Мереуца Дмитрий Павлович
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации

Сидоренко Иван Дмитриевич
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации

Дидилика Евгений Ренатович
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации

Кузьмич Александр Александрович
Кандидат технических наук
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ОБЕСПЕЧЕНИЯ УДАЛЕННОГО КОНТРОЛЯ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ VPN

Аннотация. В статье рассматриваются актуальные проблемы обеспечения безопасности виртуальных частных сетей (VPN) в условиях роста числа удаленных подключений. Проанализированы ключевые угрозы, связанные с удаленным доступом. Предложена архитектура системы удаленного контроля параметров информационной безопасности VPN, включающая модули сбора данных, корреляции событий и визуализации. Определен перечень критически важных для мониторинга параметров, таких как состояние туннелей, аутентификация пользователей и активность сетевых интерфейсов. Разработаны практические предложения по реализации системы контроля, позволяющие осуществлять проактивное выявление инцидентов безопасности и повышать общую устойчивость корпоративной ИТ-инфраструктуры.

Ключевые слова: VPN, информационная безопасность, удаленный контроль, мониторинг, SIEM, киберугрозы, туннелирование.

Введение

Современная бизнес-среда характеризуется повсеместным распространением удаленных форматов работы, что обуславливает критическую важность технологий виртуальных частных сетей (VPN). VPN обеспечивает защищенный канал для передачи данных между удаленными пользователями и корпоративной сетью. Однако сама инфраструктура VPN становится привлекательной мишенью для злоумышленников, а ее уязвимости или некорректная настройка могут привести к компрометации всей корпоративной информационной системы.

Традиционные подходы к управлению VPN часто ограничиваются первоначальной настройкой и реактивным устранением неисправностей. Недостаточное внимание к непрерывному мониторингу и анализу параметров безопасности в реальном времени создает значительные риски. В связи с этим разработка комплексных предложений по обеспечению удаленного контроля параметров информационной безопасности VPN является своевременной и научно-практической задачей.

1. Анализ угроз безопасности удаленных VPN-подключений

Основными угрозами для VPN-инфраструктуры являются атаки на протоколы шифрования, подбор учетных данных, эксплуатация уязвимости в программном обеспечении, а также атаки типа «человек посередине». Отсутствие непрерывного контроля усугубляет последствия этих угроз.

Для организации эффективного противодействия необходима система, способная в режиме 24/7 отслеживать ключевые метрики. К таким метрикам относятся: количество активных туннелей, частота и исход попыток аутентификации, подозрительная сетевая активность (например, сканирование портов), а также соответствие конфигураций установленным политикам безопасности.

Категория параметра Конкретный параметр Цель мониторинга

Состояние подключений Количество активных туннелей, длительность сессии, объем переданных данных Выявление аномальной активности, DDoS-атак

Аутентификация Число неудачных попыток входа, повторные подключения с одного аккаунта Обнаружение брут-форс атак и компрометации учетных записей

Сетевая активность Нестандартные порты, подозрительные IP-адреса, аномальные протоколы Выявление сканирования и попыток эксплуатации уязвимостей

Конфигурация Версия ПО, настройки шифрования, актуальность обновлений Обеспечение соответствия политикам безопасности

2. Архитектура системы удаленного контроля безопасности VPN

Предлагаемая архитектура системы контроля строится на модульном принципе и включает три основных компонента: агенты сбора данных, центральный сервер обработки и модуль визуализации с системой оповещений.

Агенты сбора данных размещаются на VPN-шлюзах и серверах аутентификации. Их задача – сбор логов и системных метрик. Центральный сервер, выполняющий функции системы SIEM (Security Information and Event Management), осуществляет прием, нормализацию и корреляцию событий от всех источников. На этом этапе применяются правила и алгоритмы для выявления сложных, распределенных во времени атак. Модуль визуализации предоставляет администратору информативную панель управления (dashboard) для наблюдения за текущим состоянием безопасности.

3. Практические предложения по реализации контроля

На основе предложенной архитектуры сформулированы практические рекомендации по реализации.

1. Внедрение централизованного сбора логов. Необходимо настроить перенос логов со всех VPN-шлюзов (например, на базе решений Cisco ASA, FortiGate, OpenVPN) в централизованное хранилище. Это обеспечит единую точку анализа.

2. Разработка правил корреляции. На центральном сервере SIEM должны быть созданы правила, например: «Более 5 неудачных попыток аутентификации с одного IP-адреса в течение 2 минут» или «Установление VPN-подключения из географически нехарактерного местоположения».

3. Создание панели мониторинга. Панель должна визуализировать ключевые показатели эффективности (KPI) безопасности: карту подключений в реальном времени, график попыток аутентификации (успешных/неуспешных), список активных инцидентов.

4. Настройка системы оповещений. Критические события, такие как множественные неудачные аутентификации или остановка VPN-сервиса, должны немедленно передаваться администратору через каналы мгновенных сообщений (Telegram, Slack) или электронную почту.

Реализация данных предложений позволяет перейти от реактивной к проактивной модели безопасности, когда инциденты выявляются на ранних стадиях, а не после наступления негативных последствий.

Заключение

В ходе исследования была обоснована необходимость внедрения систем непрерывного удаленного контроля для VPN-инфраструктуры. Разработанная архитектура и практические предложения позволяют комплексно подойти к решению проблемы мониторинга безопасности удаленных подключений.

Ключевым преимуществом предложенного подхода является его масштабируемость и адаптивность. Система может быть доработана для учета специфики конкретной организации и интегрирована с другими подсистемами безопасности. Дальнейшие исследования целесообразно направить на разработку интеллектуальных алгоритмов анализа поведения пользователей (UEBA) для более точного выявления аномалий, не описываемых статичными правилами корреляции.

Список литературы:

1. Щербаков А.Ю. Современные угрозы безопасности виртуальных частных сетей // Труды института системного программирования РАН. – 2021. – Т. 33, № 4. – С. 155-170.

2. Романова С.В., Козлов Д.А. Методы и средства защиты информации в корпоративных сетях. – М.: Издательский дом «Альянс», 2022. – 320 с.

3. Cisco Systems. Cisco ASA Series CLI Configuration Guide, 2023. – URL: https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-book.html

4. NIST Special Publication 800-46 Revision 2. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, 2023.

5. OpenVPN Technologies Inc. OpenVPN Administration Guide, 2023. – URL: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/