УДК 004.056.53:004.056.57

БЕЗОПАСНОСТЬ СЕТЕВОГО ОБОРУДОВАНИЯ

Лещенко Е.А., Романюк М.В., Ласевич Е.В.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Алексеев В.Ф. – к.т.н., доцент, доцент кафедры ПИКС

Аннотация. В статье рассматриваются различные методы атак, которые могут привести к серьезным последствиям для организаций и пользователей, а также основные сетевые протоколы, их функции и уязвимости, которые могут быть использованы злоумышленниками для атак на сетевое оборудование. Также подчеркивается важность защиты сетевого оборудования и необходимость применения мер предосторожности для предотвращения киберугроз и обеспечения безопасности в цифровом мире.

Ключевые слова: сетевое оборудование, атака, уязвимость

Введение. В современном мире сетевое оборудование является критически важной частью любой инфраструктуры. От его бесперебойной работы зависит доступ к информации, сервисам и приложениям. В связи с этим, обеспечение безопасности сетевого оборудования становится все более актуальной задачей.

Основная часть. Современные киберугрозы могут привести к серьезным последствиям для организаций и частных лиц. В данном контексте необходимо рассмотреть различные методы атак, такие как фишинг, вредоносный код, DDoS атаки, уязвимости в программном обеспечении и социальная инженерия.

Фишинг – это метод атаки, при котором злоумышленники выдают себя за надежные источники для получения информации. Этот вид атаки может привести к серьезным последствиям, таким как потеря данных, финансовые убытки и репутационный ущерб.

Другой метод атаки – это вирусное программное обеспечение. Оно может нанести вред устройствам или сетям. Последствия таких атак могут быть разнообразными, включая потерю данных, финансовые потери и нарушение работы системы.

DDoS атаки направлены на перегрузку серверов, делая их недоступными для пользователей. Это может привести к недоступности ресурсов, потере доходов и клиентов.

Социальная инженерия является распространенным методом атаки, при котором хакеры манипулируют людей, чтобы получить доступ к конфиденциальной информации. Последствия могут быть серьезными, включая потерю конфиденциальных данных, финансовые потери и компрометацию безопасности.

Рансомвары блокируют доступ к данным или устройству и требуют оплаты выкупа. Последствия таких атак могут включать потерю доступа к данным, финансовые потери и простой бизнес-процессов.

Во втором квартале 2023 года число кибератак на российские ИТ-компании выросло в 4 раза по сравнению с аналогичным периодом 2022 года и достигло 4 тысяч [1]. Об этом сообщили в «МТС RED». Оценки Positive Technologies показывают утроение доли атак на ИТ-компании, достигнув 17%. В «Газинформсервисе» также отмечается рост атак на 20-25% при общем увеличении рынка на 10-15%. Центр мониторинга кибербезопасности «Лаборатория Касперского» указывает на сохранение ИТ-рынка в тройке наиболее уязвимых отраслей. В первом полугодии 2023 года количество кибератак выросло вдвое, но число инцидентов, критичных для бизнеса, сократилось на 20%. Наиболее атакуемыми отраслями стали информационные технологии (35%), промышленность (21%) и ритейл (15%). Высококритичные инциденты в основном относятся к телекоммуникационным компаниям (81%) и банкам (27%). Организации сферы услуг также стали чаще подвергаться атакам.

Сейчас активно применяется более десятка сетевых протоколов, каждый из которых имеет свою специфику и предназначение. Например, Ethernet используется для организации проводных сетей, а WLAN – для беспроводных. Существует несколько

специализированных протоколов, используемых для различных операций в сети [2]. Однако некоторые из них имеют уязвимости, которые могут быть использованы злоумышленниками для атак на сетевое оборудование.

ARP (Address Resolution Protocol) имеет уязвимость, связанную с невозможностью идентификации MAC-адреса. В одноранговых сетях отсутствует возможность определить, откуда идут данные, что позволяет хакерам связать свой MAC-адрес с IP пользователя и получить доступ к его трафику.

DNS (Domain Name System) позволяет преобразовывать IP-адреса в доменные имена. Хакеры могут провести атаку "отравления" кэша и изменить информацию об удаленном сервере, что может привести к перенаправлению пользователя на вредоносные сайты.

FTP (File Transfer Protocol) предназначен для передачи файлов, но не предусматривает шифрования соединения и данных для аутентификации, что делает перехват данных тривиально простым.

HTTP/S (Hypertext Transfer Protocol/Secure) обеспечивает безопасную передачу данных между пользователем и сайтом. Уязвимости в протоколе могут позволить злоумышленникам взломать шифрование и получить доступ к конфиденциальной информации.

POP3 (Post Office Protocol version 3) предназначен для работы с электронной почтой. Хакеры могут использовать атаку FireWire для получения доступа к электронным сообщениям.

Для эффективной защиты от атак, использующих эти протоколы, необходимо применить меры безопасности, такие как мониторинг сетевой активности, использование шифрования данных и аутентификации, регулярное обновление программного обеспечения сетевого оборудования и применение систем обнаружения вторжений.

В условиях постоянно возрастающей угрозы кибератак эффективная защита информационных ресурсов становится очень важной задачей. Рассмотрим основные методы защиты и их эффективность в противодействии разнообразным видам атак.

