MICROSERVICE

KEAMANAN DALAM MICROSERVICE

Disusun Oleh:
AMANDA FAHIRA JURICA
2301083022

SEMESTER 4

PROGRAM STUDI D3 TEKNIK KOMPUTER

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI PADANG

2024/2025

BAB I

PENDAHULUAN

a. Latar belakang

Dalam pengembangan perangkat lunak modern, arsitektur microservice semakin populer karena mampu meningkatkan skalabilitas dan fleksibilitas aplikasi. Microservice membagi sistem menjadi beberapa layanan kecil yang saling berkomunikasi. Meskipun pendekatan ini membawa banyak keuntungan, tantangan keamanan menjadi lebih kompleks karena banyaknya titik komunikasi antar layanan. Oleh karena itu, pemahaman tentang keamanan dalam microservice menjadi hal yang sangat penting.

b. Rumusan Masalah

- Apa saja tantangan keamanan dalam arsitektur microservice?
- Bagaimana cara mengamankan komunikasi antar layanan microservice?
- Teknologi atau pendekatan apa saja yang dapat digunakan untuk meningkatkan keamanan?

c. Tujuan penulisan

- Menjelaskan tantangan keamanan pada arsitektur microservice
- Memberikan gambaran solusi yang bisa digunakan untuk menjaga keamanan
- Meningkatkan pemahaman mahasiswa tentang praktik keamanan dalam pengembangan sistem terdistribusi

BAB II

PEMBAHASAN

a. Pengertian microservie

Microservice adalah pendekatan arsitektur dalam pengembangan aplikasi, di mana setiap fungsi aplikasi dibagi menjadi layanan-layanan kecil yang berjalan secara independen dan bisa saling berkomunikasi melalui protokol jaringan, seperti HTTP atau gRPC.

b. Keamanan dalam konteks microservice

Keamanan dalam microservice berbeda dengan monolitik karena sistem ini lebih terbuka terhadap jaringan dan memiliki lebih banyak "pintu" yang harus diamankan. Oleh karena itu, keamanan menjadi aspek yang krusial agar data dan proses tetap terlindungi.

c. Tantangan keamanan dalam microservice

- Setiap layanan saling berkomunikasi melalui jaringan, sehingga rawan terhadap serangan seperti *man-in-the-middle*.
- Harus dipastikan hanya layanan atau pengguna yang memiliki izin yang bisa mengakses layanan tertentu.
- Manajemen konfigurasi rahasia seperti API key atau password layanan yang harus disimpan secara aman.
- Monitoring dan logging harus bisa mendeteksi aktivitas mencurigakan atau serangan terhadap sistem.
- Serangan internal (insider attack) karena layanan tersebar, bisa saja ada celah dari dalam.

d. Solusi keamanan untuk microservice

- **Otentikasi dan Otorisasi Terpusat**
  Gunakan sistem seperti OAuth2 atau OpenID Connect untuk memastikan setiap layanan bisa memverifikasi identitas layanan lain atau pengguna.
- **Gateway API**
  Dengan menggunakan API Gateway, semua permintaan masuk bisa disaring di satu titik. API Gateway juga bisa menangani otentikasi, otorisasi, dan rate-limiting.
- **TLS (Transport Layer Security)**
  Semua komunikasi antar layanan sebaiknya dienkripsi menggunakan TLS untuk mencegah penyadapan.
- **Service Mesh (contohnya Istio atau Linkerd)**
  Service mesh membantu mengelola komunikasi antar layanan, termasuk fitur keamanan seperti mutual TLS (mTLS), tracing, dan load balancing secara otomatis.

- **Penyimpanan Rahasia dengan Aman**
  Gunakan tools seperti HashiCorp Vault atau Secret Manager dari cloud provider untuk menyimpan informasi sensitif.
- **Logging dan Monitoring**
  Gunakan tools seperti Prometheus, Grafana, dan ELK Stack (Elasticsearch, Logstash, Kibana) untuk memantau aktivitas layanan dan mendeteksi anomali.

BAB III

PENUTUP

a. Kesimpulan

Keamanan dalam arsitektur microservice sangat penting dan tidak bisa dianggap sepele. Tantangan yang muncul lebih kompleks dibanding arsitektur monolitik, karena banyaknya interaksi antar layanan. Namun, dengan pendekatan yang tepat seperti penggunaan API Gateway, TLS, otentikasi terpusat, dan service mesh, keamanan dapat tetap dijaga.

b. Saran

Mahasiswa dan pengembang perlu memahami bahwa keamanan bukan hanya soal alat, tetapi juga budaya dan proses. Maka, penting untuk terus belajar dan mengikuti perkembangan teknologi keamanan agar sistem yang dikembangkan tetap aman dan andal.