УДК 004.056

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ И МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ

Коробская Е.С., студент гр. 21-К-КБ1, 4 курс,
Таран Е.А., ассистент кафедры,
Шарай В.А., к.т.н., доцент
Научный руководитель: Шарай В.А., к.т.н., доцент
Кубанский государственный технологический университет
г. Краснодар

VPN – это виртуальная частная сеть, которая используется для обеспечения защищенного подключения к сети. В современном мире виртуальные частные сети стали неотъемлемой частью инфраструктуры многих организаций и индивидуальных пользователей, обеспечивая защиту передаваемых данных, скрытие IP-адреса, обход географических ограничений, надежный канал связи и доступ к ресурсам через интернет. Однако, несмотря на все преимущества, VPN подвержены различным угрозам безопасности, которые могут привести к серьёзным последствиям, включая утечку конфиденциальной информации, атаки на протоколы шифрования, перехват трафика и эксплуатацию уязвимостей серверных инфраструктур, а также нарушение работы критически важных систем.

Основные современные угрозы безопасности VPN:

1. Атаки «человек посередине» (Man-in-The-Middle, MITM).

Это вид кибератак, при котором злоумышленник внедряется в канал связи между двумя сторонами, участвующими в обмене данными, и перехватывает, изменяет или фальсифицирует информацию, передаваемую между ними. Атака MITM в VPN заключается в том, что нарушитель устанавливает соединение с одной или обеими сторонами, участвующими в VPN-соединении, и выдает себя за легитимного участника. В некоторых случаях правонарушитель может создать поддельное VPN-соединение, чтобы заставить пользователей подключиться к нему и передать свои данные.

Возможные векторы атаки:

– использование фальшивых сертификатов безопасности и перенаправление трафика через поддельный сервер;

– DNS-спуфинг, при котором злоумышленник изменяет DNS-запросы, перенаправляя жертву на поддельные сайты;

– подмена шлюза в сети, позволяющая злоумышленнику прослушивать весь трафик.

Основные способы защиты от атак MITM в VPN представлены на рисунке 1 [2].

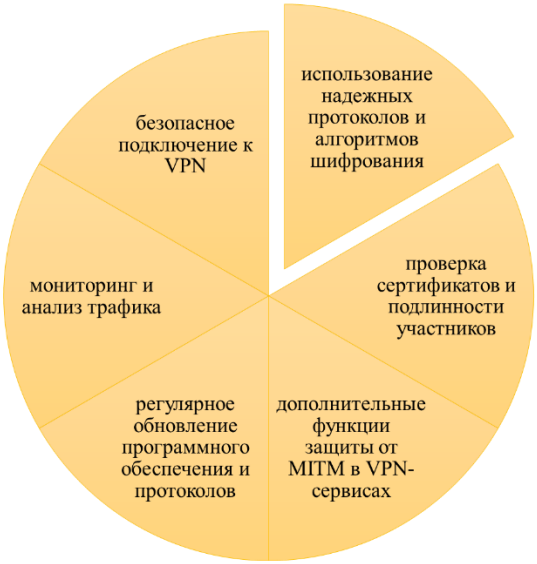

Рисунок 1. – Способы защиты от атак MITM в VPN

2. Уязвимости в протоколах VPN.

Уязвимости в протоколах VPN представляют собой слабые места в механизмах шифрования и аутентификации, используемых в виртуальных частных сетях. Они могут быть использованы злоумышленниками для перехвата, подмены или изменения передаваемых данных, что ставит под угрозу конфиденциальность и целостность информации.

Некоторые устаревшие или неправильно настроенные протоколы VPN подвержены взлому с использованием инструментов дешифрования. Например, протокол PPTP (Point-to-Point Tunneling Protocol) давно признан небезопасным из-за использования слабых алгоритмов аутентификации. L2TP/IPSec при некорректной настройке также может быть уязвимым к атакам перебора паролей. OpenVPN и WireGuard считаются безопасными, но требуют регулярного обновления и правильной конфигурации.

