MAKALAH

KEAMANAN DALAM MICROSERVICES

DISUSUN OLEH :

AULIA RAHMI

2301081001

TK 2A

JURUSAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK KOMPUTER

POLITEKNIK NEGERI PADANG

2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Arsitektur microservices adalah pendekatan pengembangan perangkat lunak yang membagi aplikasi menjadi layanan-layanan kecil, independen, dan saling terhubung melalui API atau protokol tertentu. Meskipun memberikan banyak keuntungan seperti skalabilitas dan fleksibilitas, pendekatan ini juga menghadirkan tantangan keamanan yang lebih kompleks dibandingkan arsitektur monolitik.

Menurut laporan Cybersecurity Ventures, serangan terhadap API meningkat sebesar 300% dalam lima tahun terakhir, menunjukkan perlunya perhatian serius terhadap keamanan dalam arsitektur microservices.

1.2 Rumusan Masalah

- Apa saja tantangan keamanan yang dihadapi dalam arsitektur microservices?
- Strategi apa saja yang dapat diterapkan untuk meningkatkan keamanan microservices?

1.3 Tujuan Penulisan

- Menjelaskan konsep keamanan dalam microservices.
- Mengidentifikasi tantangan keamanan yang dihadapi.
- Memberikan rekomendasi strategi keamanan untuk mengatasi tantangan tersebut.

1.4 Manfaat Penulisan

Makalah ini diharapkan dapat menjadi referensi bagi pengembang perangkat lunak, tim keamanan IT, dan akademisi untuk memahami pentingnya keamanan dalam arsitektur microservices serta cara mengimplementasikannya.

BAB II

TINJAUAN PUSTAKA

2.1 Pengertian Microservices

Microservices adalah pendekatan pengembangan perangkat lunak yang membagi aplikasi menjadi layanan-layanan kecil, independen, dan saling terhubung melalui API atau protokol tertentu (Newman, 2015). Dengan pendekatan ini, setiap layanan dapat dikembangkan, diuji, dan dikelola secara terpisah.

2.2 Konsep Keamanan dalam Arsitektur Microservices

Keamanan dalam microservices melibatkan berbagai aspek seperti autentikasi, otorisasi, enkripsi data, pemantauan aktif, serta penerapan prinsip zero trust untuk memastikan setiap layanan terlindungi dari ancaman eksternal maupun internal (Gonzalez et al., 2020).

2.3 Tantangan Keamanan pada Microservices

Beberapa tantangan utama meliputi:

- **Kompleksitas komunikasi antar-layanan**: Meningkatkan risiko serangan seperti *man-in-the-middle* (MiTM).
- **Banyaknya titik akses API**: Setiap layanan memiliki API yang dapat menjadi target serangan jika tidak diamankan dengan baik.
- **Perlindungan data sensitif**: Data sensitif yang tersebar di berbagai layanan membutuhkan strategi perlindungan yang kuat.

BAB III

PEMBAHASAN

3.1 Strategi Keamanan dalam Microservices

3.1.1 Pengamanan Komunikasi

Gunakan protokol HTTPS/TLS untuk mengenkripsi data antar-microservices dan implementasikan autentikasi antar-layanan (*service-to-service authentication*). Sertifikat SSL digunakan untuk memastikan identitas layanan yang berkomunikasi sehingga mencegah serangan *man-in-the-middle* (Meyer et al., 2020).

3.1.2 Autentikasi dan Otorisasi

Terapkan mekanisme autentikasi berbasis token seperti OAuth atau JWT serta kontrol akses berbasis peran (RBAC) untuk membatasi akses sesuai kebutuhan (Hardt, 2012). Misalnya:

- OAuth digunakan untuk memberikan akses terbatas kepada aplikasi pihak ketiga tanpa membagikan kredensial pengguna.

3.1.3 Keamanan API

Gunakan API gateway sebagai titik kontrol tunggal untuk mengelola permintaan eksternal dan internal serta validasi input untuk mencegah serangan injeksi seperti SQL injection atau cross-site scripting (XSS) (Nash et al., 2019).

3.1.4 Manajemen Data dan Enkripsi

Enkripsi data sensitif saat transit (menggunakan TLS) dan saat istirahat menggunakan algoritma seperti AES atau RSA (Kahn et al., 2020). Gunakan alat manajemen rahasia seperti HashiCorp Vault untuk mengelola kredensial secara aman.

3.1.5 Pemantauan dan Logging

Implementasikan sistem pemantauan terpusat menggunakan alat seperti SIEM (Security Information and Event Management) atau IDS (Intrusion Detection System) untuk mendeteksi ancaman secara proaktif (Sullivan et al., 2020).

3.1.6 Zero Trust Architecture (ZTA)

Terapkan prinsip "never trust, always verify" dengan autentikasi terpusat menggunakan alat seperti Keycloak untuk memastikan setiap permintaan akses diverifikasi tanpa asumsi kepercayaan sebelumnya (Chow et al., 2020).

3.1.7 Pengujian Keamanan

Lakukan pengujian penetrasi secara berkala untuk mengidentifikasi kelemahan sistem serta evaluasi konfigurasi keamanan secara rutin menggunakan alat seperti OWASP ZAP atau Burp Suite.

3.2 Studi Kasus Implementasi Keamanan Microservices

Studi Kasus: Netflix

Netflix adalah contoh sukses penerapan arsitektur microservices dengan fokus pada keamanan:

- Netflix menggunakan Spring Boot untuk membangun microservices-nya.
- Mereka menerapkan *service-to-service authentication* menggunakan OAuth2 dan JWT.
- Penggunaan API Gateway memungkinkan mereka mengelola trafik masuk dengan aman serta menerapkan throttling dan rate limiting untuk mencegah serangan DDoS.

Studi Kasus: Amazon Web Services (AWS)

Amazon menggunakan AWS Lambda untuk menjalankan fungsi tanpa server yang terintegrasi dengan microservices mereka:

- Menggunakan IAM (Identity and Access Management) untuk kontrol akses ketat.
- Data sensitif dienkripsi menggunakan AWS KMS (Key Management Service) saat istirahat dan saat transit.

BAB IV

KESIMPULAN DAN SARAN

4.1 Kesimpulan

Keamanan dalam microservices merupakan aspek penting yang harus diperhatikan guna melindungi data, layanan, dan pengguna dari ancaman eksternal maupun internal. Dengan menerapkan strategi keamanan yang tepat, organisasi dapat membangun sistem microservices yang tangguh terhadap ancaman.

4.2 Saran

Pengembang perlu menerapkan strategi keamanan secara holistik dengan memanfaatkan teknologi terbaru seperti enkripsi data, zero trust architecture, serta pengujian penetrasi secara berkala untuk memastikan sistem tetap aman.

DAFTAR PUSTAKA

Chow, R., Golle, P., & Staddon, J.(2020). "Zero Trust Security." IEEE Security & Privacy.

Gonzalez, A., & Velez, J.(2020). "Microservices Security: Challenges and Solutions." Journal of Computer Networks and Communications.