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

УДК 004.056+004.54

Кармаз
Елена Викторовна

СОЦИОТЕХНИЧЕСКИЕ МЕТОДИКИ ТЕСТИРОВАНИЯ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В СИСТЕМАХ УПРАВЛЕНИЯ

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

1-23 80 08 – Психология труда, инженерная психология, эргономика

Магистрант Е.В. Кармаз

Научный руководитель
К.Д. Яшин, кандидат технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат технических наук, доцент

Минск 2020

ВВЕДЕНИЕ

На сегодняшний момент тяжело представить современный мир без тех технологий, которыми мы пользуемся. Каждая компания и организация использует различные технические устройства, многие процессы автоматизированы, множество систем работает по написанным программам, а человеку остаётся лишь контролировать процесс исполнения деятельности.

С помощью современных программ, а также компьютерных технологий, люди достигли больших высот и преобразований почти во всех сферах жизни общества. Однако, это имеет свои уязвимые аспекты, во-первых, человек стал зависим от своих технологий, во- вторых, теперь уязвимость одной технологии может привести к полной уязвимости организации, и есть те, кто может этим воспользоваться в корыстных целях. Именно поэтому сейчас любая организация имеет свой отдел безопасности, в работу которых входит в том числе защита информации [1].

В последнее время специалисты по информационной безопасности обсуждают полезность такого вида аудита информационной безопасности, как тестирование на проникновение.

Тестирование на проникновение – это имитация действий потенциального злоумышленника с целью оценки возможности несанкционированного доступа к корпоративной информационной системе и демонстрации уязвимостей существующей системы информационной безопасности. Тестирование на проникновение позволяет выявить уязвимости и слабые места в системе ИБ до того, как это сделают злоумышленники, оценить «практическую» защищенность от атак из «реального мира» [2].

Очевидным достоинствами методов тестирования на проникновение являются: высокая достоверность сведений о выявленных уязвимостях благодаря фактическому подтверждению возможности их использования злоумышленником; достаточность результатов исследования для оценки критичности выявленных уязвимостей; наглядность получаемых результатов.

Целью данной магистерской диссертации является разработка социотехнической методики поиска уязвимости в системе управления, для оценки уровня защищенности информационной системы.

Для достижения поставленной цели были установлены следующие задачи:

1) провести обзор существующих методов поиска уязвимостей, законодательства в области информационной безопасности, а также стандарта, используемого для проведения тестирования на проникновение;

2) разработать методику поиска уязвимостей в системах управления и провести тестирование разработанной методики;

3) выработать рекомендации по улучшению системы защиты информации, сформулировать выводы по проделанной работе.

ОБЩАЯ ХАРАКТЕРИСТИКА

Магистерская диссертация посвящена социотехническим методикам для поиска уязвимостей в системах управления.

Целью данной магистерской диссертации была разработка социотехнической методики для проведения тестирования на проникновение с целью поиска уязвимостей в системе управления.

Был проведен анализ существующих методик поиска уязвимостей, так же был проведен анализ законодательства в области информационной безопасности (ИБ), и рассмотрен стандарт, используемый для проведения тестирования на проникновение.

Было проведено внутреннее тестирование сотрудников с целью оценки их уровня осведомленности в области ИБ. Предложены мероприятия, которые необходимо проводить с сотрудниками для улучшения их осведомленности в области ИБ и уменьшения рисков организации, вызванных непосредственно человеческим фактором.

Выбранная тема магистерской диссертации является крайне актуальной в наше время. Техническое тестирование на проникновение – неотъемлемая часть объективной оценки безопасности, без которой сложно представить комплексную защиту информации. Однако, как показывает практика, самым слабым звеном в автоматизированной информационной системе с точки зрения обеспечения ее безопасности является человек, являющийся либо оператором данной системы, либо ее пользователем. Именно социотехническое тестирование на проникновение помогает с решением данной проблемы.

