# MAKALAH KEAMANAN DALAM MICROSERVICE

**“Menerapkan Pendekatan Zero Trust dalam Keamanan Microservices”**

****

**Oleh:**

**Rasihan Yusri Mazid (2301081011)**

**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI PADANG**

**2025**

**Kata Pengantar**

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan makalah yang berjudul "Menerapkan Pendekatan Zero Trust dalam Keamanan Microservices: Tantangan dan Solusi". Makalah ini disusun sebagai salah satu tugas dalam mata kuliah Keamanan Sistem Informasi.

Dalam penyusunan makalah ini, penulis berusaha memberikan pemahaman mengenai pentingnya penerapan pendekatan Zero Trust sebagai solusi untuk mengatasi tantangan keamanan dalam arsitektur microservices yang semakin banyak diadopsi dalam pengembangan aplikasi modern. Penulis berharap makalah ini dapat memberikan manfaat dan wawasan baru bagi pembaca, khususnya dalam bidang keamanan sistem informasi.

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

Akhir kata, penulis mengucapkan terima kasih kepada dosen pengampu mata kuliah serta semua pihak yang telah memberikan dukungan dan bantuan dalam penyusunan makalah ini.

Padang, 8 April 2025

Penulis

**DAFTAR ISI**

**Cover ...................................................................................................................... i**

**Kata Pengantar ...................................................................................................... ii**

**Daftar Isi ................................................................................................................ iii**

**BAB I PENDAHULUAN ..................................................................................... 1**

**1.1 Latar Belakang 1**

**1.2 Tujuan Penulisan 1**

**1.3 Pentingnya Keamanan dalam Arsitektur Microservices 1**

**1.4 Pengantar Pendekatan Zero Trust 1**

**BAB II KONSEP DASAR MICROSERVICES ..................................................... 2**

**2.1 Definisi Microservices 2**

**2.2 Karakteristik Microservices 2**

**2.3 Keuntungan dan Kerugian Microservices 2**

**2.4 Peran Microservices dalam Pengembangan Aplikasi Modern 2**

**BAB III PENDEKATAN ZERO TRUST ............................................................. 3**

**3.1 Definisi Zero Trust 3**

**3.2 Prinsip Utama Zero Trust 3**

**3.3 Perbandingan dengan Model Keamanan Tradisional 3**

**3.4 Manfaat Penerapan Zero Trust 3**

**BAB IV TANTANGAN PENERAPAN ZERO TRUST DALAM MICROSERVICES ... 4**

**4.1 Kompleksitas Arsitektur Microservices 4**

**4.2 Manajemen Identitas dan Akses 4**

**4.3 Pengawasan dan Monitoring yang Efektif 4**

**4.4 Integrasi dengan Sistem yang Ada 4**

**4.5 Keterbatasan Sumber Daya dan Keahlian 4**

**BAB V SOLUSI UNTUK MENGATASI TANTANGAN ...................................... 5**

**5.1 Implementasi Otentikasi dan Otorisasi yang Kuat 5**

**5.2 Penggunaan Teknologi Enkripsi 5**

**5.3 Penerapan Micro-Segmentation 5**

**5.4 Penggunaan Alat dan Platform Keamanan yang Tepat 5**

**5.5 Pelatihan dan Kesadaran Keamanan bagi Tim Pengembang 5**

**BAB VI STUDI KASUS ..................................................................................... 6**

**6.1 Contoh Perusahaan yang Berhasil Menerapkan Zero Trust 6**

**6.2 Analisis Keberhasilan dan Pembelajaran dari Implementasi 6**

**6.3 Dampak Penerapan Zero Trust terhadap Keamanan dan Kinerja 6**

**BAB VII KESIMPULAN ..................................................................................... 7**

**7.1 Ringkasan Temuan Utama 7**

**7.2 Pentingnya Penerapan Zero Trust dalam Keamanan Microservices 7**

**7.3 Rekomendasi untuk Penelitian dan Implementasi Selanjutnya 7**

**DAFTAR PUSTAKA ............................................................................................ 8**

# BAB I

# Pendahuluan

## 1.1 Latar Belakang

Arsitektur microservices telah menjadi pilihan utama dalam pengembangan perangkat lunak modern karena kemampuannya dalam meningkatkan skalabilitas, fleksibilitas, dan kecepatan pengembangan. Namun, kompleksitas sistem yang meningkat menimbulkan tantangan besar dalam hal keamanan. Model keamanan tradisional yang mengandalkan perimeter tidak lagi memadai untuk melindungi sistem microservices yang sangat dinamis dan tersebar.

