**Nama : Ryan Kevin Arielotha**

**NIM : 2301081014**

**Matkul : Microservice**

**KEAMANAN DALAM MICROSERVICES**

**BAB I: PENDAHULUAN**

**1.1 Latar Belakang** Microservices adalah pendekatan arsitektur dalam pengembangan perangkat lunak di mana aplikasi dibangun sebagai kumpulan layanan kecil yang dapat berjalan secara independen. Keamanan dalam microservices menjadi tantangan karena sifat terdistribusi dari sistem ini, yang meningkatkan risiko serangan dan kebocoran data.

**1.2 Rumusan Masalah**

1. Apa saja tantangan keamanan dalam arsitektur microservices?
2. Bagaimana cara mengamankan komunikasi antar layanan dalam microservices?
3. Teknologi dan metode apa yang dapat digunakan untuk meningkatkan keamanan microservices?

**1.3 Tujuan Penelitian** Makalah ini bertujuan untuk:

1. Mengidentifikasi tantangan keamanan dalam microservices.
2. Menjelaskan metode perlindungan komunikasi antar layanan.
3. Menyajikan teknologi dan strategi yang dapat digunakan untuk meningkatkan keamanan.

**BAB II: TANTANGAN KEAMANAN DALAM MICROSERVICES**

**2.1 Identifikasi Ancaman**

1. **Serangan Man-in-the-Middle (MitM):** Penyusup dapat mencegat komunikasi antar layanan.
2. **Serangan Injection:** Seperti SQL Injection atau Code Injection yang bisa mengeksploitasi kelemahan API.
3. **Masalah Otorisasi dan Autentikasi:** Tidak adanya sistem identitas yang kuat dapat menyebabkan akses tidak sah.
4. **Keamanan Data dalam Transportasi dan Penyimpanan:** Data yang tidak dienkripsi dapat mudah dicuri.

**2.2 Kompleksitas dalam Pengelolaan Keamanan** Karena microservices terdiri dari banyak layanan yang berjalan secara independen, mengelola keamanan menjadi lebih sulit dibandingkan dengan arsitektur monolitik.

**BAB III: STRATEGI KEAMANAN MICROSERVICES**

**3.1 Autentikasi dan Otorisasi**

* **OAuth 2.0 dan OpenID Connect:** Digunakan untuk manajemen identitas pengguna.
* **JSON Web Token (JWT):** Digunakan untuk otentikasi tanpa status.

**3.2 Keamanan API**

* **Rate Limiting dan Throttling:** Membatasi jumlah permintaan yang dapat diterima API.
* **Validasi Input:** Mencegah serangan injection.
* **Gateway API:** Bertindak sebagai pengaman dan pengontrol akses ke layanan.

**3.3 Keamanan Jaringan dan Komunikasi Antar Layanan**

* **TLS/SSL:** Untuk mengenkripsi komunikasi antar layanan.
* **Service Mesh (Istio, Linkerd):** Mengelola lalu lintas jaringan dan keamanan antar layanan.

**3.4 Pemantauan dan Logging**

* **Centralized Logging:** Menggunakan ELK Stack atau Prometheus untuk pemantauan keamanan.
* **Intrusion Detection System (IDS):** Mendeteksi aktivitas mencurigakan dalam sistem.

**BAB IV: IMPLEMENTASI TEKNOLOGI KEAMANAN**

**4.1 Penggunaan Kubernetes untuk Keamanan Microservices** Kubernetes menyediakan fitur seperti Network Policies, Role-Based Access Control (RBAC), dan Secrets Management untuk meningkatkan keamanan dalam ekosistem microservices.

**4.2 Penggunaan API Gateway untuk Keamanan** API Gateway seperti Kong atau Apigee berfungsi sebagai lapisan tambahan yang mengatur lalu lintas dan mengimplementasikan autentikasi serta otorisasi.

**4.3 Service Mesh untuk Keamanan dan Manajemen Lalu Lintas** Service Mesh memungkinkan keamanan berbasis proxy, seperti mutual TLS (mTLS) untuk komunikasi aman antar layanan.

**BAB V: KESIMPULAN DAN SARAN**

**5.1 Kesimpulan** Keamanan dalam microservices merupakan aspek penting yang harus diperhatikan dalam pengembangan perangkat lunak berbasis layanan. Dengan menerapkan autentikasi yang kuat, enkripsi komunikasi, serta pemantauan yang baik, risiko keamanan dapat diminimalisir.

**5.2 Saran** Diperlukan pendekatan yang holistik dan berlapis dalam implementasi keamanan microservices, termasuk penerapan standar keamanan modern serta pemantauan secara kontinu untuk mendeteksi dan mengatasi ancaman dengan cepat.