ФИЛЬТРАЦИЯ ТРАФИКА СОЦИАЛЬНЫХ СЕТЕЙ (VIBER И ДР.) В СЕТИ УЧЕБНОГО ЗАВЕДЕНИЯ

Хожевец О.А.[1], Ткачева А.В.[2]

[1] *УО«БГУИР», г. Минск, Беларусь, a.dmitrenko@bsuir.by;*
[2] *НИИ ВСРБ, г. Минск, Беларусь, a.dmitrenko@bsuir.by*

Abstract. The problem of using social networks during work or school hours is analyzed. The need to restrict access to various network resources is considered. The paper analyzes the filtering of social network traffic: filtering methods, identifying the advantages and disadvantages of filtering. Much attention is paid to the comparison of the Squid proxy server with free software and the paid integrated solution Ideco ICS.

Появление сети Интернет кардинально изменило все сферы жизни людей. Данная система представляет собой хранилище разнообразной информации и сервисов. При этом часто возникает необходимость ограничения доступа к различным ресурсам сети. Это связано, во-первых, с нерациональной тратой времени, предназначенного для работы или для обучения, во-вторых, с желанием работодателя оптимизировать деятельность своих сотрудников, а также руководителей учебного заведения ограничить студентов от нежелательного контента на время проведения занятий.

В связи с обозначенной проблемой рассмотрим фильтрацию трафика социальных сетей в корпоративной сети и в частности в учебном заведении.

Оптимизация использования сетевых ресурсов занимается системный администратор корпоративной сети. Здесь можно выделить несколько основных проблем, с которыми он сталкивается в своей работе:

- чрезмерная нагрузка на сеть, обусловленная неконтролируемым скачиванием сотрудниками больших файлов из глобальной сети;
- нерациональное использование ресурсов, которое предполагает, что работники или студенты проводят большое количество времени в социальных сетях не в рабочих или учебных целях, а в личных интересах;
- снижение уровня безопасности сети предприятия, так как очень часто внутренние ресурсы и данные компании являются объектом угроз и рисков при отсутствии полноценного контроля за посещением сотрудниками сайтов той или иной тематики.

Проблема использования социальных сетей в рабочее или учебное время является на сегодняшний день актуальной для многих организаций. Проведенные исследования компании Palo Alto Networks , показывают, что использование Twitter увеличивается в год на 700 % в том числе и за счет использования на рабочих местах. При этом Ведомости со ссылкой на The Financial Times приводят цифру - 1,4 млрд фунтов, именно такой убыток несут британские компании из-за своих сотрудников, которые проводят значительную часть своего рабочего времени в социальных сетях [1].

В нашей стране данная проблема не менее остра, так Ведомости со ссылкой на исследование Kelly Services отмечают, что у белорусов и россиян показатель использования интернета в личных целях самый высокий в Европе.

Необходимо отметить тот факт, что ключевой основой данной проблемы является не только нерациональная трата времени сотрудников и студентов, но также и другой не менее важный аспект. Социальные сети стали объектом интересов злоумышленников, как удобная среда для сбора данных о корпоративном сегменте методом социальной инженерии. Пользователь – это одно уязвимое звено, он неумышленно становится источником раскрытия сведений о компании, которые в дальнейшем могут быть использованы злоумышленниками. Метод социальной инженерии является одним из основных принципов, на котором строятся APT (advanced persistent threat) атаки.

В связи с этим многие организации, в числе которых и бизнес-компании, и учебные заведения, принимают меры для ограничения доступа к социальным сетям своих сотрудников и студентов на время, отведенное для трудовой деятельности.

Существует множество различных методов. Некоторые организации выбирают полный запрет на доступ к социальным сетям. Однако, данный метод не всегда эффективен, так как сказывается на невозможности использования этого активно растущего сегмента сети Интернет, например, в маркетинговых целях.

Поэтому одним из вариантов решения проблемы является фильтрация трафика. Фильтрация трафика подразумевает собой основную функцию систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находящимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети [2].

Есть несколько способов фильтрации трафика социальных сетей, среди которых:

- прокси-серверы и программы, разрешающие или блокирующие доступ к определенным сайтам и протоколам;
- программы для фильтрации контента, которые находят и блокируют определенный контент;
- параметры конфигурации, которые задают уровень конфиденциальности и мониторинга сайтов (например, фильтр Google SafeSearch, Privolock) [3].

Одним из основных методов фильтрации трафика социальных сетей является внедрение специальных прокси-серверов. В ходе исследования бы-

ли рассмотрены прокси-сервер Squid и программное решение Ideco ICS.