Материалы данной магистерской работы были опубликованы в сборнике 56-й Научно-технической конференция аспирантов, магистрантов и студентов БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе магистерской диссертации, были рассмотрены технологии тестирования на проникновение. Основной упор был сделан именно на тестирования на базе социотехнических методов. Данные методы позволяют не искать уязвимости в программно-аппаратных средствах защиты информации, а всеми доступными методами, в частности методами социальной инженерии, получать интересующую информацию от самих лиц, осуществляющих обработку информации. Такая технология менее затратная, однако она крайне эффективна для поиска уязвимости в системе. Она выявляет реальные проблемы и помогает построить эффективную стратегию по их устранению. Так же были рассмотрены популярные техники социальной инженерии. Особое место в данном разделе было отведено рассмотрению законодательного аспекта проведения тестирований на проникновение.

Во второй главе данной магистерской диссертации разрабатывалась социотехническая методика для поиска уязвимостей в системе управления. Была описана законодательная подготовка к тестированию на предприятии и основные фазы тестирования на проникновение. Главной частью второй главы являлась разработке пошагового футпритинга. Основной упор при разработке социотехнической методики для поиска уязвимостей в системе управления был сделан на этапе футпритинга с помощью социальных сетей.

Угроза атак в социальных сетях всегда находится на рекордно высоком уровне и включает в себя как банальный взлом аккаунта, так и мошенничество, а также различные способы распространения вредоносных программ и фишинг атаки. Самые серьезные атаки всегда нацелены на организации, независимо от размеров предприятия.

Однако в последние 3-4 года тема информационной безопасности и приватности в социальных сетях привлекает много внимания. Это вполне объяснимо: сети все больше открываются внешнему миру, были случаи утечки личных данных, аккаунты пользователей легко взламываются, а у администрации сетей есть доступ к любой информации. Но все это только внешняя часть, которая лежит на поверхности и о которой пишет пресса, однако это далеко не полная картина потенциальных угроз для личных данных.

Была расписана структура атаки в социальных сетях с целью получения конфиденциальной информации.

Поскольку социальные сети существует за пределами корпоративной сети, угроза атаки в социальных сетях может проявиться задолго до того, как вредоносное поведение будет выявлено внутри сети. Распознание и устранение подобных угроз требует глубокого понимания их природы. Если мы сравним тактику, методы и процедуру атак в социальных сетях с традиционными сетевыми атаками, то сможем сделать некоторые важные выводы.

Злоумышленники осуществляют атаку на корпоративную сеть в два этапа: разведка и реализация. Разведка включает в себя футпринтинг (например, сбор информации об IP-адресе и доменах организации),

сканирование (определение систем, использующих данные IP-адреса) и составление перечня (с указанием сервисов и доступных портов в целевых системах). Когда злоумышленники используют социальные сети, то их стратегия аналогична, но применяются совершенно иные методы. В социальных сетях атака на организации и корпоративные сети включает в себя футпринтинг, мониторинг и составление характеристики, взлом аккаунта и, наконец, непосредственно саму атаку.

На данный момент социальные сети по сути являются огромной базой данных с самой разнообразной информацией о сотнях миллионов людей по всему миру, которая к тому же неплохо структурирована. В последнее время сети все больше открываются внешнему миру, а многие личные данные пользователей уже доступны для всех желающих. Чем больше человек общается в разнообразных социальных сетях, тем больше информации о нем можно собрать без каких-либо трудов.

Современные социальные сети предлагают пользователям указать практически все о себе: фото; видео; связи (в том числе и по типам); интересы; образование; информацию о работе; места, в которых бывает человек; предпочитаемые продукты; личные мысли и т.д. Большинство информации доступно без регистрации, достаточно найти страницу пользователя в популярных социальных сетях, остальное можно увидеть после добавления пользователя в друзья, а вся информация, включая личную переписку (как минимум), доступна администрации этой сети, и никакие настройки приватности не скроют её.

