ZERO TRUST

APPLICATION & WORKLOAD

Zero Trust Application

Fokus: Sichere App-Nutzung

- Anwendungen sind oft ein Einfallstor für Angreifer. Zero Trust Application stellt sicher, dass jede Anwendung kontinuierlich überwacht & überprüft wird.

Kernmaßnahmen:

✅Zugriffsbeschränkungen für Cloud- & SaaS-Anwendungen
✅Runtime Application Self-Protection (RASP) – Apps erkennen und blockieren Angriffe in Echtzeit
✅Sicherheitsprüfungen vor der App-Nutzung

Beispiel: Ein Cloud-Service erlaubt nur Zugriff, wenn der Nutzer mit einem firmeneigenen Gerät & VPN verbunden ist.

Zero Trust Workload

2

Fokus: Sicherer Datenaustausch zwischen IT-Workloads

- In Cloud-Umgebungen kommunizieren viele Workloads untereinander (z. B. Container, APIs, Microservices).
- Zero Trust Workload stellt sicher, dass nur genehmigte & gesicherte Workloads miteinander interagieren.

Kernmaßnahmen:

✅Container-Security (z. B. Schutz für Kubernetes-Workloads)
✅Sichere API-Gateways
✅Cloud-Sicherheitsrichtlinien für Workloads

Beispiel: Eine Zero-Trust-Architektur verhindert, dass ein kompromittierter Microservice Zugang zu anderen Cloud-Ressourcen erhält.

Zero Trust Network

Zero Trust Identity

Zero Trust Application

ZERO TRUST

SECURITY

Zero Trust Workload

Zero Trust Endpoint

Zero Trust Data