Squid – это высокопроизводительный кэширующий прокси-сервер. В его основе лежит гибкая система фильтрации внешних ссылок. Она построена на возможности заблокировать доступ к определенным ресурсам, избавить от нежелательной рекламы, всплывающих окон и т.д. Для этого задаются определенные настройки. Он может быть установлен как в отдельной организации, так и в корпоративной сети.

Таким образом, основные достоинства прокси-сервера Squid – это:

− возможность ограничить определенный контент, в том числе нежелательную рекламу, всплывающие окна и т.д.;

− пакетная фильтрация и фильтр протоколов/приложений;

− управление пропускной способностью.

Следующее комплексное программное решение для фильтрации трафика социальных сетей – это Ideco ICS. В основе данного прокси-сервера лежит операционная система Linux и большое число различных компонентов, более 30, задача которых оперативно справляться с любыми проблемами по управлению трафиком: от маршрутизации до шифрования и балансировки нагрузки. Ideco ICS способствует быстрому и эффективному выполнению многих рутинных процессов сетевого администрирования, в связи, с чем общий уровень защищенности и управляемости работы в Интернете возрастает во много раз. Данное программное решение позволяет одновременно решить три проблемы, актуальные для любой корпоративной сети, как в бизнес сектора, так и в образовательном учреждении, это: эффективность; безопасность; надежность.

Ideco ICS является достаточно эффективным средством борьбы с нерациональным использованием сети Интернет в рабочее или учебное время. С помощью него возможно ограничить доступ к социальным сетям в короткий промежуток времени. При этом есть возможность установить ограничения как для определенных сотрудников, так и для конкретных отделов компании. По результатам использования Интернета за выбранные промежутки времени можно сформировать отчет со статистикой посещаемых ресурсов, необходимый для дальнейшего принятия эффективных управленческих решений.

В тоже время фильтрация трафика не эффективна на все 100%. У нее сеть два характерных недостатка: недостаточная и избыточная блокировка. Под недостаточной блокировкой понимается неспособность заблокировать доступ ко всему целевому контенту. С другой стороны технологии фильтрации часто блокируют контент, который они не должны блокировать, что называется избыточным блокированием. Оба указанных недостатка появляются вследствие создания множества «черных» списков с использованием сочетания ручных настроек и автоматизированных поисковых систем, которые часто содержат веб-сайты, классифицированные неправильно. Дополнительные проблемы возникают, когда контент размещается под тем же IP-адресом или в том же домене. Более того, методы фильтрации не удаляют незаконное содержимое из Интернета, и их зачастую можно обойти. Они также могут случайным образом ограничить свободное и открытое общение и тем самым ограничить права отдельных людей или групп меньшинств.

Далее обратимся к анализу одной из часто используемых социальных сетей Вайбер. К нему в последнее время особенно широк интерес, как источнику трафика, что неудивительно, ведь компания позиционирует себя как глобальный оператор связи с аудиторией 249 млн. активных пользователей ежемесячно. В 2018 компания выпустила 2 значимых обновления: создание сообществ в вайбере и публичные аккаунты.

Украина, Республика Беларусь и Таджикистан безусловно увлечены таким «лайт-стайл» мессенджером, где он составляет выбор до 90% пользователей в сегменте, в России, конечно, в лидеры выдвигается WhatsApp, хотя разрыв невелик 30% против 27% по количеству упоминаний. При этом, как правило, на смартфоне у человека стоят оба приложения, но, если у одного имеется приоритет, второй используется лишь опционально. Деление продиктовано и качеством работы мессенджера в зоне охвата.

Таким образом, существуют различные способы фильтрации трафика социальных сетей, например зеркальная технология, DNS-блокировка, блокировка по URL. Одни из них более эффективны, другие менее, но ни один из способов не является эффективным на 100%.

Анализируя результаты исследования, необходимо отметить, что современные программные решения на сегодняшний день могут ограничивать доступ к различным сайтам, но не существует такой фильтрации, которая была бы абсолютно эффективной и надежной. В современных реалиях это оказывается не так просто сделать, из-за того, что сегодня существует множество путей для обхода реализованных ограничений, среди которых: различные прокси-сервера, сайты зеркала или анонимайзеры, а также более продвинутые средства обхода, например, TOR.

Литература

1. Емельянов Д.А. Фильтрация сетевого контента в образовательных учреждениях // Информационно-коммуникационные технологии в образовании. 2018. С. 75-82.

2. Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Научно-методический электронный журнал «Концепт». 2015. №2 (февраль). С. 71–75.

3. Средства и методы фильтрации контента в интернете [Электронный ресурс]. — Режим доступа: https://sites.google.com/site/metodyblokirovkinezelanojinfor/sredstva-i-metody-filtracii-kontenta-v-internete — Дата доступа: 22.03.2021.