Тип работы: Дипломная работа

Предмет: Информационные технологии

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В данной ВКР проведён анализ технологий обеспечения защиты корпоративных сетей от угроз, связанных с факторами информационной безопасности с использованием сервисов компании-провайдера. Работа современных организаций в значительной степени определяется качеством использования информационных ресурсов, доступности данных, возможностями обмена информацией как внутри компаний, так и с внешними контрагентами.
Защита сетевых ресурсов обеспечивается как в технической части, что связано с использованием систем защиты оборудования, бесперебойного питания, физической защиты помещений. Одной из основных составляющих системы защиты сетевых ресурсов является защита от угроз программного типа, включающих сетевые атаки, активность вредоносных систем, необходимость обеспечения защиты каналов передачи данных. Таким образом, задачи по обеспечению защиты корпоративных сетей являются актуальными в условиях организаций различного профиля деятельности.
Цель дипломной работы заключается в разработке мер по обеспечению безопасности в области защиты от сетевых угроз с использованием возможностей компании-провайдера.
Компании-провайдеры в рамках обслуживания клиентов могут предлагать услуги по обеспечению защиты трафика, настройки сетевого оборудования, защиты от СПАМ-рассылок, шифрования каналов передачи данных.
Задачи работы:
 анализ специфики организации защиты от сетевых атак на информационные ресурсы компаний;
 анализ основных видов сетевых угроз на информационные ресурсы компаний;
 выбор услуг провайдеров для обеспечения защиты сетевых ресурсов;
 разработка архитектуры безопасности на основе программного обеспечения и настройки сетевого оборудования.
Объект исследования: системы защиты от сетевых угроз.
Предмет исследования: системы защиты от сетевых угроз на информационные ресурсы.

Работа содержит: введение, две главы, заключение, список использованных источников. Во введении проведено обоснование актуальности проблематики обеспечения защиты сетевых ресурсы организаций от сетевых атак, проведена постановка цели и задач исследования. В главе 1 проведен анализ теоретических аспектов обеспечения защиты от сетевых угроз, проведена их классификация, определены основные направления по обеспечению защиты от угроз каждого вида, построена модель угроз и модель нарушителя в условиях ООО «Символ». В главе 2 проведено определение мер по обеспечению защиты от сетевых угроз, включающих сетевые атаки, СПАМ-рассылки, подбор паролей, возможности сканирования систем на наличие уязвимостей. В главе 3 проведено описание настройки сетевого оборудования, позволяющие сократить вероятность успешной реализации сетевых угроз. В разделе 4 проведена разработка проекта внедрения разработанных решений, оценена стоимость, с помощью риск-ориентированного подхода оценено снижение факторов риска успешной реализации сетевых угроз.

1. Аналитическая часть
1.1. Обзор законодательных актов в области защиты информации

Нормативная база в области защиты персональных данных включает:
- 152- ФЗ «О Персональных данных» от 27.07.2006;
- 149 – ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006;
- Статьи Трудового кодекса, кодекса об административных правонарушениях;
- Локальные нормативные акты.

Нормативной базой технологии систем информационной безопасности являются: федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и ФСБ России, регулирующие вопросы безопасности информации.
В соответствии с нормативными документами в области защиты информации, каждое предприятие и организация, в которой производится обработка персональных данных, обязано принять ряд организационных и технологических мер по обеспечению защиты информации.
Приведем основные положения законодательных актов в области информационной безопасности.
Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным
Согласно Федеральному закону от 27 июля 2006г. № 152-ФЗ, оператор в рамках обработки персональных данных должен обеспечивать комплекс необходимых правовых, организационных и технических мер по обеспечению конфиденциальности персональных данных, что достигается путем определения угроз безопасности, оценки эффективности мероприятий по обеспечению безопасности, контроля за принимаемыми мерами по защите информации [8].
Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Постановление № 1119 содержит довольно подробную классификацию информационных систем персональных данных, угроз безопасности таких систем (п. 6), уровней защищенности информационных систем от указанных угроз
Приказ ФСТЭК России № 21 от 18.02.2013 определяет принципы классификации систем персональных данных. Согласно приказу ФСБ от 10.07.2014 № 378 определены четыре уровня защищенности персональных данных.
Каждый из присвоенных уровней защищенности предполагает применение соответствующих мер по обеспечению информационной безопасности.
В зависимости от соотношения типа информационной системы и характерных для нее угроз выделены четыре уровня защищенности персональных данных, необходимых для конкретной информационной системы.

