Ноянов Р.С. Использование микросегментации для повышения безопасности в крупных объектах информатизации // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 33–36

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.736

ИСПОЛЬЗОВАНИЕ МИКРОСЕГМЕНТАЦИИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ В КРУПНЫХ ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Ноянов Р.С.
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: romannoyanov@gmail.com

Микросегментация — это передовая методика, которая позволяет улучшить безопасность информационных систем, особенно в крупных организациях с разветвлённой IT-инфраструктурой. Микросегментация обеспечивает защиту на уровне приложений, минимизируя возможности lateral movement (бокового проникновения) злоумышленников в случае успешного взлома одного из компонентов. В статье рассматриваются основные принципы микросегментации, её значение для защиты от кибератак, а также приводятся примеры её внедрения и рекомендации для крупных объектов информатизации.

Ключевые слова: Микросегментация, информационная безопасность, крупные организации, боковое проникновение, защита данных, сегментация сети.

THE USE OF MICROSEGMENTATION TO IMPROVE SECURITY IN LARGE INFORMATION FACILITIES

Nayanov R.S.
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: romannoyanov@gmail.com

Microsegmentation is an advanced technique that improves the security of information systems, especially in large organizations with complex IT infrastructures. It provides application-level security, reducing the risk of lateral movement by attackers if one component is compromised. The article covers the core principles of microsegmentation, its importance in cyberattack prevention, and practical examples of its deployment in large information systems.

Keywords: Microsegmentation, information security, large organizations, lateral movement, data protection, network segmentation.

Введение

С ростом объёма информации и сложностью IT-инфраструктур безопасность крупных объектов информатизации становится одной из первостепенных задач для организаций. Современные компании и государственные учреждения сталкиваются с целым рядом угроз, таких как взломы, утечка данных и целевые атаки, направленные на компрометацию их систем. Чтобы уменьшить риски, специалисты по безопасности используют различные техники сегментации сети, и одной из наиболее эффективных из них является микросегментация. В отличие от традиционной сегментации, микросегментация позволяет детализировать контроль и изолировать каждое приложение и сервис в пределах одного

сегмента, что обеспечивает высокую степень защиты от так называемого бокового проникновения (lateral movement), когда злоумышленник может перемещаться по сети, получив доступ к одной её части.

Применение микросегментации помогает изолировать рабочие процессы и сервисы друг от друга, что особенно актуально для крупных организаций, которые работают с конфиденциальной информацией. Это позволяет не только повысить безопасность данных, но и управлять политиками доступа на уровне приложений. Микросегментация даёт возможность контролировать связи между сервисами и пользователями, создавая своеобразные «цифровые барьеры» в пределах корпоративной сети и защищая критически важные ресурсы от несанкционированного доступа. В этой статье рассмотрены принципы, которые лежат в основе микросегментации, её преимущества для крупной инфраструктуры, а также примеры использования этой технологии.

Использование микросегментации для повышения безопасности в крупных объектах информатизации

Микросегментация — это методика, которая предполагает разбивку сети на мелкие логические сегменты, каждый из которых имеет свои правила и политики безопасности. Это позволяет точно контролировать доступ и взаимодействие как между отдельными устройствами, так и между приложениями, работающими в пределах одного сегмента сети. Одним из основных преимуществ микросегментации является её способность предотвращать распространение угроз в случае взлома одного из сегментов. В обычной сети, если злоумышленник получает доступ к одному устройству, он может с легкостью распространить атаку на другие устройства внутри этой же сети. Микросегментация же создаёт «защитные зоны» для каждого компонента, ограничивая доступ к ним и минимизируя последствия атаки[1].

К примеру, в случае атаки с использованием уязвимости в приложении, злоумышленник может попытаться использовать её для бокового проникновения. Если инфраструктура крупной организации сегментирована с помощью микросегментации, атакующий будет ограничен в доступе и не сможет перейти к другим важным системам, таким как базы данных или сервисы обработки платежей. Это особенно полезно для организаций, работающих с чувствительными данными, такими как финансовые учреждения, медицинские центры и государственные ведомства. В условиях сложных сетевых архитектур, где тысячи устройств и пользователей взаимодействуют между собой, возможность контролировать доступ на уровне приложения и отдельно каждой сессии позволяет значительно усилить защиту[2].

Ключевая особенность микросегментации — гибкость и масштабируемость. Современные решения по микросегментации позволяют легко адаптировать политику безопасности к новым приложениям, обновлениям или требованиям бизнеса. Это особенно важно в крупных организациях, где постоянно происходят изменения в архитектуре сети[3]. Например, если в систему добавляется новое приложение, микросегментация позволяет быстро задать необходимые правила доступа для него, без необходимости глобальных изменений всей сети. Также микросегментация может быть интегрирована с системами мониторинга, чтобы отслеживать активность внутри каждого сегмента и выявлять подозрительные действия в режиме реального времени[4].

Ещё один важный аспект микросегментации — возможность автоматизации управления. Благодаря технологиям микросегментации специалисты по безопасности могут создавать автоматические сценарии для защиты данных и управления доступом. Например, если в одном из сегментов происходит необычная активность, система может автоматически заблокировать доступ к этому сегменту, уведомить администратора и предотвратить распространение угрозы. Такой подход позволяет значительно снизить нагрузку на IT-отделы и минимизировать человеческий фактор.

Технически, микросегментация реализуется с помощью различных решений, таких как программно-определяемые сети (SDN) и системы виртуализации. Они позволяют изолировать не только физические устройства, но и виртуальные среды и облачные сервисы. С помощью этих технологий микросегментация может быть реализована в различных типах инфраструктуры, будь то традиционная корпоративная сеть, облачные решения или гибридные системы. Это делает микросегментацию одним из наиболее универсальных инструментов для повышения безопасности[5].

Несмотря на очевидные преимущества, внедрение микросегментации требует тщательного планирования и грамотной настройки. Необходимо разработать четкие правила доступа и взаимодействия для каждого сегмента, определить приоритетные ресурсы и настроить мониторинг активности внутри сегментов. Для крупных организаций этот процесс может занять значительное время, но результат оправдывает вложенные усилия: микросегментация позволяет снизить риск распространения атак, минимизировать потенциальные потери данных и обеспечить более высокий уровень безопасности для критически важных систем.

Заключение

Микросегментация представляет собой мощный инструмент для защиты крупных объектов информатизации от внутренних и внешних угроз. Её способность детально контролировать взаимодействие между компонентами сети и изолировать каждый процесс обеспечивает высокий уровень безопасности, необходимый для защиты современных корпоративных инфраструктур. Это особенно важно для крупных организаций, где большое количество пользователей и сервисов увеличивает риск несанкционированного доступа и утечек данных.

В условиях, растущих киберугроз микросегментация становится важным элементом стратегии безопасности, позволяя предотвратить распространение атак и защитить критически важные ресурсы. Внедрение микросегментации требует серьёзных ресурсов и усилий, однако преимущества, которые она предоставляет, делают её оптимальным решением для компаний, стремящихся к максимальной защите своей информации.

Список литературы

1. 1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных

//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.

3. 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.
4. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
5. 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.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High–tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
2. Minyaev A. A. Method for evaluating the effectiveness of an information protection system geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
3. 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.
4. Gelfand A.M. Methods of choosing stegocontainers for data transmission //Regional Informatics and information security. – 2020. – pp. 260-262.
5. 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.