Бютнер С.И. Построение сети для изоляции атакуемых сервисов: использование DMZ // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 1(51) с. 108–111

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.738

ПОСТРОЕНИЕ СЕТИ ДЛЯ ИЗОЛЯЦИИ АТАКУЕМЫХ СЕРВИСОВ: ИСПОЛЬЗОВАНИЕ DMZ

Бютнер С.И.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: serafimkavasaki@gmail.com

Использование демилитаризованной зоны (DMZ) в архитектуре сетей позволяет изолировать атакуемые сервисы, минимизируя риск доступа злоумышленников к внутренним сетям. DMZ служит буфером между публичными ресурсами и внутренними сетями организации, защищая чувствительные данные. Статья объясняет принципы работы DMZ, её ключевые компоненты, преимущества и недостатки, а также даёт рекомендации по настройке для повышения уровня безопасности.

Ключевые слова: DMZ, изоляция сетей, защита сервисов, архитектура сети, безопасность данных, фаерволы, настройки сети.

BUILDING A NETWORK TO ISOLATE VULNERABLE SERVICES: USING A DMZ

Buetner S.I.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

Using a demilitarized zone (DMZ) in network architecture allows for isolating vulnerable services, minimizing the risk of attackers accessing internal networks. A DMZ acts as a buffer between public resources and an organization's internal networks, safeguarding sensitive data. The article explains the principles of DMZ operation, its key components, advantages and drawbacks, and provides recommendations for configuration to enhance security.

Keywords: DMZ, network isolation, service protection, network architecture, data security, firewalls, network configuration.

Введение

С ростом числа киберугроз и атак на сетевые ресурсы организации всё чаще сталкиваются с необходимостью изолировать свои критически важные сервисы от внешних угроз. Одним из эффективных способов достижения этой цели является использование демилитаризованной зоны (DMZ). DMZ — это специализированная сеть, которая размещает публично доступные сервисы, такие как веб-серверы, почтовые серверы или DNS-серверы, в изолированном пространстве между внешним интернетом и внутренней корпоративной сетью.

Идея DMZ заключается в том, чтобы создать буфер, который защитит внутренние системы от прямых атак, даже если публичный сервер будет скомпрометирован. Такой подход особенно актуален для организаций, работающих с конфиденциальными данными,

финансовыми транзакциями или предоставляющих услуги через интернет. Однако, несмотря на очевидные преимущества, эффективное построение и настройка DMZ требуют понимания её архитектуры и грамотного подхода к безопасности.

Построение сети для изоляции атакуемых сервисов

Демилитаризованная зона (DMZ) представляет собой отдельную подсеть, которая служит буфером между внешним интернетом и внутренней сетью компании. Её основное предназначение — размещение публично доступных сервисов, таких как веб-сайты, почтовые серверы, FTP-серверы и DNS. Эти ресурсы чаще всего подвергаются атакам со стороны злоумышленников, и их размещение в изолированной зоне помогает минимизировать риск для остальных компонентов инфраструктуры. Основной принцип работы DMZ базируется на использовании двух фаерволов: внешний фаервол ограничивает доступ из интернета в DMZ, а внутренний защищает корпоративную сеть, предотвращая передачу трафика из DMZ внутрь без строгой проверки. Такое разделение позволяет защитить внутренние данные и ресурсы даже в случае успешной компрометации одного из сервисов в демилитаризованной зоне[1].

Размещение сервисов в DMZ даёт множество преимуществ. Во-первых, это изоляция наиболее атакуемых ресурсов. Например, если веб-сервер в DMZ скомпрометирован, злоумышленники не смогут напрямую атаковать внутреннюю сеть, поскольку её доступ ограничен внутренним фаерволом. Во-вторых, это упрощает мониторинг: трафик, проходящий через DMZ, легче отслеживать на наличие аномалий, что повышает эффективность систем обнаружения и предотвращения вторжений (IDS/IPS). Ещё одним плюсом является удобство управления: все публичные сервисы находятся в одной изолированной зоне, что упрощает их настройку и контроль[2].

Однако реализация DMZ требует грамотного подхода. Неправильная настройка может свести на нет её защитные функции. Например, слишком широкие правила фаерволов могут позволить злоумышленникам обойти защиту и проникнуть во внутреннюю сеть. Кроме того, администрирование DMZ требует высокого уровня компетенции: регулярное обновление серверов, установка патчей и использование современных протоколов шифрования, таких как HTTPS и SFTP, являются обязательными мерами. Для повышения безопасности рекомендуется использовать сегментацию внутри самой DMZ, когда каждый сервер размещается в отдельной подсети. Это предотвращает распространение угрозы на другие ресурсы в случае компрометации одного из них[3].

При создании DMZ важно учитывать специфику работы организации. Например, если компания активно использует удалённые подключения, то DMZ должна быть настроена с учётом этих требований. Использование VPN для доступа к серверам в DMZ поможет дополнительно защитить данные от перехвата. Для мониторинга активности в DMZ стоит применять системы логирования и анализа трафика, которые позволят оперативно реагировать на попытки атак. Ещё одной важной мерой является ограничение доступа: подключение к серверам в DMZ должно быть разрешено только с конкретных IP-адресов или через определённые порты[4].

Несмотря на все преимущества, DMZ имеет свои ограничения. Она не является универсальным решением и не может защитить сеть от всех типов атак. Например, социальная инженерия или фишинг могут позволить злоумышленникам получить доступ к внутренней сети, минуя DMZ. Поэтому её использование должно быть частью комплексной стратегии

безопасности, включающей регулярные аудиты, обучение сотрудников и резервное копирование данных[5].

Заключение

Использование демилитаризованной зоны (DMZ) является одним из ключевых методов обеспечения сетевой безопасности, позволяя изолировать уязвимые сервисы от внутренних систем. Благодаря правильной настройке и использованию современных технологий, таких как IDS/IPS, фаерволов и шифрования, DMZ помогает организациям защищать свои ресурсы от киберугроз.

Однако для достижения максимального уровня безопасности важно не только внедрять DMZ, но и регулярно обновлять её компоненты, а также проводить аудит сетевой инфраструктуры. Современные угрозы требуют комплексного подхода к безопасности, в котором DMZ становится лишь одним, но крайне важным элементом общей стратегии.

В условиях увеличивающегося числа атак на публично доступные ресурсы создание DMZ — это не только эффективное, но и необходимое решение для защиты критически важных данных и систем.

Список литературы

1. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
2. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Current problems of infotelecommunications in science and education. - 2021. – pp. 409-414.
3. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.

4. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
5. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruevich, 1996.