Антивирусное программное обеспечение предназначено для обнаружения и удаления вредоносных программ, таких как вирусы, троянские программы и черви.

Брандмауэры используются для контроля и фильтрации сетевого трафика, блокируя нежелательные подключения и предотвращая несанкционированный доступ к сети или устройствам, что эффективно защищает от DDoS атак и внедрения через уязвимости.

Патч-управление предполагает регулярное обновление программного обеспечения и операционных систем для устранения обнаруженных уязвимостей, что существенно снижает вероятность успешного внедрения через уязвимости и повышает уровень общей безопасности.

Многофакторная аутентификация (МФА) требует предъявления двух или более форм идентификации для подтверждения личности пользователя, что значительно повышает уровень защиты от фишинга, социальной инженерии и несанкционированного доступа.

Обучение и осведомленность пользователей включает в себя обучение основам кибербезопасности, что помогает снизить риск успешных социальных инженерных атак, а регулярные резервные копии данных являются важным методом защиты от рэнсомваров и других атак, блокирующих доступ к данным, обеспечивая быстрое восстановление работоспособности системы и данных.

Подход к защите от киберугроз должен быть комплексным и включать различные меры безопасности. Противодействие фишингу можно обеспечить путем регулярного обучения сотрудников, нацеленного на распознавание признаков фишинговых писем и сообщений. Также эффективным методом является внедрение систем фильтрации входящей почты, способных автоматически обнаруживать и блокировать подозрительные сообщения. Для дополнительного уровня защиты можно внедрить двухфакторную аутентификацию.

Противодействие вредоносному коду требует регулярного обновления антивирусного программного обеспечения и операционных систем. Также эффективно использовать программы для контроля целостности файлов, которые могут обнаруживать изменения в системных файлах, свидетельствующие о внедрении вируса.

Для противодействия DDoS атакам рекомендуется использовать услуги DDoS-защиты, предоставляемые хостинговыми провайдерами или специализированными компаниями. Также важно правильно сконфигурировать сетевое оборудование для фильтрации и блокирования атакующего трафика. Дополнительный уровень защиты можно обеспечить, используя облачные CDN (Content Delivery Networks) для распределения нагрузки и снижения уязвимости к DDoS атакам.

Противодействие внедрению через уязвимости предполагает регулярное сканирование сетевого оборудования и программного обеспечения на наличие уязвимостей. Быстрое обновление и исправление программного обеспечения для закрытия обнаруженных уязвимостей также является важным шагом.

Противодействие социальной инженерии включает обучение сотрудников распознавать и отвечать на социально-инженерные атаки. Внедрение политик безопасности информации, а также проведение регулярных проверок безопасности и аудитов, помогает выявить и устранить потенциальные уязвимости в системах безопасности.

Крайне важно выявить и перекрыть все пути доступа, по которым злоумышленники могли проникнуть в ваши системы [3]. Независимо от типа кибератаки, рекомендуется выполнить следующее: отключить зараженную сеть от интернета, отключить возможность удаленного доступа к сети, перенаправить сетевой трафик и сменить все уязвимые пароли.

Заключение. В заключение, защита сетевого оборудования и противодействие киберугрозам становятся все более важной задачей в современном мире. Различные методы атак, такие как фишинг, вредоносный код, DDoS-атаки, уязвимости и социальная инженерия, представляют серьезную угрозу для организаций и пользователей. Поэтому необходимо применять широкий спектр мер предосторожности, включая использование антивирусного программного обеспечения, брандмауэров, многофакторную аутентификацию, обучение пользователей и регулярные резервные копии данных. Кроме того, важно проводить анализ сетевых протоколов и устранять их уязвимости, чтобы предотвратить возможные атаки на сетевое оборудование. Только комплексный подход к кибербезопасности позволит эффективно защищать информацию и обеспечивать безопасность в цифровой среде.

Список литературы

1. *Число кибератак в России и в мире [Электронный ресурс]. – Интернет-портал TADVISER, 2024. – Режим доступа : https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире. – Дата доступа: 26.02.24.*

2. *Сетевая безопасность: что это такое? [Электронный ресурс]. – Банковско-финансовая телесеть – Режим доступа: https://www.bfn.by/rasprostranennye-uyazvimosti-i-ugrozy-v-sfere-setevoj-bezopasnosti/. – Дата доступа: 03.03.24.*

3. *Предотвращение кибератак [Электронный ресурс]. – Лаборатория Касперского, 2024 – Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks. – Дата доступа: 05.03.24.*

UDC 004.056.53:004.056.57

NETWORK EQUIPMENT SECURITY

Leshchenko E.A., Romaniuk M.V., Lasevich E.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alekseev V.F. – Cand. of Sci., associate professor, associate professor of the department of ICSD

Annotation. The article discusses various attack methods that can lead to serious consequences for organizations and users, as well as the main network protocols, their functions and vulnerabilities that can be used by attackers to attack network equipment. It also highlights the importance of protecting network equipment and the need to take precautions to prevent cyber threats and ensure security in the digital world.

Keywords: network equipment, attack, vulnerability.