Гаджиев Г.К. Исследование влияния социальных аспектов на кибербезопасность: как человеческий фактор влияет // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 34–37

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СОЦИАЛЬНЫХ АСПЕКТОВ НА КИБЕРБЕЗОПАСНОСТЬ: КАК ЧЕЛОВЕЧЕСКИЙ ФАКТОР ВЛИЯЕТ

Гаджиев Г.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

В статье рассматривается влияние социальных аспектов на кибербезопасность, а также роль человеческого фактора в уязвимости цифровых систем. Анализируются основные угрозы, связанные с недостаточной кибер-грамотностью, фишинговыми атаками, социальной инженерией и инсайдерскими угрозами. Описаны методы защиты, включая обучение пользователей, усиленную аутентификацию, технические меры безопасности и мониторинг поведения. Особое внимание уделяется необходимости формирования культуры кибербезопасности как ключевого элемента защиты информации.

Ключевые слова: Кибербезопасность, человеческий фактор, социальная инженерия, фишинг, инсайдерские угрозы, кибер-грамотность, многофакторная аутентификация, мониторинг пользователей.

RESEARCH INTO THE IMPACT OF SOCIAL ASPECTS ON CYBERSECURITY: HOW HUMAN FACTORS AFFECT

Gadzhiev G.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article examines the impact of social aspects on cybersecurity, as well as the role of the human factor in the vulnerability of digital systems. The main threats related to insufficient cyber literacy, phishing attacks, social engineering and insider threats are analyzed. Protection methods are described, including user training, enhanced authentication, technical security measures, and behavior monitoring. Special attention is paid to the need to form a culture of cybersecurity as a key element of information protection.

Keywords: Cybersecurity, human factor, social engineering, phishing, insider threats, cyber literacy, multifactor authentication, user monitoring.

Введение

С развитием технологий и повсеместной цифровизации всё больше аспектов жизни переходят в онлайн-пространство. Это приводит к росту числа кибератак, в которых центральную роль играет человеческий фактор. Социальные аспекты, такие как психологические особенности пользователей, уровень их осведомлённости в области информационной безопасности, а также социальная инженерия, значительно влияют на уязвимость цифровых систем. Независимо от уровня технологической защиты, ошибки пользователей, недостаточная подготовка сотрудников и влияние социальных механизмов остаются важными факторами, способствующими угрозам безопасности.

Основные уязвимости, связанные с человеческим фактором.

Одной из ключевых уязвимостей является низкий уровень кибер-грамотности пользователей. Многие пользователи используют слабые пароли, игнорируют двухфакторную аутентификацию и не проверяют источники информации перед её обработкой. Это делает их лёгкой мишенью для киберпреступников, использующих фишинг, социальную инженерию и вредоносное ПО.

Фишинговые атаки являются одной из наиболее распространённых угроз. Киберпреступники создают поддельные веб-сайты или электронные письма, побуждая пользователей вводить конфиденциальные данные, такие как логины и пароли. Недостаточная бдительность и нехватка знаний об этих угрозах приводят к значительному числу успешных атак [1-2].

Другим важным аспектом является поведенческая предсказуемость пользователей. Злоумышленники анализируют поведение жертв, используя методы социальной инженерии, чтобы заставить их выполнить нужные действия. Это может включать предоставление личных данных, загрузку вредоносных файлов или открытие доступа к конфиденциальным системам.

Также следует отметить проблему инсайдерских угроз [3]. Сотрудники компаний, будь то по неосторожности или с умышленным умыслом, могут становиться источником утечек данных и компрометации систем. Внутренние угрозы сложно обнаружить, так как инсайдеры зачастую обладают высоким уровнем доступа к информации.

Методы защиты от угроз, связанных с человеческим фактором.

Для повышения уровня безопасности необходимо внедрение комплексных мер, направленных на минимизацию влияния человеческого фактора [4].

Обучение и повышение осведомлённости. Регулярные тренинги по кибербезопасности позволяют пользователям распознавать угрозы и реагировать на них корректным образом. Имитационные фишинговые атаки помогают выявлять слабые места в подготовке сотрудников и улучшать их кибер-грамотность.

Усиленная аутентификация. Использование многофакторной аутентификации (MFA) снижает риск несанкционированного доступа даже в случае компрометации паролей. Биометрическая идентификация и аппаратные ключи безопасности также являются эффективными инструментами защиты.

Технические меры защиты. Антивирусное ПО, системы предотвращения вторжений (IDS/IPS) и решения для мониторинга сетевой активности помогают обнаруживать и предотвращать атаки, связанные с социальной инженерией.

Контроль доступа и мониторинг поведения пользователей. Внедрение ролевой модели доступа (RBAC) позволяет ограничивать уровень привилегий сотрудников, снижая вероятность вредоносных действий. Поведенческий анализ пользователей с помощью машинного обучения помогает выявлять аномальные действия и предотвращать инсайдерские угрозы.

Культура кибербезопасности. Формирование у сотрудников и пользователей осознания важности защиты данных и ответственности за цифровую безопасность способствует снижению риска человеческих ошибок.

Заключение.

Человеческий фактор остаётся одним из наиболее уязвимых звеньев в кибербезопасности. Несмотря на технологические достижения в защите данных, ошибки пользователей, предсказуемость их поведения и социальная инженерия продолжают представлять серьёзную угрозу. Комплексный подход, включающий обучение, технические меры защиты и формирование культуры кибербезопасности, позволяет значительно снизить риски и повысить устойчивость цифровых систем к атакам. В условиях продолжающейся цифровой трансформации внимание к социальным аспектам кибербезопасности становится ключевым элементом защиты информации и цифровых активов.

Список литературы

1. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.
2. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2015. – p. 63 - EDN CMMEML.
2. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelec communications in science and education (APINO 2020). – 2020. – pp. 563-568.
3. Suvorov A.M., Tsvetkov A. Y. Investigation of buffer overflow attacks in 64-bit unix-like operating systems //Actual problems of infotelec communications in science and education (APINO 2018). – 2018. – pp. 570-573.

4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 72-76.
5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.