Гаджиев Г.К. Методы обнаружения и предотвращения атак на мобильные устройства // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 10(48) с. 30–33

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

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 рассматриваются основные методы защиты мобильных устройств от киберугроз. Включены такие меры, как использование антивирусного ПО, регулярные обновления ОС и приложений, VPN, многофакторная аутентификация, проверка прав доступа приложений и обучение пользователей. Также описаны современные подходы, включая ИИ и машинное обучение, мониторинг сетевой активности, сетевая сегментация и обновление политик безопасности. Применение этих методов обеспечивает комплексную защиту данных и личной информации на мобильных устройствах.

Ключевые слова: Киберугрозы, мобильные устройства, безопасность, антивирус, VPN, многофакторная аутентификация, ИИ, машинное обучение.

METHODS FOR DETECTING AND PREVENTING ATTACKS ON MOBILE DEVICES

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 discusses the main methods of protecting mobile devices from cyber threats. Measures included include the use of antivirus software, regular OS and application updates, VPN, multi-factor authentication, checking application permissions and user training. Modern approaches are also described, including AI and machine learning, network activity monitoring, network segmentation, and updating security policies. The use of these methods provides comprehensive protection of data and personal information on mobile devices.

Keywords: Cyber threats, mobile devices, security, antivirus, VPN, multi-factor authentication, AI, machine learning.

Введение

С развитием технологий и расширением возможностей мобильных устройств увеличивается их уязвимость перед различными видами кибератак. В настоящее время мобильные устройства становятся основными средствами доступа к информации и проведения финансовых операций, что привлекает внимание киберпреступников. Для защиты данных и личной информации на мобильных устройствах разрабатываются различные методы обнаружения и предотвращения атак. В данной статье рассмотрим основные методы защиты мобильных устройств от киберугроз.

Использование антивирусного программного обеспечения

Один из наиболее распространенных методов защиты мобильных устройств - использование антивирусного программного обеспечения. Антивирусные приложения сканируют файлы и приложения на устройстве на предмет вредоносных программ и вирусов. Они также могут предотвращать установку вредоносного программного обеспечения, контролируя доступ к недоверенным сайтам и блокируя подозрительные ссылки.

Регулярное обновление операционной системы и приложений на мобильных устройствах является одним из наиболее важных методов защиты от киберугроз. Производители операционных систем и разработчики приложений регулярно выпускают обновления, в которых исправляют обнаруженные уязвимости и улучшают безопасность системы. Пользователи должны следить за обновлениями и устанавливать их как можно скорее.[1]

Виртуальные частные сети (VPN) обеспечивают шифрование интернет-соединения и защиту данных от перехвата. При использовании VPN данные, передаваемые между мобильным устройством и удаленным сервером, защищены от кибератак и прослушивания третьими лицами. VPN также позволяют обходить блокировки и ограничения доступа к интернет-ресурсам.

При установке новых приложений на мобильное устройство необходимо внимательно изучать запросы на предоставление различных прав доступа. Некоторые приложения могут запрашивать излишние или ненужные права, которые могут быть использованы для получения доступа к личной информации или выполнения вредоносных действий. Пользователи должны быть осмотрительны и отказывать в предоставлении прав, если это кажется им подозрительным.[2]

Многофакторная аутентификация - это метод защиты, при котором для доступа к устройству или приложению требуется не только пароль или пин-код, но и дополнительный фактор аутентификации, такой как отпечаток пальца, голосовое распознавание или код, отправленный на зарегистрированный телефон или электронную почту. Этот метод повышает безопасность доступа к устройству и защищает от несанкционированного доступа.

Важной составляющей безопасности мобильных устройств является обучение пользователей основам кибербезопасности и правилам безопасного поведения в сети. Пользователи должны быть осведомлены о возможных угрозах и уметь распознавать подозрительные признаки, такие как фишинговые письма, вредоносные ссылки и приложения. Обучение пользователей помогает снизить риск успешной атаки и повышает общий уровень безопасности мобильных устройств.

Для обнаружения аномального поведения и потенциальных угроз мобильной безопасности может быть полезным внедрение систем мониторинга сетевой активности на мобильных устройствах. Эти системы могут анализировать сетевой трафик и обнаруживать необычные или подозрительные активности, такие как попытки взлома, атаки перехвата данных или внедрение вредоносного программного обеспечения.

Современные системы безопасности все чаще используют методы искусственного интеллекта (ИИ) и машинного обучения (МО) для обнаружения и предотвращения кибератак на мобильные устройства. [3] Эти технологии могут анализировать большие объемы данных и выявлять аномалии, которые могут указывать на наличие угрозы безопасности. Например, системы ИИ и МО могут обнаруживать необычные попытки доступа к устройству, аномальные сетевые запросы или атаки фишингом.

Разработка и развертывание защищенных мобильных приложений является важным аспектом обеспечения безопасности мобильных устройств. Разработчики должны следовать передовым практикам безопасности программного обеспечения, таким как использование шифрования данных, проверка входных данных на предмет уязвимостей и регулярные аудиты безопасности приложений.[4]

Сетевая сегментация может помочь уменьшить потенциальные угрозы безопасности, разделяя сеть на отдельные сегменты и ограничивая доступ к чувствительным данным и ресурсам. Это позволяет изолировать потенциально компрометированные устройства от остальной части сети и предотвращать распространение атак на мобильные устройства на другие участки сети.

Регулярное обновление политик безопасности и процедур является важным аспектом обеспечения безопасности мобильных устройств. Организации должны периодически пересматривать свои политики и процедуры безопасности, учитывая новые угрозы и технологии. [5] Это позволит адаптироваться к изменяющейся угрозовой среде и улучшить защиту мобильных устройств.

Заключение

Обеспечение безопасности мобильных устройств является важной задачей в условиях роста числа киберугроз и увеличения объема цифровой активности. Для защиты данных и личной информации на мобильных устройствах используются различные методы обнаружения и предотвращения атак, такие как использование антивирусного программного обеспечения, регулярное обновление операционной системы и приложений, использование VPN, проверка прав доступа приложений, многофакторная аутентификация и обучение пользователей. Комплексное применение этих методов позволяет обеспечить надежную защиту мобильных устройств от киберугроз и повысить уровень безопасности в целом.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
2. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
3. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
5. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.

References

1. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 262-266.
2. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. - 2018. – No. 8. – pp. 91-97.
3. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. – 2020. – Vol. 12. – No. 4. – pp. 76-84.
4. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics "RI-2018". – 2018. – pp. 149-149.
5. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 266-270