определенный набор команд, которые в дальнейшем обеспечат удаленный доступ к локальной машине.

3. Троянский конь (или троян) — это вредоносный код, проникающий на компьютер жертвы под видом легального программного обеспечения. Чаще всего используется для сбора конфиденциальной информации, реже для ее разрушения или модификации, а также для нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях. Данная техника основана на любопытстве пользователей. Чаще всего злоумышленник отправляет жертве электронное сообщение, содержащее так называемый «вау!» контент или другую информацию, способную его заинтересовать. Открывая прикрепленный к письму файл, пользователь собственноручно устанавливает на свою машину вредоносное программное обеспечение.

4. Сбор информации из открытых источников. Применение техник социальной инженерии требует умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из социальных сетей, регистраторов доменных имен, баз данных операторов связи и тд.

5. Дорожное яблоко – этот метод атаки использует отчуждаемые носители. Злоумышленник подбрасывает зараженные носители (CD, USB флэш, флэш карты) в местах, часто посещаемых сотрудниками компании-жертвы.

Носитель подделывается под официальный, и сопровождается подписью, которая обязательно вызовет интерес.

6. Обратная социальная инженерия. Это метод, когда жертва, как ни парадоксально, сама сообщает злоумышленнику нужную ему информацию. Например, сотрудники службы технической поддержки никогда не будут спрашивать у пользователей логин или пароль, так как эта информация у них уже есть или она им не нужна. Однако, многие пользователи ради ускорения процесса добровольно сообщают эти сведения злоумышленнику, представившемуся сотрудником техподдержки, по телефону.

Для проведения своих атак, злоумышленники, применяющие техники социальной инженерии, зачастую эксплуатируют доверчивость, лень, любезность и даже энтузиазм пользователей и сотрудников организаций. Защититься от таких атак достаточно сложно, потому что жертвы могут и не подозревать, что их обманули. Злоумышленники, использующие методы социальной инженерии, преследуют, в общем, такие же цели, что и любые другие злоумышленники: им нужны деньги, информация или ИТ-ресурсы компании-жертвы. Для защиты от таких атак, необходимо изучить их разновидности, понять, что нужно злоумышленнику и оценить ущерб, который может быть причинен организации. Обладая всей этой информацией, можно интегрировать в политику безопасности необходимые меры защиты.

Различают два вида средств для защиты пользователей от методов СИ: административный и технический.

Административный. Сотрудники зачастую недооценивают значимость информации, которой владеют, и легко делятся ею с каждым, кто об этом попросит, не осознавая пагубные последствия своих действий. Но даже самые бдительные сотрудники не всегда могут распознать, что действует социальный инженер, и что они подвергаются атаке. Поэтому ключевым фактором успеха в защите информации является обучение.[3]

К технической защите можно отнести средства, не позволяющие:

- выяснение, передачу или несанкционированную смену паролей;
- несанкционированное создание учетных записей (с правами пользователя или администратора);
- запуск вредоносного программного обеспечения;
- несанкционированный удаленный доступ к корпоративной информационной системе;
- несанкционированное добавление дополнительных прав и возможностей зарегистрированным пользователям системы;
- передача или распространение конфиденциальной информации.

Основные правила для конечных пользователей:

- Следует обращать внимание на написание адресов сайтов;
- Если Вам предлагают пересмотреть сайт / фото / видео, зазывая эмоциональными призывами - не переходите сразу. Посчитайте до 10-ти и вспомните, что это возможно пример социальной инженерии;

- Вводя логин / пароль в аккаунтах на сайтах, обращайте внимание на необычные изменения внешнего вида страниц. Если что-то вызывает подозрение - лучше проверить оригинальность ресурса еще раз;
- Критически относитесь к электронным письмам, а особенно к ссылкам, по которым предлагают перейти незнакомые отправители сообщений.

Социальная инженерия использует знания психологии и человеческого фактора. Необходимо быть предельно осторожным, социальные хакеры знают наши слабые места очень хорошо.

Литература:

1. *https://antimaidan.ru/content/8201*
2. *http://www.e-xecutive.ru/management/practices/345004-sotsialnaya-inzheneriya*
3. *http://www.e-xecutive.ru/management/practices/854878-kremlevka-v-karmane-zachem-vam-kriptografiya*
4. *Сиротский А.А. Технологии социальной инженерии как потенциальная угроза в социальной сфере. В сборнике: Информационная безопасность бизнеса и общества Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский государственный социальный университет. Москва, 2016. С. 27-33.*
5. *Фомина Н.А. Использование методов социальной инженерии при мошенничестве в социальных сетях. Под редакцией Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. 2015. С. 443-453.*

Literature:

1. *https://antimaidan.ru/content/8201*
2. *http://www.e-xecutive.ru/management/practices/345004-sotsialnaya-inzheneriya*
3. *http://www.e-xecutive.ru/management/practices/854878-kremlevka-v-karmane-zachem-vam-kriptografiya*
4. *Sirotski A.A. Technologies of social engineering as potential hazard in the social sphere. In the collection: Information security of business and society Collection of the chosen articles of scientific and pedagogical structure of department of information systems, networks and safety. Russian state social university. Moscow, 2016. Page 27-33.*
5. *Fomina N. A. Use of methods of social engineering in case of a fraud on social networks. Under G. N. Chusavitina, E. V. Chernova, O. L. Kolobova's edition. 2015. Page 443-453.*