УДК 004.428.4

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ОДНО ИЗ НАПРАВЛЕНИЙ КИБЕР-ПРЕСТУПЛЕНИЙ

Ради Мурад
студент
Брозгунова Надежда Петровна
кандидат экономических наук, доцент
nadyazhm@mail.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматривается вопросы посвященные кибер-преступности в целом и социальной инженерии в частности. Данный вид преступлений в сфере IT является особым видом, основанным на манипулирование человеком, с целью извлечения информации из компьютерной системы без необходимости выполнения каких – либо действий компьютерного взлома.

Ключевые слова: социальная инженерия, IT преступления, кибер-преступления, хакер, средства защиты.

В настоящее время кибер – преступность является серьезным явлением, тормозящим процессы цифровизации общества. Разработано значительное количество способов и методов, позволяющих похитить данные, нанести вред информационной системе. Как бы ни изощрялись компьютерные злоумышленники в технических решениях, необходимо помнить, что основная угроза безопасности данных современных информационных систем может исходить от пользователей, сотрудников фирмы [1, 2].

Несколько лет назад родилась новая форма атаки, которая становится все более и более распространенной – социальная инженерия (Social Engineering) которая основана, ни на компьютерном инструменте, эксплуатационном оборудовании или программном обеспечении. Для этого типа атаки центром действия становится пользователь информационной системы, сотрудник организации [1]. Социальная инженерия направлена на манипулирование человеком, с целью звлечения информации из компьютерной системы без необходимости выполнения каких – либо действий компьютерного взлома [3].

Чтобы осуществить атаку на информационные ресурсы организации, хакеры все чаще прибегают к социальной инженерии, которая основана на доверчивости, лени, энтузиазме, мотивации персонала. Защититься от нападения этого типа весьма сложно, адресаты могут до конца так и не понять, что они были обмануты, или не признавать этого [3, 4]. Хакеры в данном случае пытаются использовать сотрудников методом убеждения и вынудить их выдать информацию, которая даст возможность им воспользоваться системными ресурсами организации.

Руководство многих мелких и средних компаний полагает, что хакерские нападения — проблема больших корпораций или банков, ведь это сулит большую финансовую выгоду, в отличие от нападения на мелкие фирмы. Такой подход, возможно, был справедлив в прошлом, однако теперь хакеры атакуют все большее число организаций и частных лиц [5]. Преступники могут захватить компанию, атакуя информационные системы и ресурсы, но они также могут использовать компанию как площадку для нападения на другие компании.

Чтобы защитить персонал от таких атак, руководители компаний должны иметь представление о особенностях таких нападений, его возможных целях, потенциальных потерях и заблаговременно принимать меры по усилению политики безопасности [6, 7].

Социальная инженерия включает в себя совокупность подходов ориентированных на [6]:

* изменении поведения и установок людей;

* решении социальных проблем;

* адаптации социальных институтов к изменяющимся условиям;

* сохранении социальной активности.

В отношении информационной безопасности социальная инженерия позволяет организовывать и описывать прежде всего угрозы нетехнического характера.

Убеждение и манипуляция являются краеугольными камнями этой техники. Социальную инженерию можно применять в различных сценариях, что еще больше затрудняет ее выявление. Преступник стремится оказать психологическое давление на жертву, ссылаясь на срочность или конфиденциальность, чтобы быстро получить желаемую информацию [1, 6, 8].

К сожалению, существует множество примеров атак социальной инженерии. Так, например, во Франции в небольшой компании преступник присвоил адрес электронной почты менеджера, чтобы отправить электронные письма директору по финансовым вопросам. В сообщении предлагалось осуществить переводы на банковские счета для открытия и продвижения своего рынка в Китае. Упор был сделан на конфиденциальность и быстроту сделки.

В другом регионе в бизнес-пространстве велась работа по оптоволокну. Чтобы получить доступ к данным компании, на которую он нацелился, злоумышленник притворился техническим специалистом Orange. Сотрудник компании предоставил ему доступ к сетевым технологиям, через которые хакер смог получить удаленный доступ к сетевым информационным ресурсам компании.

