**MAKALAH MICROSERVICE**

**KEAMANAN DALAM MICROSERVICE**



**Disusun Oleh :**

**Mhd. Rizki Asyafiq**

**2301083006**

**KELAS 2A TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI D3 TEKNIK KOMPUTER**

**POLITEKNIK NEGERI PADANG**

**2025**

**KATA PENGANTAR**

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, makalah yang berjudul "Keamanan dalam Microservices" ini dapat diselesaikan dengan baik dan tepat waktu.

Makalah ini disusun sebagai salah satu bentuk tugas dalam rangka memperdalam pemahaman mengenai aspek keamanan pada arsitektur microservices, yang saat ini banyak digunakan dalam pengembangan perangkat lunak modern. Penulis berusaha menyajikan informasi yang relevan, mulai dari tantangan keamanan yang dihadapi, strategi pengamanan, hingga contoh implementasi di dunia nyata.

Penulis menyadari bahwa dalam penyusunan makalah ini masih terdapat kekurangan, baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca demi perbaikan di masa yang akan datang.

Ucapan terima kasih penulis sampaikan kepada semua pihak yang telah membantu dalam penyusunan makalah ini, khususnya kepada dosen pengampu dan rekan-rekan yang telah memberikan masukan serta dukungan.

Akhir kata, semoga makalah ini dapat memberikan manfaat dan menambah wawasan bagi pembaca.

Padang , 08 April 2025

Penyusun

**DAFTAR ISI**

[KATA PENGANTAR ii](#_Toc195020427)

[DAFTAR ISI iii](#_Toc195020428)

[BAB 1 1](#_Toc195020429)

[PENDAHULUAN 1](#_Toc195020430)

[1.1. Latar Belakang 1](#_Toc195020431)

[1.2. Rumusan Masalah 1](#_Toc195020432)

[1.3. Tujuan Penulisan 1](#_Toc195020433)

[BAB II 2](#_Toc195020434)

[PEMBAHASAN 2](#_Toc195020435)

[2.1. Tantangan Keamanan dalam Microservices 2](#_Toc195020436)

[2.2. Strategi Keamanan dalam Microservices 2](#_Toc195020437)

2.3. Contoh Implementasi Keamanan Microservice……………………………………………………….. 3

[BAB III 4](#_Toc195020438)

[PENUTUP 4](#_Toc195020439)

[3.1. Kesimpulan 4](#_Toc195020440)

[3.2. Saran 4](#_Toc195020441)

[DAFTAR PUSTAKA 5](#_Toc195020442)

**BAB 1**

**PENDAHULUAN**

**1.1. Latar Belakang**

Arsitektur microservices telah menjadi pilihan utama dalam pengembangan perangkat lunak modern karena kemampuannya dalam memecah sistem besar menjadi layanan-layanan kecil yang independen. Keunggulan seperti fleksibilitas, skalabilitas, dan kemudahan pemeliharaan membuat microservices banyak diadopsi oleh perusahaan teknologi besar seperti Netflix, Amazon, dan Google. Namun, arsitektur ini juga memperkenalkan tantangan baru dalam hal keamanan. Tidak seperti sistem monolitik, setiap layanan dalam microservices berkomunikasi melalui jaringan, sehingga membuka banyak celah keamanan seperti serangan man-in-the-middle, injeksi, atau eksploitasi API.

**1.2. Rumusan Masalah**

* Apa saja tantangan keamanan utama dalam arsitektur microservices?
* Bagaimana cara mengamankan komunikasi antar layanan microservice?
* Apa peran autentikasi dan otorisasi dalam kemanana microservices?

**1.3. Tujuan Penulisan**

* Menjelaskan risiko dan tantangan keamanan pada sistem microservices.
* Menguraikan strategi dan praktik terbaik dalam mengamankan microservices.
* Memberikan contoh implementasi keamanan microservices di industri.
* Meningkatkan kesadaran akan pentingnya pendekatan keamanan yang terdistribusi.

**BAB II**

**PEMBAHASAN**

**2.1. Tantangan Keamanan dalam Microservices**

* Kompleksitas Komunikasi Jaringan: Setiap layanan berkomunikasi melalui API, meningkatkan risiko serangan seperti man-in-the-middle, DDoS, atau eksploitasi endpoint yang tidak diamankan
* Permukaan Serangan yang Lebih Luas: Setiap layanan memiliki endpoint sendiri, sehingga serangan dapat terjadi di banyak titik.
* Manajemen Identitas dan Akses: Kesulitan dalam menerapkan kontrol akses yang konsisten di seluruh layanan.
* Pemantauan dan Logging: Membutuhkan sistem terdistribusi untuk mendeteksi anomali secara real-time.

**2.2. Strategi Keamanan dalam Microservices**

* Autentikasi dan Otorisasi Terpusat: Gunakan protokol seperti OAuth2, OpenID Connect, atau JWT, Implementasi API Gateway (e.g., Kong, Apigee) untuk mengelola akses.
* Enkripsi Komunikasi: Wajibkan penggunaan HTTPS/TLS untuk semua komunikasi antar layanan.
* Zero Trust Security Model: Setiap permintaan harus diverifikasi, tidak ada yang dipercaya secara default.
* Rate Limiting dan Circuit Breaker: Cegah penyalahgunaan dengan membatasi permintaan per pengguna (e.g., menggunakan Redis).
* Security Testing & DevSecOps: Integrasikan keamanan sejak awal dengan tools seperti SonarQube, Snyk, atau OWASP ZAP.

**2.3 Contoh Implementasi Keamanan Microservices**

- Netflix: Menggunakan Zuul sebagai API Gateway dan sistem pemantauan real-time.

- Amazon: Menerapkan enkripsi end-to-end dan IAM (Identity and Access Management) untuk otorisasi.

- Kubernetes: Menyediakan fitur Network Policies untuk mengisolasi lalu lintas antar layanan.

**BAB III**

**PENUTUP**

**3.1. Kesimpulan**

Keamanan dalam microservices memerlukan pendekatan holistik, mulai dari enkripsi komunikasi, manajemen identitas, hingga pemantauan terdistribusi. Prinsip "defense in depth" harus diterapkan untuk meminimalkan risiko.

**3.2. Saran**

* Tim pengembang dan keamanan harus berkolaborasi sejak fase desain.
* Adopsi DevSecOps untuk mengintegrasikan keamanan secara otomatis.
* Lakukan pelatihan rutin tentang keamanan microservices untuk tim.

**DAFTAR PUSTAKA**

Newman, S. (2015). Building Microservices. O'Reilly Media.

OWASP Foundation. (2023). OWASP Cloud-Native Application Security Top 10.

OWASP Cheat Sheet Series. (2023). Microservices Security Cheat Sheet.

Microsoft Docs. (2023). Best Practices for Securing Microservices.