УДК 004.056

С.В. МОНХ
Научный руководитель – Д.А. ДЯТЛОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРОТИВОДЕЙСТВИЕ МЕТОДАМ ОБХОДА МЕЖСЕТЕВЫХ ЭКРАНОВ

Цель исследования – разработка рекомендаций по противодействию методам обхода межсетевых экранов. Для достижения этой цели проведена классификация методов обхода, проведено исследование средств и техник, используемых злоумышленниками, и разработаны практические рекомендаций по противодействию методам обхода межсетевых экранов.

Сетевые угрозы в современном мире становятся всё более сложными, и традиционные защитные механизмы, такие как межсетевые экраны, требуют постоянного обновления и адаптации [1]. Цифровизация и глобальная взаимосвязанность сетей создают новые вызовы для информационной безопасности. Межсетевые экраны выступают барьером между внутренними сетями организаций и внешним миром, фильтруя входящий и исходящий трафик. Однако злоумышленники находят способы обойти эту защиту, используя как технические уязвимости, так и психологические методы, такие как социальная инженерия. В исследовании произведен анализ методов обхода межсетевых экранов, который разделён на две основные категории: технические и нетехнические методы.

Технические методы включают: эксплойты, туннелирование, полиморфное и метаморфное ПО, шифрование и стеганографию.

Нетехнические методы включают социальную инженерию и фишинг. Злоумышленники могут использовать обманные письма или поддельные сайты для того, чтобы получить доступ к сетям. Эти методы часто оказываются эффективными, так как многие пользователи недостаточно осведомлены о существующих киберугрозах и рисках.

Был проведен анализ программных и аппаратных средств обхода.

Среди программных средств, активно используемых злоумышленниками, выделяются Tor, OpenVPN, PuTTY, Proxifier и Psiphon. Эти программы позволяют обходить межсетевые экраны путём маскировки трафика, шифрования данных или создания туннелей [2].

Каждая из этих программ имеет свои особенности и сценарии использования, однако все они могут быть использованы для обхода

стандартных защитных механизмов. Это требует от организаций внедрения более сложных методов обнаружения, таких как глубокий анализ пакетов (DPI), который способен идентифицировать аномалии в зашифрованном трафике.

Кроме программных средств, злоумышленники могут использовать аппаратные решения, такие как Raspberry Pi или Wi-Fi Pineapple. Эти устройства позволяют создавать скрытые туннели или перехватывать беспроводной трафик. Например, Raspberry Pi может быть использован для установки VPN-сервера внутри корпоративной сети, что делает трафик незаметным для стандартных межсетевых экранов.

Были перечислены и методы сокрытия трафика: стеганография и шифрование, туннелирование через протоколы HTTPS или DNS,

Для повышения безопасности межсетевых экранов предложено внедрение следующих мер: глубокий анализ пакетов (DPI), регулярное обновление ПО, многофакторная аутентификация (MFA), сегментация сети [3].

Также следует подчеркнуть важность обучения персонала. Зачастую человеческий фактор является слабым звеном в системе безопасности, и злоумышленники используют это с помощью методов социальной инженерии. Повышение осведомлённости сотрудников и регулярные тренинги помогут снизить риск успешных атак.

В условиях постоянно развивающихся киберугроз, важно использовать как технические, так и организационные меры для повышения уровня защиты сетей. Разработанные в ходе исследования рекомендации, такие как внедрение DPI, сегментация сети и регулярное обновление ПО, помогут организациям эффективно противостоять современным атакам и снизить риск компрометации их информационных систем.

Список литературы

1. Евтеев Д. О. Методы обхода Web Application Firewall [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/download/PT-devteev-CC-WAF.pdf (дата обращения: 08.06.2024).

2. Методы обхода межсетевых экранов для приложений / В.Г. Мельников, А.В. Трифанов // Интерэкспо Гео-Сибирь. – 2017. – Т. 9, № 2. – С. 113–117 (дата обращения: 08.06.2024).

3. Методы обхода межсетевых экранов / Д.А. Украинцева, В.Г. Бурлов // Информационные технологии в образовании: Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 31 марта 2021 года / Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. – Санкт-Петербург: Российский государственный гидрометеорологический университет, 2021. – С. 97–101 (дата обращения: 09.08.2024).