https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 35 | 2023

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

СОВРЕМЕННЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ: ВЫЗОВЫ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

Шарипова У. Б, Асс., Юлдашев О. И

Самаркандский филиал Ташкентского университета, информационных технологий имени Мухаммада ал-Хорезми

A R T I C L E I N F O.

Киберпреступность:
Киберпреступники Постоянно Совершают Атаки На Компьютерные Сети С Целью Получения Конфиденциальной Информации, Финансовой Выгоды Или Нанесения Ущерба. Это Включает В Себя Вредоносные Программы, Фишинг, Хакерские Атаки, Ddos-Атаки И Другие Формы Атак. Для Борьбы С Киберпреступностью Необходимо Регулярно Обновлять Программное Обеспечение, Использовать Сильные Пароли, Обучать Персонал В Области Кибербезопасности И Устанавливать Средства Защиты, Такие Как Брандмауэры И Антивирусные Программы.

Аннотация

Сетевая безопасность стала одной из главных проблем в современном цифровом мире. С развитием информационных технологий и увеличением сетевой связности возникли новые угрозы и риски для организаций и частных лиц. В данной статье мы рассмотрим современные угрозы сетевой безопасности и предложим рекомендации по защите.

Уязвимости программного обеспечения: Уязвимости в программном обеспечении являются основным каналом проникновения злоумышленников. Недавние случаи утечек данных и атак, связанных с уязвимостями, подчеркнули важность регулярного обновления программного обеспечения и установки патчей. Компании и пользователи должны следить за обновлениями и исправлениями безопасности от разработчиков программного обеспечения, а также использовать механизмы автоматического обновления, где это возможно.

Социальная инженерия: Социальная инженерия является эффективным методом манипулирования людьми для получения конфиденциальной информации. Злоумышленники могут использовать методы фишинга, обмана или поддельных запросов для получения доступа к системам или раскрытия информации. Важно обучать персонал, особенно тех, кто работает с конфиденциальными данными, о методах социальной инженерии и обеспечивать строгие политики аутентификации и авторизации.

Интернет вещей (IoT): С ростом числа подключенных устройств IoT возникают новые угрозы для сетевой безопасности. Недостаточная защита устройств IoT может привести к

компрометации сети и утечке данных. Рекомендуется использовать сильные пароли для устройств IoT, регулярно обновлять их программное обеспечение, отключать ненужные функции и использовать сетевые сегменты для изоляции устройств IoT от основной сети.

Анализ данных и приватность: Сбор и анализ больших объемов данных создают вопросы о приватности и защите личной информации. Компании и организации должны соблюдать соответствующие правила и регуляции, такие как GDPR, для обеспечения защиты данных пользователей и соблюдения их прав. Рекомендуется шифрование данных, установка контроля доступа и мониторинг использования данных.

Современные угрозы сетевой безопасности требуют постоянного внимания и принятия соответствующих мер безопасности. Обновление программного обеспечения, обучение персонала, использование средств защиты и соблюдение регуляций являются ключевыми факторами в защите от угроз. Организации и частные лица должны принять эти вызовы и принять меры для защиты своих сетей и данных от потенциальных атак.

Литературы:

1. https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security
2. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы. Современные тенденции технических наук: материалы Междунар. науч. Конф. — Уфа, 2011. — С. 8-13. — URL: moluch.ru/conf/tech/archive/5/1115/
3. Бабенко Г.В., Белов С.В. Анализ трафика TCP/IP на основе методики допустимого порога и отклонения // Инженерный вестник Дона, 2011, №2 URL: ivdon.ru/ru/magazine/archive/n2y2011/446
4. Factmonster.com. (2019). How Many Online Worldwide? URL: factmonster.com/science/computers-internet/how-many-online-worldwide/