## 1.2 Tujuan Penulisan

Makalah ini bertujuan untuk menjelaskan pentingnya pendekatan Zero Trust dalam meningkatkan keamanan arsitektur microservices. Selain itu, makalah ini akan membahas tantangan yang dihadapi dalam penerapannya serta solusi yang dapat diterapkan untuk mengatasinya.

## 1.3 Pentingnya Keamanan dalam Arsitektur Microservices

Keamanan menjadi aspek yang sangat krusial dalam microservices karena setiap layanan dapat menjadi titik serangan. Tanpa pendekatan keamanan yang tepat, sistem microservices rentan terhadap berbagai jenis ancaman seperti penyusupan, kebocoran data, dan serangan internal.

## 1.4 Pengantar Pendekatan Zero Trust

Zero Trust adalah pendekatan keamanan yang menghilangkan kepercayaan implisit di dalam jaringan dan menggantinya dengan model "never trust, always verify". Setiap permintaan akses harus diverifikasi tanpa memandang asal permintaan, baik dari dalam maupun luar jaringan.

# BAB II

# Konsep Dasar Microservices

## 2.1 Definisi Microservices

Microservices adalah pendekatan arsitektur perangkat lunak di mana aplikasi dibangun sebagai kumpulan layanan kecil yang dapat dikembangkan, diuji, dan dideploy secara independen.

## 2.2 Karakteristik Microservices

Karakteristik utama dari microservices antara lain: layanan yang terdesentralisasi, independen, ringan, dapat diskalakan, dan berbasis API untuk komunikasi antar layanan.

## 2.3 Keuntungan dan Kerugian Microservices

**Keuntungan:** Skalabilitas tinggi, pengembangan independen, fleksibilitas dalam penggunaan teknologi.

**Kerugian:** Kompleksitas manajemen, potensi kesalahan komunikasi antar layanan, kebutuhan akan alat pemantauan dan keamanan yang lebih canggih.

## 2.4 Peran Microservices dalam Pengembangan Aplikasi Modern

Microservices memungkinkan pengembangan perangkat lunak secara cepat dan adaptif terhadap perubahan kebutuhan bisnis, menjadikannya sangat relevan dalam era DevOps dan CI/CD.

# BAB III

# Pendekatan Zero Trust

## 3.1 Definisi Zero Trust

Zero Trust adalah model keamanan jaringan yang tidak mengasumsikan kepercayaan terhadap entitas apa pun baik di dalam maupun di luar jaringan.

## 3.2 Prinsip Utama Zero Trust

1. Verifikasi identitas dan konteks setiap permintaan.

2. Batasi akses berdasarkan prinsip least privilege.

3. Gunakan segmentasi mikro untuk memisahkan beban kerja.

4. Lakukan pemantauan dan log aktivitas secara terus menerus.

## 3.3 Perbandingan dengan Model Keamanan Tradisional

Model tradisional mengandalkan firewall perimeter, sementara Zero Trust memfokuskan keamanan pada setiap elemen sistem tanpa mengandalkan zona aman.

## 3.4 Manfaat Penerapan Zero Trust

- Mengurangi risiko serangan internal

- Peningkatan kontrol akses

- Deteksi dan respon ancaman yang lebih cepat

- Peningkatan kepatuhan terhadap regulasi

BAB IV

Tantangan Penerapan Zero Trust dalam Microservices

4.1 Kompleksitas Arsitektur MicroservicesJumlah layanan yang besar dan ketergantungan antar layanan menambah kompleksitas dalam menerapkan kebijakan Zero Trust.