В Японии киберпреступники использовали службу доставки на дом для распространения компакт-дисков, зараженных трояном-шпионом. Адреса клиентов японского банка были украдены из базы данных банка. Затем хакеры отправили зараженные компакт-диски непосредственно клиентам заведения, чтобы восстановить их банковские реквизиты.

В сценарии атаки социальной инженерии многочисленны, поэтому, готового решения для защиты от этих атак не существует, но в каждой компании есть ряд методов [3, 4].

Пользователь - ключевой момент социальной инженерии. Поэтому важно, чтобы сотрудники знали о проблеме, а также о важности и значимости информации, которую они передают. Также важно, чтобы они знали о влиянии, которое они могут оказать на компьютерную систему .

Как один из методов предупреждения социальной инженерии можно также отметить внедрение тестов на фишинг. Фишинг направлен на отправку поддельных электронных писем или поддельные телефонные звонки вашим сотрудникам [8]. Цель этого теста - смоделировать атаку социальной инженерии. Этот тип упражнений позволяет проанализировать количество открытий поддельного электронного письма, выявить сотрудников, которые перешли по мошеннической ссылке. Данный тест поможет также определить наиболее уязвимых сотрудников фирмы и составить план обучения или повышения их осведомленности.

Таким образом, информационная безопасность зависит не только от сложных систем защиты на техническом уровне, но и от работы с каждым сотрудником, имеющим доступ к информационным ресурсам предприятия.

Список литературы:

1. How to Protect Insiders from Social Engineering Threats. Midsize Business Security Guidance. Microsoft, 2006. www.microsqft.com

2. Аникьева, Э.Н. Рейтинг антивирусных программ / Э.Н. Аникьева, О.С. Картечина, Т.А. Свиридова // Наука и Образование. – 2020. – Т. 3. – № 2. –

С. 15. Смыкова Е.Н. Элементы web – дизайна / Е.Н. Смыкова, Э.Н. Аникьева // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 16

3. Аникьева, Э.Н. Интернет и киберпреступность / Э.Н. Аникьева, А.А. Дегтерева // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 14

4. Скрипко, Ю.А., Использование информационных технологий в образовании / Ю.А. Скрипко, С.О. Чиркин, Л.И. Никонорова // Наука и Образование. – 2019. – Т. 2. – № 4. – С. 205.

5. Проектирование и реализация интерактивной специализированной информационно-справочной системы / С.В. Федоров, И.В. Уколов, А.А. Лукин [и др.] // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 3.

6. Zulfikar Ramzan. Drive-By Pharming: How Clicking on a Link Can Cost You Dearly, www.symantec.com

7. Копцев, П.Ю. Влияние информационных технологий на рост синергетического эффекта в АПК // П.Ю. Копцев, Н.В. Картечина, Ю.А. Скрипко // В сб.: Инженерное обеспечение инновационных технологий в АПК: материалы Международной научно-практической конференции – Мичуринск: Мичуринский государственный аграрный университет, 2018. – С. 187-190.

8. Balint technology in pedagogy: Innovations or transfer of psychological experience / N.I. Rudneva, G.V. Korotkova, O.S. Sinepupova, S.V. Belyakova // International Journal of Engineering and Advanced Technology. – 2019. - 9(1). - с. 4506-4510

UDC 004.428.4

SOCIAL ENGINEERING AS ONE OF THE DIRECTIONS OF CYBER CRIMES

Radi Myrad
student
Brozgunova Nadezhda Petrovna
Candidate of Economic Sciences, Associate Professor
nadyazhm@mail.ru
Michurinsky State Agrarian University
Michurinsk, Russia

Annotation. The article discusses issues related to cyber crime in general and social engineering in particular. This type of crime in the IT sphere is a special type based on human manipulation in order to extract information from a computer system without the need to perform any computer hacking actions.

Key words: social engineering, IT crimes, cyber crimes, hacker, means of protection.