УДК 004.056.5

М.Н. Карпович
Белорусский государственный технологический университет
Минск, Беларусь

БЕЗОПАСНОСТЬ SERVERLESS ПРИЛОЖЕНИЙ

Аннотация. *В этом докладе рассматривается serverless архитектура и с сравнивается с существующие серверными архитектурами, определяются их главные особенности и анализируются с точки зрения безопасности. Описываются основные недостатки безопасности serverless архитектуры и рассматриваются возможные решения.*

M.N. Karpovich
Belarusian State Technological University
Minsk, Belarus

SECURITY OF SERVERLESS APPLICATIONS

Abstract. *This report examines the serverless architecture and compares it with existing server architectures, identifies their main features and analyzes them from the point of view of security. The main security flaws of the serverless architecture are described and possible solutions are considered.*

Архитектура serverless является моделью разработки, ориентированная на облака, которая позволяет предприятиям быстрее создавать приложения, устраняя необходимость в управлении инфраструктурой. При использовании serverless приложений облачный провайдер автоматически выделяет и масштабирует инфраструктуру, необходимую для выполнения кода, и управляет ею. Термин «serverless вычисления» говорит о том, что вычислительная мощность может быть использована без явного выделения сервера пользователям облака [1]. Будучи однажды развернуты, serverless приложения реагируют на количество запросов и автоматически масштабируются по мере необходимости, так как сервис FaaS измеряется по требованию и, как правило, всегда доступен. После его выполнения плата больше не взимается. Основными преимуществами данной архитектуры являются:

- Отсутствие инфраструктуры, которая полностью настраивается и поддерживается провайдером.
- Стоимость, так как вы платите только за использование данного сервиса. Serverless предложения провайдеров, как правило, измеряются по требованию с помощью событийноориентированной

исполнительной модели. В результате, когда serverless функция простаивает, это ничего не стоит;

• Масштабируемость, происходит автоматически в зависимости от количества запросов, приходящих в ваш сервис;

• Упрощение работы с кодом, с использованием данной архитектуры появляется возможность небольшие функции или все приложение сразу; • Высокая скорость выхода на рынок.

Поверхность атаки [2] serverless вычисления обеспечивают значительную устойчивость по сравнению со своими предшественниками. Это происходит по трем основным причинам. Во-первых, поскольку функции не имеют состояния и предназначены только для выполнения одной задачи, они должны постоянно взаимодействовать с другими функциями и облачными сервисами для оптимизации своих функциональных возможностей. Во-вторых, функции могут запускаться внешними или внутренними источниками событий [3] с различными форматами и кодировками. В-третьих, serverless платформы включают в себя ряд новых компонентов и облачных сервисов, многие из которых являются общими для всех пользователей.

Облачные провайдеры являются единственными, кто отвечает за выполнение всех операционных и инфраструктурных задач, включая те, которые направлены на защиту их инфраструктуры и приложений от внутренних и внешних угроз. К сожалению, облачные провайдеры обычно хранят большую часть информации о своих инфраструктурах в тайне, что затрудняет экспертам по безопасности тщательную проверку безопасности и приватности данных платформ.

Облачные провайдеры стремятся разрабатывать серверные платформы, которые совместно максимизируют безопасность и производительность как их инфраструктуры, так и приложений их клиентов, сохраняя при этом затраты как можно ниже. Однако опыт показывает, что поставщики облачных услуг часто жертвуют некоторой безопасностью, чтобы иметь возможность разместить больше пользователей в своих инфраструктурах, для этого они пытаются более эффективно использовать свои ресурсы и обеспечить более высокую производительность приложений своих клиентов.

Рассмотрим разные типы архитектур и сравним их с точки зрения безопасности, данные представлены в таблице 1.

Таблица 1 - Сравнение безопасности различных типов архитектур

	Monolith	**Microservice**	**Serverless**
Вероятность длительным атак	Высокая	Высокая	Низкая
Ответственный за безопасность	Владелец	Владелец	Провайдер
Количество возможных атак	Среднее	Среднее	Большое
Устойчивость к атакам типа "Отказ в обслуживании"	Низкий	Средний	Высокий
Вероятность атаки типа "Доступ к кошельку"	Невозможно	Невозможно	Возможно
Взаимосвязь со сторонними компонентами	Отсутствует	Средняя	Высокая
Риск получения доступа к базовой архитектуре	Высокий	Высокий	Низкий

Рассмотрим решения, которые помогут решить некоторые из описанных проблемы.

Использовать управление ключами без сохранения состояния. Масштабируемая, переносимая и безопасная служба управления ключами позволяет предприятиям полностью контролировать ключи шифрования данных. Генерируемые ключи должны хорошо работать на любой платформе, не требуя расшифровки данных при миграции между различными облачными провайдерами, регионами [1].

Необходимо предусматривать защиту данных в месте их захвата. Serverless вычисления должны предоставлять предприятиям возможность запускать защищенные рабочие нагрузки в средах FaaS. Это позволяет им защищать свои данные в момент их захвата, ограничивая тем самым любые новые проблемы безопасности, которые могут возникнуть в процессе миграции данных.

Использовать многофункциональные криптографические решения. Необходимо делать выбор в пользу криптографических решениях, которые не только поддерживают различные форматы защиты данных, такие как псевдонимизация, методы анонимизации типа токенизации, сохраняющие формат шифрование (FPE) и хэширование, но и позволяют использовать специфические для различных бизнес задач возможности защиты данных.

Благодаря многофункциональным службам криптографической диагностики, независимым от конкретных провайдеров, предприятия могут не только защищать свои данные в месте их захвата, но и использовать защищенные данные для выполнения последующей обработки, в том числе для анализа данных или для использования в

других функциях, основанных на FaaS. FPE позволяет использовать защищенные данные без необходимости дешифровки.

В этой статье было рассмотрено, что serverless вычисления, с одной стороны, обеспечивают дополнительные возможности безопасности, в то время как, с другой стороны, создают новые и уникальные угрозы, что отличает их от современных технологий виртуализации и требует специального направления исследований в области безопасности. В частности, мы рассмотрели особенности serverless архитектуры, классифицировали текущие угрозы безопасности и описали направления исследований в области безопасности, позволяющие сделать serverless архитектуру более предпочтительной при поиске решений для развертывания приложений, где безопасность играет главную роль.

Список использованных источников

1. Сид Д., Усман Ш. Бессерверные вычисления требуют переосмысления подхода к защите данных / Интернет портал itWeek URL: https://www.itweek.ru/its/article/detail.php?ID=217960 (дата обращения 10.10.2022)

2. Поверхность атаки / Энциклопедия Касперского URL: https://encyclopedia.kaspersky.ru/glossary/attack-surface/217960 (дата обращения 11.10.2022)

3. AWS event types. https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/EventTypes.html (дата обращения 11.10.2022)

УДК 533:542.7

Р. Кауымбаев, Н. Сейтказы, Н. Кауымбаева, А. Серикбаева
Таразский региональный университет имени М.Х.Дулати
Тараз, Казахстан

РАЗВИТИЕ ГАЗОВОЙ ОТРАСЛИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. *Газ становится глобальным трендом в мировой экономике, особенно чувствуется это в последнее время. Тенденция к повышению потребления газа наблюдается во всем мире. В Казахстане потребление также*