УДК 004.424 EDN CWPRMI

Атаки в сети: способы борьбы с сетевыми атаками

Ю.А. Кравченко

Донской государственный технический университет, пл. Гагарина, 1, Ростов-на-Дону, 344000, Россия

E-mail: yuliakravchenkooo@gmail.com

Аннотация. Атаки в сети сегодня встречаются так часто, что любой пользователь имеет представление о них. Видов атак множество, целью их является кража какой-либо информации. Каждый пользователь должен владеть руководством по максимальной защите своего персонального компьютера, который подключен к сети, и личных данных, которые находятся на персональном компьютере. Информационные технологии плотно вошли в жизнь каждого человека, также в любой производственный процесс. Ни один вид деятельности не обходится без цифровых инновационных технологий, основанных на искусственном интеллекте. Неразделимой частью компьютера является сеть Интернет, через которую и осуществляется атака на данные пользователя. В данной статье рассмотрим виды сетевых атак, методы борьбы с ними. Рассмотрим методы, как обезопасить себя и свои данные в сети при пользовании Интернетом. На сегодняшний день имеется множество программ, которые относятся к вирусным, и участник сети, пользуясь ею, не подозревает, что его личные данные, его страница и привязанные к ней знакомые пользователи могут пострадать от кибератаки. Рассмотрим различные виды программ, через которые могут осуществляться атаки в сети, приведем методы их обхода и борьбы с ними.

Ключевые слова: информационная безопасность, атаки в сети, вирусные программы, кража данных, сеть Интернет.

Network attacks: ways to combat network attacks

Y.A. Kravchenko

Don State Technical University, Gagarin Square, 1, Rostov-on-Don, 344000, Russia

E-mail:yuliakravchenkooo@gmail.com

Abstract. Attacks on the network are so common today that any user has an idea about them. There are many types of attacks, their purpose is to steal any information. Each user must have a manual for maximum protection of his personal computer, which is connected to the network, and to the personal data that is on the personal computer. Information technologies have become firmly embedded in the life of every person, as well as in any production process. No activity is complete without innovative digital technologies based on artificial intelligence. An inseparable part of the computer is the Internet, through which the attack on user data is carried out. In this article we will consider the types of network attacks, methods of combating them. Consider the methods of how to protect yourself and your data on the network when using the Internet. To date, there are many programs that are viral, and a network participant, using it, does not suspect that his personal data, his page and familiar users associated with it may suffer from a cyber-attack. Let's look at various types of programs through which attacks can be carried out on the network, we will give methods for bypassing them and combating them.

Keywords: information security, network attacks, virus programs, data theft, the Internet.

1. Введение

Современное общество и любой вид деятельности не могут обойтись без использования информационных технологий, которые работают через сеть Интернет. Чем больше внедрений в отрасли деятельности, тем больше сетевых атак может быть.

Любой пользователь должен обладать информацией о сетевых атаках, их видах и методах. Для противодействия им необходимо владеть информацией, которая обезопасит пользователя сети. Рассмотрим данные вопросы в статье [1].

2. Материалы и методы

Сетевая атака – действие, осуществляемое в сети Интернет, имеющее цель – кражу данных пользователя.

Рассмотрим виды сетевых атак и предложим пути их решения.

Первым видом атаки в сети Интернет может быть посыл огромного количества писем на электронный почтовый ящик с помощью специальных программ. Целью такой атаки является блокировка почтового ящика получателя.

Способами защиты от такой атаки в сети являются следующие рекомендации:

1. Запрещено вводить адрес электронной почты в непроверенные источники.
2. Целесообразно иметь несколько почтовых ящиков, предназначенных для личного пользования и для рабочего процесса [2].

Другим видом сетевых атак является атака с помощью вирусных программ. Любая рабочая станция уязвима для вирусов. Это вредоносные программы, которые внедряются в персональные компьютеры и мешают их правильному функционированию или способствуют краже информации с техники. Опаснее всего то, что с помощью таких вирусных программ можно совершить кражу паролей от социальных сетей и личных кабинетов, зарегистрированных и сохраненных в персональном компьютере.

При таких сетевых атаках необходимо применять следующие способы борьбы:

1. Использование антивирусных программ, которые могут вычислить вирус и ликвидировать его.
2. Использование шифрования информации и данных.
3. Использование двойной защиты паролей: почти во всех приложениях, где требуется ввод логина и пароля, есть двойная защита, которая действует следующим образом – при вводе пароля для входа на мобильный телефон, номер которого привязан к странице, приходит сообщение с кодом, который

необходимо внести для входа. Если пользователь не совершал вход на свою страницу, но получил код, он не должен его никому сообщать, и должен немедленно сменить пароль и логин страницы [3].

Еще одним видом сетевых атак, наиболее распространенных на сегодняшний день, является фишинг-атаки. Целью таких атак является обман пользователей сети и кража их персональных данных. Этот способ предназначен для преступного использования. Качество личной информации, полученной преступниками в результате нападения, имеет значение само по себе.

Способами борьбы с такой атакой являются:

1. Пользование проверенными ресурсами.
2. Проверка страниц с помощью антивирусной программы.
3. Регулярное обновление антивирусных программ [4].

Другим видом сетевых атак является атаки на ресурсы администраторов, на какие-либо социальные сети и иные ресурсы. Называется такая атака PHP-инъекция. Способ атаки заключается во взломе сайтов, внедрение в код сайта злого сценария.

Подвергаться таким атакам могут только администраторы социальных сетей. Чтобы ликвидировать такую атаку, необходимо:

1. Тщательно проверять код страницы, которой владеет администратор на наличие в коде посторонних символов;
2. Проверять код на наличие только допустимых значений и символов.

3. Результаты и обсуждение

Так как сегодня сетевые атаки происходят каждый день, необходимо повышать уровень безопасности в сети. Для этого каждый пользователь должен помнить следующие общие правила:

1. Необходимо проверять тип вводимых данных;
2. При входе на сайты или при пользовании приложением необходимо проверить его на наличие вирусных программ;
3. Вводить в сети минимум личных данных, которые являются секретными;
4. Устанавливать сложные пароли на страницы;
5. Хранить в сети минимум информации, которая не должна быть украдена [5].

4. Заключение

Таким образом, были рассмотрены основные сетевые атаки и способы борьбы с

ними. Данная область является наиболее развивающейся, так как идет постоянное соперничество между злоумышленниками и организациями, обеспечивающими безопасность данных.

Список литературы

1. Боршевников, А.Е. Сетевые атаки. Виды. Способы борьбы / А.Е. Боршевников. – Текст: непосредственный // Современные тенденции технических наук: материалы I Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. – С. 8-13.
2. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов / Пер. с англ. – М.: Издательство «Русская Редакция»; – СПб.: Питер, 2007. – 432 с.
3. Сергеев, Р.А. Анализ уязвимости переполнения буфера / Р.А. Сергеев. – Текст: непосредственный // Молодой ученый. – 2017. – № 4(138). – С. 181-185.
4. Касперски, К. Искусство дизассемблирования / К. Касперски, Е. Рокко. – СПб.: БХВ-Петербург, 2008. – 891 с.
5. Варлатая, С.К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником / С.К. Варлатая, О.С. Рогова, Д.Р. Юрьев. – Текст: непосредственный // Молодой ученый. – 2015. – № 1(81). – С. 36-37.