УДК 004.08

МИКРОСЕГМЕНТАЦИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. А. Кучер
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Описана политика организации безопасности в облачных центрах обработки данных (ЦОД) без установки нескольких брандмауэров. Проекты развертывания облаков ЦОД базируются на информационной безопасности. Для отражения современных атак администратору требуются разнообразные средства, одно из которых — микросегментирование сети.

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

MICROSEGMENTATION IN INFORMATION SECURITY

V. A. Kucher
Don State Technical University (Rostov-on-Don, Russian Federation)

The paper describes the policy of organizing security in cloud data centers without installation of multiple firewalls. Data center cloud deployment projects are based on information security. To deal with modern attacks, the administrator needs a variety of tools, one of which is microsegmentation of the network.

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

Введение. Микросегментация — это технология сетевой безопасности, которая позволяет логически разделить центры обработки данных (ЦОД) на сегменты безопасности по конкретным рабочим нагрузкам. Такой подход 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].

Основное преимущество микросегментации заключается в том, что для злоумышленников, взломавших один сегмент, другие остаются закрытыми. Это шаг вперед по сравнению с традиционным подходом, основная цель которого — предотвращение проникновения злоумышленников в так называемый «периметр безопасности». Иными словами, микросегментация изолирует и защищает каждый элемент внутри периметра.

Основная часть. Ниже перечислены элементы, которые получают обособленную защиту при микросегментации.

— Рабочие нагрузки и приложения. Сегментирование отдельных экземпляров программных приложений (например, одной базы данных — БД) или всех экземпляров, выполняющих определенную функцию (например, всех БД на языке SQL).

— Виртуальные машины. Сегментирование отдельных виртуальных машин или групп виртуальных машин (например, трех виртуальных машин, составляющих трехуровневое приложение).

— Операционные системы (ОС). Сегментирование отдельных или нескольких операционных систем, которые следуют определенной классификации (например, все ОС Linux, используемые разработчиками).

Микросегментация не предполагает настройку ИТ-ресурсов на аппаратном уровне с помощью межсетевых экранов или виртуальных локальных сетей. Вместо этого в рамках рассматриваемого подхода ИТ-ресурсы разделяются с помощью программных политик. Задействуя эти политики, администраторы определяют права доступа каждого сегмента к ресурсам и службам [1].

Известны различные методы микросегментации. Чаще всего для этих целей используется межсетевой экран нового поколения (NGFW, от англ. next generation firewall). NGFW обеспечивает видимость всех семи уровней модели OSI (от англ. open systems interconnection model — модель взаимодействия открытых систем). Это решение позволяет организациям создавать политики логического доступа для каждого приложения, работающего в сети. Микросегментация все чаще предлагается как часть решений программно определяемой глобальной сети (SD-WAN, от англ. software-defined networking in a wide area network). Такой подход обеспечивает возможность работы с несколькими удаленными объектами.

Далее представлены распространенные подходы к микросегментации.

— Сегментация приложений защищает важные приложения, работающие на так называемых «голых» железных серверах, виртуальных машинах или контейнерах, ограничивая связь. Это отличный способ достичь требований к информационной безопасности таких глобальных (главным образом североамериканских) стандартов, как PCI DSS (защита данных индустрии платежных карт), SOX (сохранность сведений о документообороте и финансовой отчетности публичных компаний) или HIPAA (безопасность мобильности и подотчетности в сфере медицинского страхования).

— Экологическая сегментация разделяет такие среды, как разработка, тестирование и производство. Это предотвращает обмен данными между средами. для обычных операций такой обмен не предусмотрен, но его могут использовать злоумышленники. Сегментация такого типа недостижима традиционными методами, поскольку среды распределены по нескольким центрам обработки данных, локально и в облаке.

— Сегментация уровней нужна, если приложения состоят из нескольких уровней (например, веб-сервера, сервера приложений и базы данных). В этом случае целесообразно сегментировать и изолировать каждый уровень. Это предотвращает перемещение злоумышленников между уровнями приложения, в частности с внешних уровней (таких как веб-сервер) на внутренние (такие как база данных).

— Высокодетализированная сегментация на основе процессов работает на уровне процесса или обслуживания. Например, конкретную программную службу можно изолировать и позволить взаимодействия только по явно разрешенным сетевым путям, протоколам и портам.

— Сегментация пользователей применяется группами в Microsoft Active Directory или ее аналогах. Процесс идет не на сетевом уровне. Скорее, отдельные пользователи внутри виртуальной локальной сети получают тот или иной уровень доступа [3].

Заключение. Микросегментация позволяет реализовать комплексный подход, инвариантный к гипервизорам и действующий как для аппаратных узлов, так и для контейнеров Linux. Однако микросегментация — лишь один из инструментов для обеспечения информационной безопасности. Для достижения максимального эффекта следует организовать комплексную защиту. Необходима, в частности, хорошо зарекомендовавшая себя технология ввода сервисов для объединения передовых систем обеспечения информационной безопасности и управления угрозами. Стратегия администрирования должна также предусматривать отражение атак на всем временном континууме — до, после и во время атаки, включая оперативное обнаружение, отражение и анализ.

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.

3. Громов, Ю. Ю. Информационная безопасность и защита информации / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. — Старый Оскол : ТНТ, 2017. — 384 с.

Об авторе:

Кучер Владислав Александрович, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), v.cu43r@yandex.ru

Author

Kucher, Vladislav A., Student, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), v.cu43r@yandex.ru