Денисов Н.А. Фактор человеческого воздействия на безопасность: тактики социальной инженерии // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 9(47) с. 47–51

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ФАКТОР ЧЕЛОВЕЧЕСКОГО ВОЗДЕЙСТВИЯ НА БЕЗОПАСНОСТЬ: ТАКТИКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Денисов Н.А.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», г. Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ndenisoff@icloud.com

Кибербезопасность играет ключевую роль в современном мире, где зависимость от компьютерных систем и интернета только растет. Она важна для защиты персональных данных и критической инфраструктуры от различных угроз, включая киберпреступность, шпионаж и кибертерроризм. Кибербезопасность затрагивает не только компьютерные системы и сети, важную роль также играют люди, использующие эти технологии. Недавняя оценка монитора угроз показывает, что почти треть сотрудников попадают на уловки социальной инженерии. Злоумышленники используют человеческие эмоции, чтобы заставить жертву поделиться конфиденциальными личными или профессиональными данными. Эта статья анализирует взаимосвязь между социальной инженерией и кибербезопасностью, освещая ключевую роль ИТ-технологий в защите от киберугроз.

Ключевые слова: Кибернетические системы, кибербезопасность, киберугрозы, социальная инженерия, кибератаки. кибернетические системы, кибербезопасность, киберугрозы, социальная инженерия, кибератаки.

THE FACTOR OF HUMAN IMPACT ON SECURITY: TACTICS OF SOCIAL ENGINEERING

Denisov N.A.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ndenisoff@icloud.com

Cybersecurity plays a key role in today's world, where dependence on computer systems and the Internet is only growing. It is important to protect personal data and critical infrastructure from various threats, including cybercrime, espionage and cyberterrorism. Cybersecurity affects not only computer systems and networks, but people using these technologies also play an important role. A recent threat monitor assessment shows that almost a third of employees fall for the tricks of social engineering. Attackers use human emotions to force the victim to share confidential personal or professional data. This article analyzes the relationship between social engineering and cybersecurity, highlighting the key role of IT technologies in protecting against cyber threats.

Keywords: Cybernetic systems, cybersecurity, cyber threats, social engineering, cyber attacks.

Кибербезопасность (или кибернетическая безопасность) — это область, посвященная защите компьютерных систем, сетей, программного обеспечения и данных от киберугроз [1]. Она включает в себя различные методы, технологии и практики, направленные на предотвращение кибератак, обеспечение конфиденциальности, целостности и доступности информации, а также на обнаружение и реагирование на киберпреступность [2, 3]. Современные компьютерные системы и сети становятся более сложными и взаимосвязанными, что увеличивает потенциальные риски кибератак. Несмотря на развитие технологических мер безопасности, человеческий фактор продолжает играть решающую роль

в обеспечении кибербезопасности. Социальная инженерия эксплуатирует человеческие ошибки для обхода самых совершенных технологических защит.

В современном мире информационных технологий стратегия многоуровневой защиты является фундаментальным элементом кибербезопасности. Эта стратегия предусматривает комплексный подход, начиная с физической безопасности оборудования, которая предотвращает несанкционированный физический доступ к важным системам. Далее, сегментация сети позволяет эффективно управлять трафиком, чтобы минимизировать риски распространения угроз внутри сетевой инфраструктуры. Также важным элементом является применение антивирусных программ и шифрования данных, которые защищают от программных вторжений и утечек информации. Кроме того, использование облачных технологий способствует повышению устойчивости систем к атакам за счет распределения ресурсов и резервирования данных.

В дополнение к многоуровневой защите, важную роль играют интеллектуальные системы обнаружения и реагирования, которые интегрируют принципы машинного обучения и искусственного интеллекта. Эти системы способны обнаруживать угрозы в реальном времени и анализировать большие объемы данных, что позволяет предсказать потенциальные атаки. Такой подход позволяет организациям оперативно реагировать на инциденты, минимизируя ущерб.

