**A black and white logo

Description automatically generated**

**MAKALAH**

**MICROSERVICE TRORI**

**KEAMANAN DALAM MICROSERVICE**

**SEMESTER 4**

**DISUSUN OLEH**

**MHD. RAZIN YASSAR**

**2301083005**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI TEKNIK KOMPUTER**

**POLITEKNIK NEGERI PADANG**

**2025**

1. Pendahuluan

Arsitektur layanan mikro telah merevolusi cara aplikasi dibangun, memungkinkan kelincahan, skalabilitas, dan fleksibilitas yang lebih besar. Namun, pendekatan terdesentralisasi ini memperkenalkan tantangan keamanan unik yang harus ditangani untuk melindungi data sensitif, memastikan kepatuhan, dan menjaga kepercayaan pengguna. Makalah ini mengeksplorasi tantangan keamanan yang melekat dalam layanan mikro, praktik terbaik untuk memerangi ancaman ini, dan alat dan teknologi yang dapat meningkatkan keamanan.

1. Memahami Tantangan Keamanan Layanan Mikro

Arsitektur layanan mikro memungkinkan aplikasi terdiri dari layanan kecil dan independen yang berkomunikasi melalui jaringan. Meskipun modularitas ini memberikan banyak keuntungan, modularitas ini juga menimbulkan beberapa masalah keamanan:

* 1. Peningkatan Permukaan Serangan

Setiap layanan mikro meningkatkan permukaan serangan secara keseluruhan secara signifikan. Setiap layanan memiliki titik akhirnya sendiri dan berpotensi menjadi target penyerang. Interaksi antar layanan, seringkali melalui internet, memperparah risiko ini.

* 1. Komunikasi Antar-Layanan

Layanan mikro berkomunikasi melalui API atau broker pesan. Jika komunikasi ini tidak diamankan dengan benar, penyerang dapat mencegat data atau menyuntikkan muatan berbahaya. Memastikan saluran komunikasi yang aman (misalnya, HTTPS, jaring layanan) sangat penting.

* 1. Otentikasi dan Otorisasi

Dalam ekosistem layanan mikro, mengelola autentikasi dan otorisasi dapat menjadi berbelit-belit. Setiap layanan mungkin memerlukan mekanisme otentikasinya sendiri, yang menyebabkan praktik keamanan yang tidak konsisten dan meningkatkan risiko akses yang tidak sah.

* 1. Masalah Keamanan Data dan Privasi

Data sering dikirim ke berbagai layanan dan dapat disimpan di beberapa lokasi. Melindungi informasi sensitif, memastikan enkripsi dalam perjalanan dan saat tidak aktif, dan mematuhi peraturan privasi data (misalnya, GDPR) menjadi semakin kompleks.

1. Praktik Terbaik untuk Mengamankan Layanan Mikro

Mengamankan layanan mikro membutuhkan pendekatan berlapis-lapis. Di bawah ini adalah praktik terbaik utama yang ditujukan untuk meningkatkan keamanan arsitektur layanan mikro:

* 1. Keamanan API

- Gunakan Token untuk Autentikasi: Terapkan OAuth2 atau JWT (JSON Web Tokens) untuk autentikasi pengguna yang aman dan komunikasi layanan-ke-layanan. Mekanisme ini memungkinkan kontrol akses terperinci.

- Pembatasan Kecepatan dan Pembatasan: Terapkan teknik pembatasan kecepatan pada API untuk mengurangi risiko serangan penolakan layanan dan mencegah penyalahgunaan.

* 1. Keamanan Jaringan

- Service Mesh: Terapkan kerangka kerja mesh layanan (seperti Istio atau Linkerd) untuk mengelola komunikasi layanan-ke-layanan yang aman. Kerangka kerja ini menyediakan TLS timbal balik untuk enkripsi dan dapat membantu dalam otentikasi dan otorisasi.

- Firewall dan Virtual Private Network: Gunakan firewall untuk membatasi akses ke layanan dan pertimbangkan untuk menerapkan layanan dalam VPN untuk keamanan tambahan.

* 1. Pemantauan dan Pencatatan

- Terapkan Pencatatan Terpusat: Pencatatan terpusat membantu melacak interaksi layanan dan mengidentifikasi anomali. Alat seperti tumpukan ELK (Elasticsearch, Logstash, Kibana) dapat memfasilitasi pemantauan waktu nyata.

- Manajemen Informasi dan Peristiwa Keamanan (SIEM): Manfaatkan solusi SIEM untuk menganalisis log dan data untuk aktivitas mencurigakan di seluruh ekosistem layanan mikro.

* 1. Penilaian Keamanan Reguler

- Lakukan Pengujian Penetrasi: Lakukan pengujian penetrasi secara teratur untuk menemukan kerentanan dalam setiap layanan mikro dan mengatasi masalah ini sebelum penyerang mengeksploitasinya.

- Pemindaian Keamanan Otomatis: Gabungkan alat pengujian keamanan otomatis (seperti Snyk atau Aqua Security) ke dalam alur CI/CD untuk mengidentifikasi kerentanan dalam dependensi dan konfigurasi.

1. Alat dan Teknologi

Banyak alat dapat membantu mengamankan layanan mikro. Beberapa yang terkenal meliputi:

- Kubernetes: Menawarkan kontrol keamanan bawaan untuk mengelola layanan mikro dalam kontainer, termasuk kontrol akses berbasis peran (RBAC) dan Kebijakan Keamanan Pod.

- Envoy Proxy: Sering digunakan sebagai proxy sidecar dalam arsitektur mesh layanan, ia mengelola lalu lintas dan menyediakan fitur keamanan yang kuat.

- Open Policy Agent (OPA): Alat sumber terbuka yang membantu menegakkan kontrol akses terperinci dan sadar konteks di seluruh layanan mikro.

1. Kesimpulan

Meskipun arsitektur layanan mikro menawarkan manfaat substansial, arsitektur ini juga menimbulkan tantangan keamanan unik yang harus ditangani organisasi secara proaktif. Dengan memahami risiko yang melekat dan menerapkan praktik dan alat terbaik, pengembang dan tim keamanan dapat menciptakan lingkungan layanan mikro yang aman. Kewaspadaan, pendidikan, dan adaptasi yang berkelanjutan terhadap ancaman yang muncul akan sangat penting untuk memastikan keamanan yang kuat dalam lanskap yang berkembang pesat ini. Pada akhirnya, postur keamanan yang kuat tidak hanya melindungi organisasi tetapi juga meningkatkan kepercayaan pengguna terhadap layanan yang diberikan.

1. Referensi

“Spring Security Reference.” Spring Framework Documentation.

<https://spring.io/projects/spring-security>

“Open Policy Agent.” Open Policy Agent Documentation.

<https://www.openpolicyagent.org/docs/latest/>