УДК 004

АНАЛИЗ ПРОБЛЕМ ЗАЩИТЫ ОРГАНИЗАЦИИ ОТ МЕЖСЕТЕВЫХ АТАК

Ткаченко А.Л.
к.т.н., доцент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Бурцева В.В.
студент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Кузнецова В.И.
к.п.н., доцент,
Калужский филиал Финансового университета при Правительстве Российской Федерации,
Калуга, Россия

Аннотация
Одним из важнейших аспектов нашей жизни является информационная безопасность. Любые устройства, наделённые цифровым разумом сейчас могут нести угрозу для Всемирной паутины. Существуют различные виды сетевых атак, вредоносного ПО и других угроз информационной безопасности. В данной статье мы рассмотрим варианты угроз и пути их нейтрализации при помощи различных межсетевых экранов и брандмауэров.
Ключевые слова: информационная безопасность, межсетевой экран, брандмауэр, угроза, сетевая атака.

ANALYSIS OF THE PROBLEMS OF PROTECTING AN ORGANIZATION FROM INTER-NETWORK ATTACKS

Tkachenko A.L.
candidate of Technical Sciences,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Burtseva V. V.
student,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Kuznetsova V. I.
candidate of pedagogical Sciences,
Kaluga Branch of the Financial University under the Government of the Russian Federation,
Kaluga, Russia

Abstract
One of the most important aspects of our life is information security. Any devices endowed with digital intelligence can now pose a threat to the World Wide Web. There are various types of network attacks, malware and other threats to information security. In this article, we will consider the options for threats and ways to neutralize them using various firewalls and firewalls.
Keywords: information security, firewall, firewall, threat, network attack.

Одними из самых подверженных атаке устройств являются умные девайсы интернет-вещей IoT владельцы которых даже не подозревают, что эти

устройства могут быть использованы в кибератаке. Botnet часто применяют не только для DDoS атак, но так же они учавствуют в массовых рассылках спама. Например, поддельных писем, от отдельной доверенной организации, которое может содержать вредоносный файл, открыв который на своём ПК есть риск заразить его вирусом.

Как это связано с работой ПК в гос. учреждении [1]? Дело в том, что посещаемые страницы в интернете не всегда безопасны, а так как во Всемирной паутине есть устройства, неконтролируемо переносящие вредоносные файлы, естественно, атаке может подвергнуться любой из пользователей, подключившийся к ней [2, 3].

Рассмотрев некоторые варианты угроз, можем обсудить варианты защиты от них на предприятии. А именно – межсетевые экраны. Так же, их называют Firewall или брандмауэр. Firewall является сетевым устройством, обеспечивающим безопасность данной инфраструктуры. Это устройство работает на третьем – сетевом уровне модели ISO, Firewall выполняет защиту локальной сети от неавторизированного доступа из внешних не доверенных сетей. Firewall блокирует не разрешённый входящий и выходящий трафик, с помощью свода специальных правил – списка контроля доступа ASL (access control list).

Один из простейших вариантов блокировки доступа к ресурсу – настройка ASL на блокировку IP адреса этого ресурса. Так же, Firewall может ограничивать доступ на основании портов, доменных имён, протоколов или приложений.

Существует 2 типа Firewall: stateful и stateless. Первый тип – более продвинутый. Он понимает весь контекст трафика и следит за состоянием соединения. Если stateful Firewall принимает пакет, он так же проверяет его метаданные: порты, IP адреса, длину пакета, информацию уровня 3, флаги и многое другое. Stateless Firewall более простой. Он исследует каждый пришедший пакет изолировано и принимает решение на основании того, что сказано в ASL.

Прокси-экраны - это пакеты программ, которые строятся на -аппаратной платформе или на операционных системах. Firewall могут иметь несколько интерфейсов, к которым он подключается. Стандарт работает таким образом: Firewall проверяет подключение и на основе существующих стандартов генерирует решение о пропуске или отклонении, а в некоторых случаях аннулировании полученного пакета [4, 5].

Улучшение стандартов безопасности проводится с помощью модулей доступа. Что происходит за счет создания модуля доступа, который соответствует разрешаемому протоколу в прокси-экране прикладного уровня. Одними из лучших считаются те, которые специально разработаны для разрешаемого протокола. В качестве примера можно привести модуль доступа FTP, определяющий соответствие разрешённого трафика для этого протокола и соответствие правилам политики безопасности [6].

Firewall прикладного уровня использует модули доступа для входящих подключений, для защиты системы от атак и ненужных подключений, выполняемых приложениями. Модуль доступа получает входное подключение, анализирует протокол на соответствие правил политики и обрабатывает команды перед отправкой трафика получателю.

Имеется набор правил для межсетевых экранов, которые курируют доставку трафика из различных сетей. Таким образом, если входящее подключение не будет соответствовать правилам политики, то пакеты не пройдут через межсетевой экран, а также будут аннулированы.

Брандмауэры с каждым годом изменяются и улучшают свои функциональные возможности. Создатели межсетевых экранов прикладного уровня создали технологию GSP для межсетевых экранов, которая обеспечивает работу экранов прикладного уровня в качестве экранов с пакетной фильтрацией.

Для обеспечения высокого уровня безопасности разработчики межсетевых экранов с пакетной фильтрацией добавили модули доступа в своих продукты. На

данный момент модуль доступа SMTP поставляется со многими межсетевыми экранами с пакетной фильтрацией.

Рассмотрев виды межсетевых экранов можно сделать вывод, что самым практичным вариантом будет являться использование гибридного межсетевого экрана. Именно он обеспечит надёжную защиту пользователей отдельно взятой сети гос. учреждения. Для более надёжной защиты так же необходимо регулярно проводить профилактику, которая будет включать в себя проверку на вирусы, резервирование данных администрирование сетей и соответственно установка firewall.

Библиографический список:

1. Белаш, В. Ю. Из опыта решения проблемы формирования готовности бакалавров направления "Педагогическое образование" к созданию и проведению элективных курсов экономико-математического содержания / В. Ю. Белаш // Глобальный научный потенциал. – 2021. – № 1(118). – С. 17-19.

2. Имитационное моделирование демографических показателей роста и убыли наслеления / А. Л. Ткаченко, О. М. Лыкова, Е. И. Шаронов, В. И. Кузнецова // Modern Economy Success. – 2021. – № 3. – С. 110-116.

3. Кондрашова, Н. Г. Оценка экономической безопасности через систему финансовых показателей организации / Н. Г. Кондрашова, Я. А. Фрайман // Вектор экономики. – 2021. – № 4(58).

4. Кондрашова, Н. Г. Информация и ее применение в ходе управления проектами / Н. Г. Кондрашова // Дневник науки. – 2020. – № 12(48). – С. 50.

5. Ткаченко, А. Л. Имитационное моделирование распространения кибератак на промышленные предприятия / А. Л. Ткаченко, А. Ю. Гордеева, А. В. Шавренко // Инновационные технологии, экономика и менеджмент в промышленности : Сборник научных статей по итогам IV международной научной конференции, Волгоград, 22–23 апреля 2021 года. – Волгоград: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 238-240.).

6. Tkachenko, A., Lavrentev, D., Denisenko, M., Kuznetsova, V. Development of a simulation model for the spread of COVID-19 coronavirus infection in Kaluga region // E3S Web of Conferences, 2021, 270, 01003. DOI: 10.1051/E3SCONF/202127001003.

Оригинальность 75%