Еще одним критическим аспектом современной кибербезопасности является аутентификация и управление доступом. Биометрические технологии и многофакторная аутентификация на сегодняшний день становятся стандартом в обеспечении защиты доступа к критической инфраструктуре. Эти методы снижают риск несанкционированного доступа, укрепляют защиту информационных ресурсов и обеспечивают высокий уровень безопасности в цифровой среде.

Таким образом, многоуровневая защита, совместно с интеллектуальными системами и продвинутыми технологиями аутентификации, формирует основу надежной защиты в сфере информационной безопасности, обеспечивая комплексный подход к противодействию киберугрозам.

Психология социальной инженерии занимается изучением методов манипуляции и влияния на поведение людей для получения конфиденциальной информации, доступа к системам или выполнения определённых действий. Основываясь на глубоком понимании человеческой психологии, социальных норм и межличностных отношений, социальная инженерия использует комплексные техники для достижения своих целей.

Социальные инженеры применяют манипуляции, включающие обман и создание доверительных отношений для убеждения людей поступать определенным образом. Например, они могут создать ложную идентичность или представить себя как доверенное лицо организации для обмана цели. Также они могут собирать информацию через фишинг или прослушивание, используя эти данные для дальнейших атак.

Одна из ключевых стратегий в социальной инженерии — установление и поддержание доверительных отношений, что позволяет манипуляторам получать необходимую информацию или провоцировать определённые действия. Знание и использование социальных норм помогает злоумышленникам убедить людей в необходимости выполнения определённых действий или раскрытия информации. Более того, понимание эмоциональных

реакций и манипулирование чувствами, такими как страх, вина или любопытство, также являются эффективными инструментами социальной инженерии.

Психология социальной инженерии находит применение в множестве сфер, включая кибербезопасность, маркетинг и продажи, а также в криминальной деятельности. Понимание её основных принципов и методов помогает обороняться от манипуляций и распознавать попытки социальной инженерии, уменьшая риск успешных атак.

Понимание человеческого поведения и применение принципов влияния важны не только для преступников, но и для добросовестных работников компании, так как социальная инженерия включает в себя множество тактик, направленных на манипуляцию людьми для доступа к конфиденциальной информации или ресурсам. Компаниям важно образовывать сотрудников, чтобы избежать утечки данных.

Злоумышленники могут представляться как доверенные лица или члены организации для доступа к информации. Они также могут создавать ложные идентичности, чтобы убедить цель в их подлинности. Важной тактикой является использование авторитета или создание ситуации, где цель чувствует давление или страх перед негативными последствиями в случае отказа сотрудничать. Злоумышленники могут опираться на социальные нормы и ожидания, чтобы убедить человека выполнить требуемые действия или раскрыть информацию.

Фишинг является одной из распространённых форм социальной инженерии, в которой сотрудникам отправляются ложные сообщения, имитирующие законные запросы, для получения конфиденциальных данных. Эмоциональные приемы, такие как вызывание страха, чувства вины или любопытства широко используются для манипулирования поведением цели. Кроме того, инженерия социальных связей помогает выявлять уязвимые точки в межличностных отношениях для дальнейшей манипуляции.

Эти методы активно применяются как в офлайн, так и в онлайн средах для достижения разнообразных целей, включая киберпреступления, шпионаж и мошенничество. Понимание и осведомлённость о данных тактиках повышают бдительность и защищённость людей от возможных манипуляций.

Социальная инженерия, хотя и часто связывается с психологическими аспектами манипуляции, в современной информационной безопасности преимущественно основывается на технологических подходах для воздействия на жертв. Это направление изучает методы влияния на человека, заставляя его предпринимать действия, которые могут быть против его собственных интересов, и применяется как в киберпреступности, так и в законных сферах бизнеса и маркетинга.

Атаки социальной инженерии используют тщательно подобранные тактики для вызова эмоциональной реакции, такие как страх или жадность. Например, популярными методами являются фишинговые атаки, где злоумышленники могут отправлять электронные письма, уведомляя жертв о мошеннической активности в их банковских счетах, что создает срочность и страх потери средств. Это заставляет жертву предпринимать немедленные действия, такие как изменение паролей или передача конфиденциальной информации, что и является целью злоумышленника.