1.2. Общая характеристика видов сетевых угроз

В рамках данной работы проведен анализ обеспечения защиты от сетевых угроз с использованием сервисов компании-провайдера.
Виды сетевых угроз, характерных для информационных систем организаций, связаны со следующими факторами [10]:
 атаки на серверные ресурсы организаций;
 попытки несанкционированного подключения к информационным ресурсам, перехвата информации, передаваемой по каналам связи;
 активность вредоносных программ;
 использование уязвимостей в системных и прикладных программных средствах в целях, поставленных злоумышленниками.
В рамках проведения сетевых атак осуществляются попытки нарушения функционирования программных средств с использованием инструментария, генерирующего запросы и скрипты, нарушающие штатный режим функционирования целевой системы.
Возможными целями проведения внешних воздействий на сетевые ресурсы могут являться [11]:
 получение несанкционированного доступа к информационным ресурсам;
 нарушение доступности информационного ресурса атакуемой системы;
 использование вычислительных мощностей атакуемой системы в заданных целях.
Сетевые атаки на профессиональном уровне могут осуществляться в рамках конкурентной борьбы компаний, в деятельности специальных служб государств.
Инструменты реализации внешних атак представляют собой либо самостоятельно разработанные скрипты, либо специальные программные системы, генерирующие команды, целями которых является отправка запросов на удаленные системы, реализация вредоносных рассылок, активация вредоносных кодов и др.
Существует множество вариантов реализации атак в зависимости от конечной цели.
Одним из примеров атак, направленных на получение несанкционированного доступа к удаленным системам, является атака на основе подключения злоумышленника между источником и потребителем передаваемой информации (MITM). Результатом успешности реализации атаки на подобной основе является перехват платежных данных, корпоративной почты, аутентификационной информации.
Механизм выявления признаков проведения атак подобного типа затруднен вследствие использования систем маскировки.
На рисунке 1 приведена схема MITM-атаки.

Рисунок 1 - Схема MITM-атаки

Успешность реализации атаки подобного типа зависит от невозможности детектирования внешнего подключения. В качестве объекта атак подобного типа наиболее часто выступают устройства беспроводного доступа, в которых злоумышленники используют уязвимости в прошивках оборудования. Процесс проведения атаки предполагает подключение устройства через Wi-Fi, генерацию перезагрузки роутера атакуемой сети и перенаправление трафика через беспроводную сеть устройства злоумышленника. При успешном осуществлении атаки весь трафик начинает передаваться через роутер злоумышленника. При этом весь поток передаваемой конфиденциальной информации перехватывается.
Таким образом, при проектировании системы сетевой безопасности необходимо использовать специальные средства, позволяющие выявлять факты подмены сетей, анализировать идентификаторы используемого сетевого оборудования.
Также одним из типичных видов сетевых угроз является проведение атак на отказ в обслуживании. Алгоритмы атак подобного вида предусматривают генерацию запросов на внешние сервера, которые, при достижении определенного уровня интенсивности поступления запросов, требуют возможности их обработки, что приводит к неработоспособности информационных ресурсов.
Инструментом атак подобного вида является специализированное ПО, в котором настраивается адресация атакуемой системы, настраивается интенсивность, типы отправляемых пакетов. Цель атак подобного вида связана с невозможностью обработки запросов и удалёнными системами и приведение их в состояние неработоспособности.
Как правило, целями атак могут являться сервера крупных компаний (при проведении атак по заказу конкурирующих организаций), серверы государственных органов, СМИ, ресурсы силовых структур.
Обеспечение защиты от атак подобного типа проводится на уровне сетевых устройств, систем защиты от сетевых угроз. также признаки подобных атак определяются на серверах приложений, баз данных. Защиты