Таким образом, информация в социальных сетях дает поистине безграничные возможности для социального футпритинга. Была расписана схема получения различных данных с помощью социальных сетей.

В третей главе было описано провидение тестирования на предприятии. Учитывая законодательную специфику проведения тестирования на проникновения с использованием социотехнических методик, при описании проводимого эксперимента название организации, а так же некоторая информация об участниках эксперимента были изменены для сохранения конфиденциальности полученных данных.

В данной магистерской диссертации для проведения аудита была выбрана организация, особенностью которой является ее мейдийность. Работники активно используют социальные сети для работы.

Для проверки действенности метода, описанного во второй главе, был выбран отдел организации, работники которого, как правило, не владеют техническими аспектами знаний систем защиты информации, т.к. основное направление данного отдела журналистика и реклама. Работники данного отдела, как правило, не владеют критически важной информацией об организации, однако, профессиональная деятельность журналиста тесно связана с таким понятием как конфиденциальность — обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её

обладателя; за несоблюдение конфиденциальности информации журналист может быть привлечён к административной или уголовной ответственности в судебном порядке.

Было проведено успешное тестирование по 10 шагу футпритинка описанного во второй главе магистерской диссертации. Проведя ряд несложных манипуляций с общедоступными ресурсами в сети, мы частично получили интересующую нас информацию. Тем самым мы проверили действенность разработанного метода, а так же подтвердили актуальность одной их самых опасных проблем в защите информации, как человеческий фактор.

Так же в третей главе магистерской диссертации были описаны меры противодействия социальной инженерии.

Сегодня в крупных компаниях систематически проводят всевозможные тесты на сопротивляемость социальной инженерии. Почти никогда действия людей, подпавших под атаку социальных хакеров, не носят умышленного характера. Но тем они и опасны, ведь если от внешней угрозы защититься сравнительно легко, то от внутренней – намного сложнее.

Чтобы повысить безопасность, руководство компаний проводит специализированные тренинги, контролирует уровень знаний своих сотрудников, а также само инициирует внутренние диверсии, что позволяет установить степень подготовленности людей к атакам социальных хакеров, их реакцию, добросовестность и честность.

Самый основной способ защиты от социальной инженерии — это обучение. Т.к. тот, кто предупреждён – тот вооружён. И незнание в свою очередь не освобождает от ответственности. Все работники компании должны знать об опасности раскрытия информации и способах ее предотвращения.

Кроме того, сотрудники компании должны иметь четкие инструкции о том, как, на какие темы говорить с собеседником, какую информацию для точной аутентификации собеседника им необходимо у него получить.

Кроме этого, можно выделить следующие правила:

1 Пользовательские учетные данные являются собственностью компании. Всем сотрудникам в день приема на работу должно быть разъяснено то, что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п.), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.

2 Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности. Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.

3 Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации. Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.

4 На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение. На компьютерах сотрудников также необходимо установить брандмауэр.

5 В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак. Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фитиновых атак.

6 Все сотрудники должны быть проинструктированы, как вести себя с посетителями. Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетители в службу безопасности.

7 Необходимо максимально ограничить права пользователя в системе. Например, можно ограничить доступ к web-сайтам и запретить использование съемных носителей. Ведь, если сотрудник не сможет попасть на фишинговый сайт или использовать на компьютере флеш-накопитель с «троянской программой», то и потерять личные данные он также не сможет.

Говоря о социальных сетях, в последнее время пользователи все меньше доверяют социальным сетям и все чаще начинают фильтровать информацию, которую готовы доверить сети, давать ложную информацию или вообще удаляются из сети, однако даже удаление не дает уверенности: часто информация сохраняется на серверах компании и может использоваться в дальнейшем, в частности так делает Facebook, ВКонтакте и другие сети. Поэтому размещение любой информации в социальных сетях требуют осмысленного подхода.