4.2 Manajemen Identitas dan AksesMenetapkan identitas unik untuk setiap layanan dan pengguna serta mengelola hak akses memerlukan sistem otentikasi dan otorisasi yang kuat.

4.3 Pengawasan dan Monitoring yang EfektifDiperlukan alat dan sistem pemantauan yang mampu memberikan visibilitas menyeluruh terhadap interaksi antar layanan.

4.4 Integrasi dengan Sistem yang AdaMengadopsi Zero Trust memerlukan perubahan besar terhadap sistem lama yang belum dirancang untuk mendukung model ini.

4.5 Keterbatasan Sumber Daya dan KeahlianKurangnya sumber daya manusia yang memahami Zero Trust serta keterbatasan anggaran menjadi penghalang utama penerapannya.

BAB V

Solusi untuk Mengatasi Tantangan

5.1 Implementasi Otentikasi dan Otorisasi yang KuatMenggunakan protokol standar seperti OAuth 2.0 dan OpenID Connect untuk autentikasi serta penerapan RBAC atau ABAC.

5.2 Penggunaan Teknologi EnkripsiMengamankan komunikasi antar layanan dengan enkripsi TLS dan penyimpanan data dengan enkripsi AES.

5.3 Penerapan Micro-SegmentationMembagi jaringan menjadi beberapa segmen kecil agar dapat mengisolasi potensi serangan dan membatasi penyebarannya.

5.4 Penggunaan Alat dan Platform Keamanan yang TepatMengintegrasikan layanan keamanan seperti API gateway, service mesh (misalnya Istio), dan sistem pemantauan keamanan.

5.5 Pelatihan dan Kesadaran Keamanan bagi Tim PengembangMeningkatkan literasi keamanan melalui pelatihan berkelanjutan dan integrasi praktik keamanan dalam pengembangan.

BAB VI

Studi Kasus

6.1 Contoh Perusahaan yang Berhasil Menerapkan Zero TrustGoogle dengan inisiatif BeyondCorp berhasil menerapkan model Zero Trust secara menyeluruh untuk karyawan dan layanannya.

6.2 Analisis Keberhasilan dan Pembelajaran dari ImplementasiKeberhasilan BeyondCorp menunjukkan pentingnya perencanaan, investasi jangka panjang, dan dukungan dari manajemen.

6.3 Dampak Penerapan Zero Trust terhadap Keamanan dan Kinerja MicroservicesPeningkatan deteksi dini terhadap serangan, pengurangan akses tidak sah, serta peningkatan efisiensi pengelolaan sistem.

BAB VII

Kesimpulan

7.1 Ringkasan Temuan UtamaPenerapan Zero Trust dalam arsitektur microservices penting untuk meningkatkan ketahanan terhadap ancaman modern. Tantangan dalam penerapan dapat diatasi dengan strategi dan teknologi yang tepat.

7.2 Pentingnya Penerapan Zero Trust dalam Keamanan MicroservicesZero Trust membantu menciptakan sistem yang lebih aman, fleksibel, dan siap menghadapi berbagai bentuk serangan siber.

7.3 Rekomendasi untuk Penelitian dan Implementasi SelanjutnyaDiperlukan penelitian lebih lanjut mengenai otomatisasi dalam Zero Trust dan pengembangan toolset yang lebih efisien serta edukasi yang menyeluruh bagi pengembang.

**Daftar Pustaka**

Kindervag, J. (2010). "No More Chewy Centers: Introducing the Zero Trust Model of Information Security". Forrester Research.

Google. (n.d.). BeyondCorp: A New Approach to Enterprise Security.

NIST Special Publication 800-207: Zero Trust Architecture.

Newman, S. (2015). "Building Microservices: Designing Fine-Grained Systems". O'Reilly Media.

Fowler, M. (2014). Microservices - a definition of this new architectural term.