Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

УДК 316.62

Порошков

Максим Михайлович

МЕТОДЫ И ПРИНЦИПЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

АВТОРЕФЕРАТ

Диссертации на соискание степени магистра технических наук

по специальности 1-23 80 08 Психология труда, инженерная психология, эргономика

Заведующий кафедрой ИПиЭ
Константин Дмитриевич Яшин
кандидат технических наук, доцент

Научный руководитель
Денис Сергеевич Лихачев
кандидат технических наук, доцент

Нормоконтролер
Юлия Игоревна Кмита
магистр технических наук

Минск 2015

ВВЕДЕНИЕ

Социальная инженерия – термин, использующийся злоумышленниками для обозначения несанкционированного доступа к информации, не связанного со взломом программного обеспечения. Основная цель – обмануть людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы.

Популярность социальной инженерии среди злоумышленников растет потому, что нередко сами работники предприятия – люди являются самым слабым звеном в системе защиты.

Существует несколько распространенных техник и видов атак, которыми пользуются социальные инженеры. Все эти техники основаны на особенностях принятия людьми решений, известных как когнитивные предубеждения. Эти предрассудки используются в различных комбинациях, с целью создания наиболее подходящей стратегии обмана в каждом конкретном случае. Но общей чертой всех этих методов является введение в заблуждение, с целью заставить человека совершить какое-либо действие, которое не выгодно ему и необходимо социальному инженеру.

Социальная инженерия является важным аспектом в контексте предприятия в целом, так как системы защиты создают для злоумышленника довольно сложно преодолеваемый барьер, и в данном случае неважно, какого именно работника удалось злоумышленнику обмануть, так как результат – доступ ко всем внутренним ресурсам, минуя барьер защиты, будет одинаковым во всех случаях. Атаки социальной инженерии нередко ориентированы на работников, у которых есть самые большие права доступа к работе с конфиденциальной информацией, однако злоумышленник нередко оценивает и потенциальные знания цели. Одной из важных причин распространения социальной инженерии как метода атаки – это очень дешевый вид нападения, атакующий может не быть специалистом в сфере информационных технологий.

Согласно мировой статистике, количество хакерских атак использующих методы социальной инженерии неуклонно растет. Поэтому для повышения эфективности защиты от них, необходимо учитывать наиболее распространенные виды мошенничества и понимать, как обычно действуют взломщики, а также своевременно организовывать подходящую политику безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью работы является исследование методологии социальной инженерии, ее основных методов и принципов, а также разработка комплексных мер по противодействию получения несанкционированного доступа к конфиденциальной информации с её помощью.

В первой главе магистерской работы производится анализ предметной области социальной инженерии. Рассматриваются сферы использования и применения хакерских атак производящихся описанными методами. Также показываются главные отличительные особенности и преимущества подобных методов. Введены основные понятия и термины для дальнейшего более детального разбора. На основании проведенного анализа ставятся задачи на исследование.

Во второй главе приводятся более детальное описание существующих и применяемых способов атаки. Приведено множество достойных примеров, а также указаны слабые места в системах, где неподготовленный оператор имеет доступ к конфиденциальной информации. Определен круг, лиц для которых будет актуальна разработка специальных мер и служебных инструкций для ознакомления и применения к действию в работе с секретной информацией.

В третьей главе производится непосредственная разработка алгоритмов действий для операторов, имеющих доступ к конфиденциальной информации. Приведены правильные паттерны поведения и описаны основные технические и организационные меры противодействия социальной инженерии.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Социальная инженерия – метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека. Основной целью социальных инженеров, как и других хакеров и взломщиков, является получение доступа к защищенным системам с целью кражи информации, паролей, данных о кредитных картах и т.п. Основным отличием от стандартной кибератаки является то, что в данном случае в роли объекта атаки выбирается не машина, а ее оператор. Именно поэтому все методы и техники социальных инженеров основываются на использовании слабостей человеческого фактора, что считается крайне разрушительным, так как злоумышленник получает информацию, например, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего. Для защиты от атак данного вида следует знать о наиболее распространенных видах мошенничества, понимать, что на самом деле хотят взломщики и своевременно организовывать подходящую политику безопасности.

Существует несколько распространенных техник и видов атак, которыми пользуются социальные инженеры. Все эти техники основаны на особенностях принятия людьми решений, известных как когнитивные предубеждения. Эти предрассудки используются в различных комбинациях, с целью создания наиболее подходящей стратегии обмана в каждом конкретном случае. Но общей чертой всех этих методов является введение в заблуждение, с целью заставить человека совершить какое-либо действие, которое не выгодно ему и необходимо социальному инженеру. Для достижения поставленного результата злоумышленник использует целый ряд всевозможных тактик: выдача себя за другое лицо, отвлечение внимания, нагнетание психологического напряжения и т.д. Конечные цели обмана так же могут быть весьма разнообразными.

Наиболее распространённые методы социальной инженерии описаны ниже.

Претекстинг – это набор действий, проведенный по определенному, заранее готовому сценарию (претексту).

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Ложные антивирусы и программы для обеспечения безопасности. Подобное мошенническое программное обеспечение, также известное под названием «scareware», – это программы, которые выглядят как антивирусы, хотя, на самом деле, все обстоит совсем наоборот.

Телефонный фишинг – Вишинг (англ. vishing – voice phishing) назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений, с целью воссоздать "официальные звонки" банковских и других IVR систем.

Плечевой серфинг включает в себя наблюдение личной информации жертвы через ее плечо. Этот тип атаки распространен в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Квид про кво – в английском языке это выражение обычно используется в значении «услуга за услугу». Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону или электронной почте.

Троянская программа – это вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях.

«Дорожное яблоко» – это метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации в местах общего доступа, где эти носители могут быть легко найдены.

В работе эти методы и принципы были рассмотрены более детально, а также приведены примеры использования и описаны все плюсы и минусы данных методик.

Основной способ противодействия социальной инженерии заключается в обучении персонала неукоснительному соблюдению инструкций и выработке ответственности и дисциплины при оперировании конфиденциальными данными.

Разработанные рекомендации для организаций, а также составленные алгоритмы поведения операторов должны свести угрозы социальной инженерии к минимуму.

ЗАКЛЮЧЕНИЕ

В магистерской работе была исследована одна из опаснейших угроз информационной безопасности, которая согласно статистике стремительно набирает силу по всему миру. В связи с тем, что угроза социальной инженерии непосредственно связана с человеческим фактором, осуществить математическую оценку риска и рассчитать стоимость этого риска не представляется возможным. А то, что возможно рассчитать, сегодня компании не используют в виду дороговизны проведения такой оценки и отсутствием достаточного количества специалистов по предметной области.

В работе была рассмотрена история появления социальной инженерии, как термина, а затем как формирование межотраслевой науки. Были выяснены задачи и цели, решением которых она является. Определена методическая и научная база, которая вошла в качестве инструментов в социальную инженерию. Было рассмотрено, где сегодня социальная инженерия нашла свое применение, а также как один из инструментов мошенничества. Были изучены основные методы и принципы социальной инженерии, приведены достойные примеры. Кроме того, осуществлён анализ достоинств и недостатков существующих методов в исследуемой области.

На основании проведенной работы были разработаны общие рекомендации по снижению уровня риска и повышению общей защищенности систем, а также составлены алгоритмы поведения людей имеющий доступ к конфиденциальной информации.

Таким образом, все задачи, поставленные в техническом задании рассмотрены и выполнены.