Другой пример — это мошенничество с "виртуальным похищением", где жертвам говорят, что их близкие в опасности и требуется выкуп. Эти сценарии специально

разработаны, чтобы максимизировать эмоциональное воздействие и заставить жертву действовать под давлением.

В цифровую эпоху социальные инженеры также используют онлайн платформы для распространения своих атак, применяя методы, такие как отправка манипулирующих сообщений через социальные сети или электронную почту. Эти сообщения могут обещать большие выгоды или эксклюзивный доступ к товарам и услугам, вызывая любопытство и желание у жертвы воспользоваться предложением. Как правило, такие атаки приводят к утечке личных данных или финансовых средств.

В контексте информационной безопасности, понимание и применение защитных мер против тактик социальной инженерии крайне важно. Компании и индивидуальные пользователи должны обучаться распознаванию признаков фишинга и других форм социальной инженерии, а также использовать многофакторную аутентификацию и другие технологические средства для защиты своих систем и данных от несанкционированного доступа.

Заключение

Таким образом, социальная инженерия совмещает психологические и технологические аспекты в сфере информационной безопасности. Эффективность таких атак подтверждает, что технологические средства защиты, несмотря на своё развитие и сложность, оказываются уязвимыми перед хорошо организованными манипуляциями с человеческим фактором. Важно осознавать, что технологии не могут полностью защитить от угроз, если не принимать во внимание человеческий элемент.

Современные методы киберзащиты должны включать не только физические и программные меры безопасности, но и активное применение стратегий противодействия социальной инженерии. Это включает в себя образование и тренировки сотрудников, развитие корпоративной культуры осведомлённости о киберугрозах и постоянное обновление политик безопасности в ответ на новые методы атак.

Список литературы

1. Tsvetkov V.Ya., Shaytura S.V., Sultaeva N. L. Digital Enterprise Management in Cyberspace. - Proceedings of the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth” (MTDE 2020), Yekaterinburg, Russia, pp. 361 – 365, doi:10.2991/aebmr.k.200502.059
2. Филимонова А.В., Заливина Д. А., Митрофанова Т. В. О социальной инженерии в кибербезопасности // Информационные технологии. Проблемы и решения. 2020. № 1(10). С. 139–144.
3. Сулейманов Р. Фишинг — ловля рыбы в темной воде // Системный администратор. 2020. № 4(209). С. 52–53.
4. Старостенко Н.И. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. 2020. № 1(47). С. 80–83.
5. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы противодействия // Вестник науки. 2020. Т. 1, № 2(23). С. 85–88.

6. Сахно В.В., Пищаева А.С. Социальная инженерия, ее техники и способы защиты // Modern Science. 2020. № 2-2. С. 349–351.
7. Демидов М.А., Васильев В.А. Социальная инженерия и методы борьбы с ней // Трибуна ученого. 2020. № 7. С. 336–339

References

1. Tsvetkov V.Ya., Shaytura S.V., Sultaeva N.L. Digital Enterprise Management in Cyberspace. - Proceedings of the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth” (MTDE 2020), Yekaterinburg, Russia, pp. 361 – 365, doi:10.2991/aebmr.k.200502.059
2. Filimonova A.V., Zalivina D.A., Mitrofanova T.V. About social engineering in cybersecurity // Information technologies. Problems and solutions. 2020. No. 1(10). pp. 139–144.
3. Suleymanov R. Phishing - fishing in dark water // System administrator. 2020. No. 4(209). pp. 52–53.
4. Starostenko N.I. Forensic aspect of social engineering techniques in the commission of crimes // Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2020. No. 1(47). pp. 80–83.
5. Sozaev S.S., Kunashev D.A. Social engineering, its techniques and methods of counteraction // Bulletin of Science. 2020. T. 1, No. 2(23). pp. 85–88.
6. Sakhno V.V., Pishchaeva A.S. Social engineering, its techniques and methods of protection // Modern Science. 2020. No. 2-2. pp. 349–351.
7. Demidov M.A., Vasiliev V.A. Social engineering and methods of combating it // Tribune of a Scientist. 2020. No. 7. pp. 336–339