БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ

Д.В. Хомельянский, Н.В. Ермакович, Е.А. Криштопова

Микросервисная архитектура – сервис-ориентированная архитектура программного обеспечения, направленный на взаимодействие насколько это возможно небольших, слабо связанных и легко изменяемых модулей – микросервисов [1].

Для обеспечения защиты микросервисной архитектуры используются такие сервисы, как: smart endpoints и dumb pipes (клиентские приложения), принцип децентрализованного управления, а также организация управления данными. Как и в традиционных системах функции, обеспечивающие безопасность должны быть встроены в шаблоны архитектуры, дизайна, и интегрирована во весь жизненный цикл разработки, чтобы приложения и данные оставались защищенными.

При использовании платформы облачных вычислений Amazon web services (AWS) предоставляет сервис Amazon Macie, который помогает защитить данные, аккаунты и рабочие нагрузки от несанкционированного доступа. Сервисы защиты данных обеспечивают возможности для шифрования, управления ключами и обнаружения угроз, среди их числа AWS Key Management Service (KMS), AWS CloudHSM (аппаратное хранилище ключей для соответствия нормативным требованиям).

Для идентификации угроз для микросервисных архитектур используются сервисы Security Hub, Network Firewall и Shield, которые непрерывно отслеживают активность в сети и поведение в аккаунтах вашей облачной среды [2]. Каждый микросервис отвечает за конкретно сформированную задачу, при этом является взаимозаменяемым, что позволяет не зависеть от конкретной технологии и полностью соответствует принципам построения микросервисной архитектуры.

Литература

1. Фаулер М., Льюис Д. Микросервисы [Электронный ресурс]. – Режим доступа: https://martinfowler.com/articles/microservices.html. – Дата доступа: 23.03.2021.

2. Amazon веб-сервисы [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ – Дата доступа: 23.03.2021.