Возможные векторы угрозы:

– использование устаревших алгоритмов шифрования, например, MD5 и SHA-1 считаются небезопасными и могут быть скомпрометированы;

– атака «человек посередине» (Man-in-the-Middle, MITM);

– атака на протоколы аутентификации (использование слабых или статических паролей упрощает правонарушителям взлом учетных записей);

– компрометация ключей шифрования.

К способам защиты от уязвимости в протоколах VPN, помимо способов, перечисленных на рисунке 1, также относятся:

– шифрование ключей и управление ими;

– использование систем обнаружения вторжений (IDS/IPS).

3. Утечки DNS и IP-адресов в виртуальных частных сетях (VPN).

DNS (система доменных имён) — это распределённая система, которая преобразует доменные имена в IP-адреса и наоборот, обеспечивая идентификацию и доступ к сетевым ресурсам.

Некорректная конфигурация VPN может привести к утечке данных о реальном IP-адресе пользователя, а также его DNS-запросов, что позволяет тре-

тьим сторонам отслеживать активность. Данная проблема особенно актуальна при использовании VPN в корпоративных сетях и при обходе географических блокировок.

Возможные векторы угрозы:

– перехват и анализ трафика сети;

– эксплойты и уязвимости в VPN-клиентах и серверах;

– внедрение вредоносного кода в передаваемые данные, к примеру, вирусы, трояны, шпионское ПО и руткиты;

– манипулирование DNS-запросами и перенаправление пользователя на поддельные сайты в случае использования ненадежных сетей и неправильной настройки VPN;

– запись IP-адреса пользователей и их поведение в сети;

– атаки на серверы VPN, такие как фишинг и социальная инженерия, DDoS-атаки и атаки на доверенные узлы [3].

Основные способы защиты от утечек DNS и IP-адресов:

– использование надежных VPN-сервисов с проверенной репутацией;

– использование надежных DNS-серверов, таких как Cloudflare DNS или Google Public DNS;

– настройка VPN-клиентов в соответствии с рекомендациями производителя;

– установка и регулярное обновление антивирусного ПО;

– использование надёжных паролей и двухфакторной аутентификации;

– избегание использования ненадёжных публичных Wi-Fi сетей для доступа к конфиденциальной информации;

– проверять логи VPN-клиента и сервера на наличие подозрительной активности, проводить аудит безопасности сети;

– обучение сотрудников и пользователей основам кибербезопасности.

4. Эксплойты и вредоносное ПО.

Эксплойты – это программные коды или инструменты, которые используют уязвимости в программном обеспечении или оборудовании для выполнения несанкционированных действий. Эксплойты могут быть использованы для обхода мер безопасности, перехвата данных или внедрения вредоносного кода в сеть. Вредоносное ПО – это программное обеспечение, разработанное с целью нанесения вреда компьютерным системам, сетям или получения несанкционированного контроля над устройством.

Возможные векторы угрозы:

– уязвимости в VPN-протоколах (OpenVPN, IPSec или WireGuard), которые могут позволить расшифровать трафик;

– уязвимости в серверном ПО;

– атаки на шифрование, когда используются устаревшие алгоритмы шифрования (MD5, SHA-1);

– атаки на сетевую инфраструктуру;

– фальшивые VPN-клиенты, то есть хакеры могут распространять зараженные версии популярных VPN-сервисов;

– фишинговые атаки.

Основные способы защиты от эксплойтов и вредоносного ПО:

– мониторинг уязвимостей с помощью сканеров безопасности (Nessus, OpenVAS);

– ограничение доступа, то есть настройка VPN таким образом, чтобы доступ к сети имели только доверенные IP-адреса;

– использование антивирусов и системы EDR (Endpoint Detection & Response);

– фильтрация трафика;

– цифровая подпись обновлений.

5. Атаки на серверы VPN.

