МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное

образовательное учреждение высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИМЕНИ В.И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

ОТЧЕТ ПО ТЕМЕ

«СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ»

студента 3 курса

группы ИВТ-б-о-222(1)

Гоголева Виктора

Симферополь, 2024

Цель работы

Изучить понятие социальной инженерии, причины возникновения, акктуальность, рассмотреть методы социальной инженерии, ознакомиться со статистическими данными.

Ход работы

Социальная инженерия — это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и является очень эффективным.

1. Причины возникновения социальной инженерии

По моему мнению, причиной возникеновения методов социальной инжнерии, явялется то, что с каждым годом вводятся новые инструменты защиты систем и инфраструктур, из-за чего к ним становится гораздо труднее получить доступ, однако все еще в процессах систем остается человек, который является «узким горлышком». Так как, на человека, в отличии от «бездушной машины», можно влиять на уровне эмоций и психики,в следствии чего его можно расположить к себе, влиться в доверие,ввести в заблуждение, или же наоборот – запугать.

Из сказаного выше следует, что реализовать атаки методами социальной инженерии гораздо проще и дешевле, чем атаками на аппаратные или программные составляющие системы.

1. Акктуальность социальной инженерии

Я считаю, что акктуальность данного инструмента для атак обусловленна увеличением числа пользователей сетью Интернет, доступностью информационных технологий, а так же популяризацией смартфонов, компьютеров, из-за снижения их стоимости. По данным ТАСС сетью Интернет в РФ на конец 2022 пользуется около 130 миллионов жителей(90 % населения). На рисунке ниже показан график распределения пользователей сети в РФ по вовзрасту.

Еще одной причиной роста популярности социальной инжнерии является, то что это один из лучших инструментов для обхода политик конфеденциальности организации, политик доступа и аудита пользователей, так как права доступа явлются основной проблемой для многих атак.



Рисунок 1 – график распределения пользователей Интеренет по возрасту в РФ

По графику можно заметить, что сейчас достаточно много людей в возрасте и детей (которые не учитываются в статистике) пользуются сетью. Некоторые дети еще разговаривать не научились, а уже держат сматрфон в руках. В следствии чего осведомоленность и уровень безопасности в Сети у этих возрастных групп находятся под большой угрозой, чем мошенники и пользуются.

1. Статистические данные по социальной инженерии

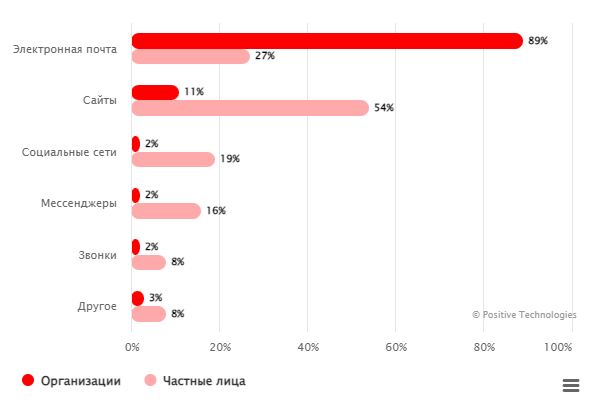
Цитата из отчета Positive Technologies за 3 квартал 2023 года: «Социальная инженерия все так же остается главной угрозой для частных лиц (92%) и одним из основных векторов атаки на организации (37%). За рассматриваемый период в результате успешных атак организации чаще всего встречались с утечкой данных (56%). В III квартале 2023 года в успешных атаках на частных лиц злоумышленники применяли разные каналы социальной инженерии. Чаще всего преступники использовали фишинговые сайты (54%) и электронные письма (27%), а также выстраивали мошеннические схемы в социальных сетях (19%) и мессенджерах (16%).»

Рисунок 2 – используемые злоумышелнниками каналы социальной инженерии

Злоумышленники продолжали эксплуатировать для фишинга темы трудоустройства, служб доставки, политических событий и быстрого заработка, в том числе с помощью криптовалют. Для проведения атак киберпреступники использовали платформы, предоставляющие своим клиентам инструменты для проведения фишинговых атак. Например, специалисты Proofpoint сообщили о масштабной кампании с использованием EvilProxy. Мошенники отправили более 120 000 фишинговых писем. В прошлом году мы рассказывали о появлении этой платформы, а сейчас уже наблюдаем ее прицельное применение киберпреступниками, направленное на руководство более 100 компаний: 65% жертв относились к высшему руководящему звену, а у остальных 35% целей имелся доступ к финансовым активам или конфиденциальным данным компании.

1. Методы социальной инженерии

* фишинг: Популярный метод, когда мошенники отправляют поддельные электронные письма или сообщения, маскируясь под официальные организации, чтобы выманить у жертвы логины, пароли или банковские данные;
* cмишинг и вишинг: Смишинг — это фишинг через SMS, а вишинг — через голосовые звонки. Цель та же: выманить конфиденциальные данные или деньги;
* редтекстинг: Мошенник создает ложную историю или предлог для общения с жертвой, чтобы выманить информацию. Например, может представиться сотрудником банка и попросить данные карты для "проверки";
* байтинг: Это создание заманчивых, но фальшивых предложений или файлов, которые жертва скачивает, предоставляя доступ к своему устройству;