ЗАКЛЮЧЕНИЕ

Целью данной магистерской диссертации была разработка социотехнических методик тестирования для поиска уязвимостей в системе управления. Поставленная цель магистерской диссертации была выполнена путем решения следующих задач:

1) Был проведен анализ существующих методик поиска уязвимостей, а также был проведен анализ законодательства в области ИБ и рассмотрен стандарт, используемый для проведения тестирования на проникновение.

2) Был разработан план метода поиска уязвимости

3) Было проведено внутреннее тестирование сотрудников с целью оценки их уровня осведомленности в области ИБ. Предложены мероприятия, которые необходимо проводить с сотрудниками для улучшения их осведомленности в области ИБ и уменьшения рисков для организации, вызванных непосредственно человеческим фактором.

Выбранная тема магистерской диссертации является крайне актуальной в наше время. Тестирование на проникновение – неотъемлемая часть объективной оценки безопасности, без которой сложно представить комплексную защиту информации. Еще несколько лет назад компаниям было достаточно провести классическое техническое тестирование на проникновение для оценки уязвимости информационной системы. Однако, популяризация использования социальных сетей привела к новым возможностям получения конфиденциальной информации.

Угроза атак в социальных сетях находится на рекордно высоком уровне и включает в себя, как банальный взлом аккаунта, так и мошенничество. Именно поэтому, основной упор при разработке социотехнической методики для поиска уязвимостей в системе управления был сделан на этапе футпритинга с помощью социальных сетей

Современные социальные сети предлагают пользователям указать практически все о себе: фото, видео, связи, интересы, образование, информацию о работе, места, в которых бывает человек, предпочитаемые продукты, личные мысли и т.д. Большинство информации доступно без регистрации. Для этого достаточно найти страницу пользователя в популярных социальных сетях. Таким образом, информация в социальных сетях дает поистине безграничные возможности для социального футпритинга. Далее остается лишь грамотно воспользоваться полученной информацией из социальных сетей и методами социальной инженерии, чтобы получить конфиденциальную информацию.

Рассмотренная структура атак в социальных сетях малозатратна, однако может нанести невероятный ущерб для организации при ее успешной реализации. Именно это объясняет востребовательность социотехнического тестирования на проникновение, которое позволяет вовремя найти уязвимость в системе.

Рассмотренные в данной работе методы получения информации за счет воздействия на персонал организаций и методы противодействия являются актуальными.

Степень угрозы информации не может быть в общем случае адекватно и всесторонне оценена и ранжирована в зависимости от тяжести нанесенного ущерба. Человеческое мышление не всегда поддается логическому анализу, и, вследствие этого, невозможно сформировать четкий алгоритм его работы. Можно только определить перечень целей и требовать от сотрудника строгого его соблюдения.

Обеспечение деятельности персонала организации в рамках утвержденных инструкций и правил работы является одной из главных задач руководителя организации. Если руководитель организации с такой задачей справится, то методы социальной инженерии не будут представлять в целом значимой угрозы.

Самый основной способ защиты от социальной инженерии — это обучение. Все работники компании должны знать об опасности раскрытия информации и способах ее предотвращения. Кроме того, сотрудники компании должны иметь четкие инструкции о том, как, на какие темы говорить с собеседником, какую информацию для точной аутентификации собеседника им необходимо у него получить.

Так же любому сотруднику организаций стоит помнить о том, что размещение любой информации в социальных сетях требуют осмысленного подхода.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Кармаз, Е.В. Социальные сети, как источник информации для социотехнических методик тестирования на проникновение и поиска уязвимостей в системе/ Е.В. Кармаз// Сборник тезисов 56-й Научной конференции аспирантов, магистрантов и студентов БГУИР – Минск, 2020 – С. 49.

2-А. Кармаз, Е.В. Основные типы тестирования на проникновение в зависимости от количества предоставляемой информации о системе/ Е.В. Кармаз// Сборник тезисов 56-й Научной конференции аспирантов, магистрантов и студентов БГУИР – Минск, 2020 – С. 51.