Атаки на серверы VPN – это попытки злоумышленников получить несанкционированный доступ к серверам виртуальных частных сетей (VPN) с целью нарушения их работы, кражи данных или использования инфраструктуры VPN для других преступных действий.

Основные виды таких атак представлены на рисунке 2.

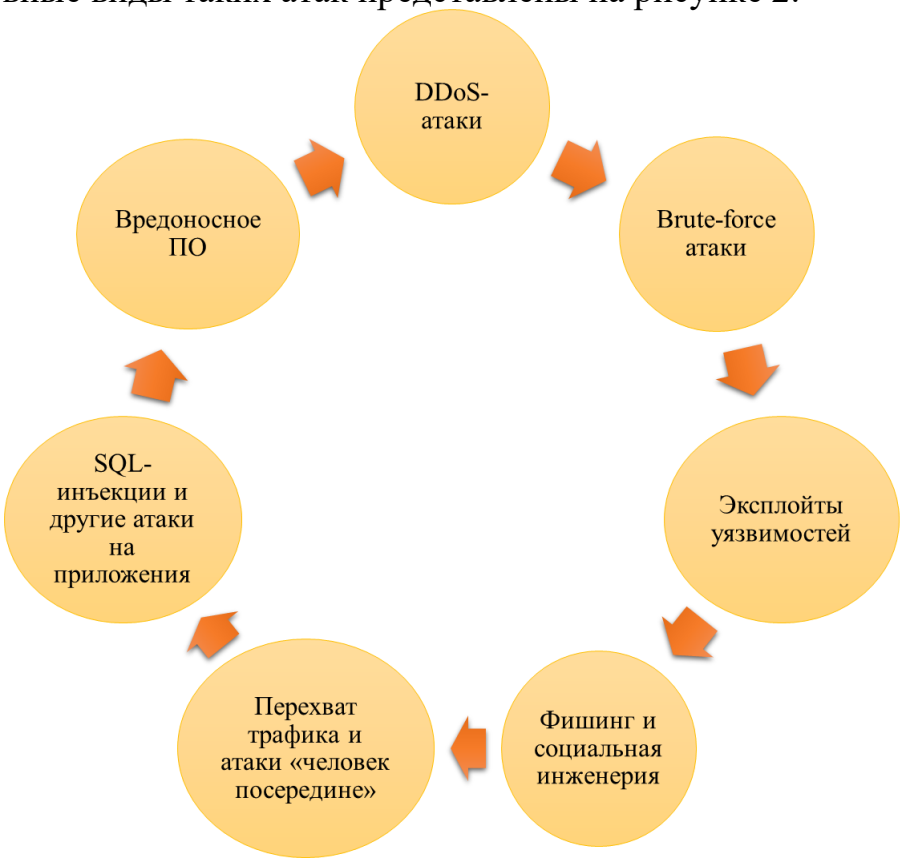

Рисунок 2. – Виды атак

Основные способы защиты от атаки на серверы VPN:

– настройка брандмауэров и других средств защиты для блокировки подозрительного трафика;

– мониторинг и анализ логов сервера VPN для выявления необычных паттернов;

– использование надежных методов шифрования для защиты трафика между клиентами и сервером;

– ограничение доступа к VPN.

Для обеспечения безопасности виртуальных частных сетей необходимо не только выявлять и анализировать угрозы, но и принимать активные меры по их предотвращению. Рассмотрим подробнее некоторые методы и технологии, которые могут быть использованы для защиты виртуальных частных сетей от современных угроз безопасности [4].

1. Использование современных и надежных протоколов и алгоритмов шифрования.

OpenVPN, который использует шифрование AES-256 и протокол TLS для защиты данных. WireGuard обеспечивает высокую скорость и надежность за счет использования современных криптографических алгоритмов. IKEv2/IPSec поддерживает защиту данных при изменении сетевого подключения и обеспечивает высокий уровень безопасности. Цифровые подписи (RSA, ECDSA) также необходимы для защиты данных от изменения и подделки.

