УДК 004 **Информационные технологии**

Черкашин Василий Юрьевич, *магистрант,*
ДГТУ Ростов-на-Дону, РФ

АТАКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация: В постоянно меняющемся ландшафте кибербезопасности угрозы становятся все более изощренными. В то время как технические средства защиты улучшились, злоумышленники нашли постоянную и часто уязвимую цель: людей. Атаки социальной инженерии представляют собой категорию киберугроз, которые используют человеческую психологию и доверие для получения несанкционированного доступа к системам, информации или ресурсам. Данная статья погружает в мир атак социальной инженерии, исследуя их различные формы, тактику, последствия, а также важность осведомленности и контрмер.

Ключевые слова: социальная инженерия, атака, информационная безопасность, киберугроза.

Annotation: In the ever-changing cybersecurity landscape, threats are becoming more sophisticated. While technical defenses have improved, attackers have found a constant and often vulnerable target: people. Social engineering attacks are a category of cyber threats that exploit human psychology and trust to gain unauthorized access to systems, information, or resources. This article dives into the world of social engineering attacks, exploring their various forms, tactics, consequences, and the importance of awareness and countermeasures.

Keywords: social engineering, attack, information security, cyber threat.

Введение

В данный момент существует множество разнообразных способов аиак на

информационную систему. Так можно выделить следующие формы атак в социальной инженерии [1]:

1. Фишинговые атаки связаны с использованием мошеннических электронных писем, сообщений или веб-сайтов, которые кажутся законными. Цель состоит в том, чтобы обманом заставить людей раскрыть конфиденциальную информацию, такую как пароли, номера кредитных карт или личные данные, удостоверяющие личность.

2. Атаки под предлогом основаны на создании сфабрикованного сценария или предлога для манипулирования жертвой с целью заставить ее разгласить информацию. Распространенные примеры включают в себя выдачу себя за кого-то из представителей власти или симуляцию чрезвычайной ситуации.

3. Атаки с травлей заманивают жертв чем-то заманчивым, например бесплатной загрузкой или предложением перейти по вредоносным ссылкам или загрузить вредоносное ПО. Это часто наблюдается при распространении вредоносных файлов или USB-накопителей.

4. При атаках "услуга за услугу" злоумышленник обещает выгоду или услугу в обмен на информацию. Например, злоумышленник может представиться специалистом ИТ-службы поддержки и запросить учетные данные для входа в систему, чтобы "устранить" проблему.

5. Слежка за персоналом - эти физические атаки с использованием социальной инженерии предполагают, что неавторизованные лица следуют за уполномоченным персоналом в безопасные зоны, пользуясь их доверием.

Рассмотрим тактика и приемы атаки социальной инженерии успешные на данном этапе развития [2]:

1. Манипулирование доверием - злоумышленники используют естественную человеческую склонность доверять другим и помогать им. Они часто выдают себя за заслуживающих доверия лиц или используют эмоциональные призывы, чтобы обмануть жертв.

2. Обман и олицетворение - злоумышленники убедительно выдают себя за других, часто используя официальные документы, веб-сайты или телефонные

номера, чтобы обмануть своих целей.

3. Создание срочности или страха, так злоумышленники часто используют тактику запугивания, такую как угрозы судебного иска или финансовых последствий, чтобы заставить жертв предпринять немедленные действия.

Атаки социальной инженерии могут иметь серьезные последствия:

1. Утечка данных: эти атаки могут привести к несанкционированному доступу к конфиденциальным данным, что приведет к утечке данных, которая может иметь финансовые, юридические и репутационные последствия.

2. Финансовые потери: жертвы могут понести финансовые потери, особенно в случаях мошенничества или кражи личных данных.

3. Ущерб репутации: отдельные лица и организации могут столкнуться с ущербом для своей репутации, подрывающим доверие между клиентами, заказчицами и партнерами.

4. Юридическая ответственность. В случае компрометации личных или конфиденциальных данных могут возникнуть юридические последствия, приводящие к штрафным санкциям со стороны регулирующих органов.

Предотвращение атак социальной инженерии

Образование и осведомленность: Комплексные программы обучения и повышения осведомленности могут научить людей распознавать тактику социальной инженерии и развить скептический настрой. Верификация и аутентификация. Всегда проверяйте личность отдельных лиц или запросы, особенно в незнакомых ситуациях или в условиях повышенного давления. Использование многофакторной аутентификации (MFA): MFA добавляет дополнительный уровень безопасности, требуя нескольких форм проверки для доступа к конфиденциальным учетным записям или данным. Политика и процедуры кибербезопасности: Разработайте и применяйте строгие политики и процедуры кибербезопасности, которые определяют, как обращаться с конфиденциальной информацией и реагировать на потенциальные угрозы. Регулярные обновления и исправления: Поддержание программного обеспечения, операционных систем и средств безопасности в актуальном

состоянии может помочь защитить от атак социальной инженерии.

Заключение

Атаки социальной инженерии представляют собой постоянную и всепроникающую угрозу в сфере кибербезопасности. Они используют человеческую психологию, доверие и эмоции для обмана отдельных лиц и получения несанкционированного доступа к информации или ресурсам. Распознавание различных форм, тактик и последствий атак социальной инженерии имеет важное значение как для отдельных лиц, так и для организаций. Повышая осведомленность, внедряя надежные меры кибербезопасности и поддерживая бдительный и скептический настрой, мы можем лучше защищаться от этих коварных угроз и защищать нашу цифровую жизнь и активы.

Библиографический список:

1. Социальная инженерия и социальные хакеры /. М.В. Кузнецов, И. В. Симдянов. СПб.: БХВ-Петербург, 2007.

2. Искусство обмана / Митник К., Саймон В. М: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2006 г.