может осуществляться с использованием интеллектуальных модулей, выявляющих наличие признаков проведения внешних атак, ручной настройки разрешенных подключений. При выявлении признаков атаки на отказ в обслуживании поступившие запросы не передаются на обработку и сервер сохраняет работоспособность.
Таким образом, основные алгоритмы обеспечения защищенности серверов от DDoS-атак включают [4]:
- настройку прошивок на уровне коммутаторов, роутеров, маршрутизаторов;
- использование криптографических систем (что позволяет распознавать происхождение поступивших сетевых пакетов, пакеты с нераспознанным ключом или незашифрованные не распознаются и отклоняются системой);
- работу с системами машинного обучения, что позволяет выявлять признаки наличия пакетов из недоверенных источников);
- использование средств защиты информации, в которые встроены средства детектирования сетевых атак.
Схема алгоритма DDOS - атак приведена на рис.5.

Рисунок 2 - Схема алгоритма DDOS - атак

Как показано на рис.2, для при проведении генерации пакетов для отправки на атакуемые системы работают специализированные подсети (зачастую компонентами которых являются узлы, зараженные вредоносными программами). Команда на запуск атаки отдается злоумышленником из удалённой системы.
Уровни реализации DDoS-атак:

Рисунок 3 - Уровни реализации DDoS-атак
Классификация средств защиты от DDoS-атак [10]:
 Системы управления адресацией трафика, встроенные в драйверы сетевого оборудования;
 Использование динамических алгоритмов SYN прокси;
 Настройка предельного количества обрабатываемых сетевых пакетов, что позволяет отклонять вредоносные пакеты;
 Выявление признаков ICMP, UDP флуда на уровне систем сетевой защиты;
 Управление скоростью поступления данных на маршрутизаторах на границе внутренней и внешней сети.
Графическими средствами мониторинга сетевой активности возможно выявление аномального поступления запросов, что является признаком проведения атаки (рис.4).

Список использованных источников

1. Внуков А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — Москва: Издательство Юрайт, 2022. — 161 с.
2. Аникин Д. В. Информационная безопасность и защита информации: учебное пособие / Д.В. Аникин. - Барнаул: Изд-во Алтайского государственного университета, 2018. - 196 с.
3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с.
4. Ахметов И. В., Карабельская И. В., Губайдуллин И. М., Сафин Р. Р. Моделирование бизнес-процессов: учебное пособие. - Уфа: Уфимский государственный университет экономики и сервиса, 2015. - 67 с.
5. Запечников С. В. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с.
6. Бабиева Н. А., Раскин Л. И. Проектирование информационных систем: учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. - Казань: Медицина, 2014. – 200с.
7. Баранников Н. И., Яскевич О. Г. Современные проблемы проектирования корпоративных информационных систем / Н. И. Баранников, О. Г. Яскевич; ФГБОУ ВПО "Воронежский гос. технический ун-т". - Воронеж: Воронежский государственный технический университет, 2014. - 237 с.
8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.
9. Белобородова Н. А. Информационная безопасность и защита информации : учебное пособие / Н. А. Белобородова; Минобрнауки России, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Ухтинский гос. технический ун-т" (УГТУ). - Ухта : УГТУ, 2016. - 69 с.

10. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта : УГТУ, 2016. - 69 с.
11. Благодаров А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
12. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей: методы и средства : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 225с.
13. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
14. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
15. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки : [учебное пособие] / А. В. Кондратьев. - Москва: Горячая линия - Телеком, 2016. - 304 с.
16. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
17. Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — Москва: Издательство Юрайт, 2022. — 473 с.
18. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.
19. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва : ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
20. Никифоров С. Н. Защита информации: защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
21. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров. - Санкт-Петербург: СПбГАСУ, 2017. - 76 с.
22. Никифоров С. Н., Ромаданова М. М. Защита информации. Пароли, скрытие, удаление данных: учебное пособие / С. Н. Никифоров, М. М. Ромаданова. - Санкт-Петербург: СПбГАСУ, 2017. - 107 с.
23. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова. - Хабаровск : Изд-во ТОГУ, 2018. – 81с.
24. Щеглов А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с
25. Суворова Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с.