2. Многофакторная аутентификация (MFA).

Для повышения уровня безопасности необходимо использовать парольную защиту, одноразовые коды (TOTP, SMS, аппаратные токены) и биометрическую аутентификацию. MFA значительно усложняет возможность несанкционированного доступа к VPN даже в случае компрометации учетных данных.

3. VPN-шлюзы и VPN-концентраторы.

Данные устройства используются для организации защищенного удаленного доступа к корпоративной сети. VPN-шлюзы обеспечивают шифрование передаваемых данных и аутентификацию пользователей, что препятствует перехвату информации злоумышленниками. VPN-концентраторы предназначены для управления множеством VPN-соединений, обеспечивая масштабируемость и отказоустойчивость удалённого доступа.

4. Системы обнаружения и предотвращения вторжений (IDS/IPS).

IDS (Intrusion Detection System) выявляет подозрительную активность, анализируя сигнатуры атак, аномалии поведения или граничные показатели трафика. IPS (Intrusion Prevention System) не только обнаруживает, но и блокирует угрозы, например, срабатывая на DDoS-атаки или попытки эксплуатации уязвимостей.

5. Виртуальные локальные сети (VLAN).

VLAN используется для сегментации сети, что ограничивает распространение вредоносного трафика, а также улучшают управление сетью и позволяют применять разные политики безопасности к различным сегментам.

6. Обновление ПО и патчинг.

Регулярное обновление операционных систем, сетевых устройств, серверов и клиентского ПО помогает закрывать известные бреши в безопасности. Разработчики постоянно выпускают патчи безопасности, исправляющие обнаруженные уязвимости. Использование централизованных систем управления обновлениями (WSUS, SCCM, Ansible, Chef) упрощает этот процесс.

7. Межсетевые экраны (Firewall).

Файрволы анализируют и фильтруют сетевой трафик в соответствии с заданными правилами. Современные NGFW (Next-Generation Firewall) дополнительно используют механизмы глубокой инспекции трафика (DPI) и интеграцию с системами предотвращения атак.

8. Защита от утечек DNS и IP-адресов.

Использование защищенных DNS-серверов (Cloudflare DNS, Google Public DNS), включение функции защиты от утечек DNS (DNS Leak Protection) и применение Kill Switch, который автоматически разрывает соединение при сбое VPN позволяют предотвратить утечки данных.

9. Обнаружение и предотвращение атак типа «человек посередине» (MITM).

Использование строгой проверки сертификатов безопасности и надежных подключений к сети, включение механизмов защиты от подмены шлюзов и DNS-спуфинга и применение TLS для защиты и передачи данных обеспечивают необходимую защиту VPN от данного типа атаки.

Таким образом, можно сделать вывод, что обеспечение безопасности VPN требует комплексного подхода, включающего в себя как технические, так и организационные меры. Только такой подход позволит эффективно противостоять современным угрозам и обеспечить надёжную защиту данных в виртуальных частных сетях.

Список литературы:

1. Пролетарский А.В. Беспроводные сети Wi-Fi: учебное пособие / Пролетарский А.В., Баскаков И.В., Федотов Р.А. и др. – 2-е изд. – Москва: ИНТУИТ, 2016. – 284 с.

2. Прытков В.А., Быстров Е.Д. Анализ современных угроз информационной безопасности и конфиденциальной информации в информационных системах с учётом динамичной киберугрозовой среды // Современные научные исследования и инновации. – 2023. – № 9. – URL: https://web.snauka.ru/issues/2023/09/100797.

3. Ланецкая А.Ю., Александрова Е.Н. Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. – 2022. – № (7-2). – С. 192-195.

4. Кибербезопасность в современном мире: актуальные угрозы и методы защиты [Электронный ресурс]. – URL: https://www.arsis.ru/blog/cyber-security.