УДК 004.08

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ МИКРОСЕГМЕНТАЦИИ

Мухаммадназир Низоми Нурзода
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Рассмотрены настройки информационной безопасности при внедрении микросегментации в организации. Описаны действия, которые могут обеспечить эффективность микросегментации, функционирование в нескольких центрах обработки данных (ЦОД) и облаках, определение шаблонов рабочих нагрузок и согласованную реализацию политик микросегментации. Показано, как достичь этих результатов, поддерживая гибридные рабочие нагрузки, работая в локальных ЦОД, частных и общедоступных облаках.

Ключевые слова: информационная безопасность, микросегментация, информационная безопасность, веб-приложения, файрвол, брандмауэр, облачные технологии, центр обработки данных, уровень доступа.

RECOMMENDATIONS FOR MICROSEGMENTATION SECURITY

Muhammadnazir Nizomi Nurzoda
Don State Technical University (Rostov-on-Don, Russian Federation)

The article discusses information security settings when implementing microsegmentation in an organization. The paper describes the actions that can ensure the effectiveness of microsegmentation, functioning in multiple data centers and clouds, defining workload patterns, and consistent implementation of microsegmentation policies. It shows how to achieve these results by supporting hybrid workloads, working in on-premises data centers, private and public clouds.

Keywords: information security, micro-segmentation, information security, web applications, firewall, brandmauer, cloud technology, data center, access layer.

Введение. Микросегментация — это технология сетевой безопасности, которая предполагает логическое разделение центров обработки данных (ЦОД) на сегменты безопасности с конкретными рабочими нагрузками. Это позволяет определять меры безопасности и ограничивать доступ к каждому сегменту [1].

Микросегментация дает возможность ИТ-отделам развертывать гибкие политики безопасности в ЦОД и облачных системах, применяя виртуализацию сети без необходимости установки нескольких брандмауэров [2].

Основная часть. Ниже перечислены передовые методики эффективной настройки информационной безопасности при внедрении микросегментации.

Тщательное определение границ. Эффективность микросегментации зависит от четкости определения архитектуры. Следует зафиксировать цели на основе классификации конечных пользователей, бизнес-приложений и ИТ-ресурсов, их чувствительности и основных рисков безопасности. Это позволит определить границы сегментации и выяснить объемы и тип информации, которая будет передаваться между сегментами.

Анализ приложений. В самом начале микросегментации обычно проводится работа с приложениями. Важно убедиться в наличии полной информации о приложениях, включая все внутренние и внешние коммуникации, службы и профили пользователей, которые имеют к ним доступ. На основе этих данных определяются сегменты для приложений и правила разрешенной связи между ними.

Определение уровней доступа. В большинстве приложений конкретные пользователи используют определенные уровни или ресурсы. Следует установить наименьшие права доступа, которые позволят пользователям выполнять их служебные функции. Нужно обозначить для каждого приложения уровни и отдельные службы и указать пользователей, которые получат к ним доступ. С учетом этих сведений проводится микросегментация.

Постепенное внедрение сегментаций. После определения границ, разрешенных коммуникаций и уровней доступа логически группируются приложения, серверы, наборы данных или пользователей. Каждая логическая группа может быть микросегментом. Проводится тестирование процесса в одной группе (желательно в менее критичной для организации), выявляются и устраняются проблемы. Затем работа продолжается в дополнительных группах.

RASP, WAF и микросегментация. Самозащита приложений во время выполнения (RASP, от англ. runtime application self-protection) — это программное обеспечение, которое тестирует безопасность приложений во время работы. RASP перехватывает запросы и блокирует действия, указывающие на атаку. Такую же функцию выполняют брандмауэры веб-приложений (WAF, от англ. web application firewall). Однако в этом случае работа фокусируется не на тестировании, а на выявлении и блокировке шаблонов вредоносного трафика. С этой целью анализируется трафик OSI Layer 7 (уровень приложений).

Оба типа инструментов можно использовать для микросегментации рабочих нагрузок. Например, функционал WAF позволяет указать на необходимость блокировки трафика, поступающего из других сегментов локальной сети.

Заключение. Для эффективной микросегментации нужны инструменты, которые могут работать в нескольких центрах обработки данных и облаках, определять шаблоны рабочих нагрузок и согласованно применять политики микросегментации. Облачный WAF достигает этих целей, поддерживая гибридные рабочие нагрузки, действуя в локальных центрах обработки данных, частных и общедоступных облаках.

Библиографический список

1. Бабаш, А. В. Информационная безопасность. Лабораторный практикум / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2016. — 136 с.

2. Гафнер, В. В. Информационная безопасность / В. В. Гафнер. — Ростов-на-Дону : Феникс, 2017. — 324 с.

Об авторе:

Мухаммадназир Низоми Нурзода, студент Донского государственного технического университета (344000, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), muhammadnazirnizomi@yandex.ru.

Author

Muhammadnazir Nizomi Nurzoda, Student, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), muhammadnazirnizomi@yandex.ru.