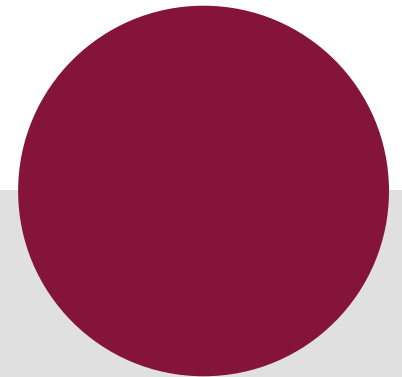




.consulting .solutions .partnership

Informationssicherheit für die Container-Orchestration mit Kubernetes und Docker

it-sa, Nürnberg, 08. Oktober 2019



Vorstellung



Jan Eltner

Business Consultant
IT-Sicherheit
Public Sector

0172 / 950 44 91

jan.eltner@msg.group



Was sind Container?



- Container kapseln Anwendungen und ihre Abhängigkeiten.
- Container entkoppeln die Anwendung von der Hardware.
- Container ermöglichen einen schnellen und einfachen Rollout von Anwendungen.
- Container vereinfacht das Einspielen von Updates und ermöglichen ein einfaches Rollback.
- Container wurden nicht primär als Sicherheitsfeature entwickelt!

Virtualisierung vs. Container

Virtualisierung	Container
mehr Overhead	Leichtgewichtig
eigener Betriebssystemkernel	geteilter Betriebssystemkernel
Änderungen sind persistent	Änderungen sind temporär

Warum Container-Orchestration?

Skalierung und Loadbalancing

- Automatische Anpassungen an den tatsächlichen Ressourcenbedarf.

Health Monitoring

- Erkennung und Neustart von „hängenden“ Containern.

Service Verwaltung

- Zugriff auf den Service statt auf eine IP-Adresse.

Sicherheitsanforderungen an Docker-Images

Images aus
vertrauenswürdiger
Quelle

Minimale Software-
Installation

Keine Secrets in
den Images

Anforderungen an Docker-Container

Ausführen mit
minimalen
Rechten

Persistent
Storage

Monitoring +
Protokollierung

Kein
SSH/Telnet

Anforderungen an das Host-System

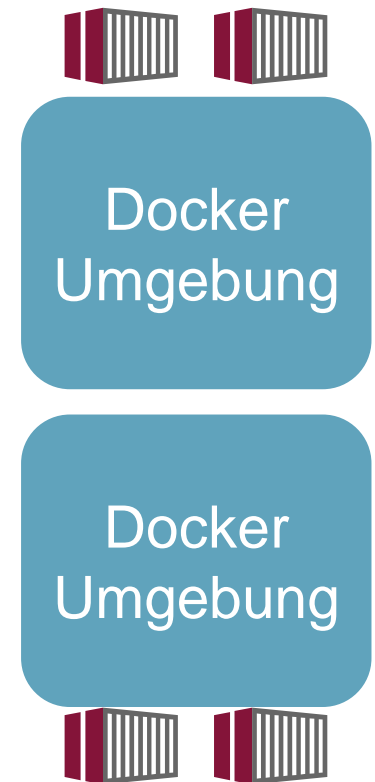
Gehärtetes Betriebssystem härten

Software minimal konfigurieren

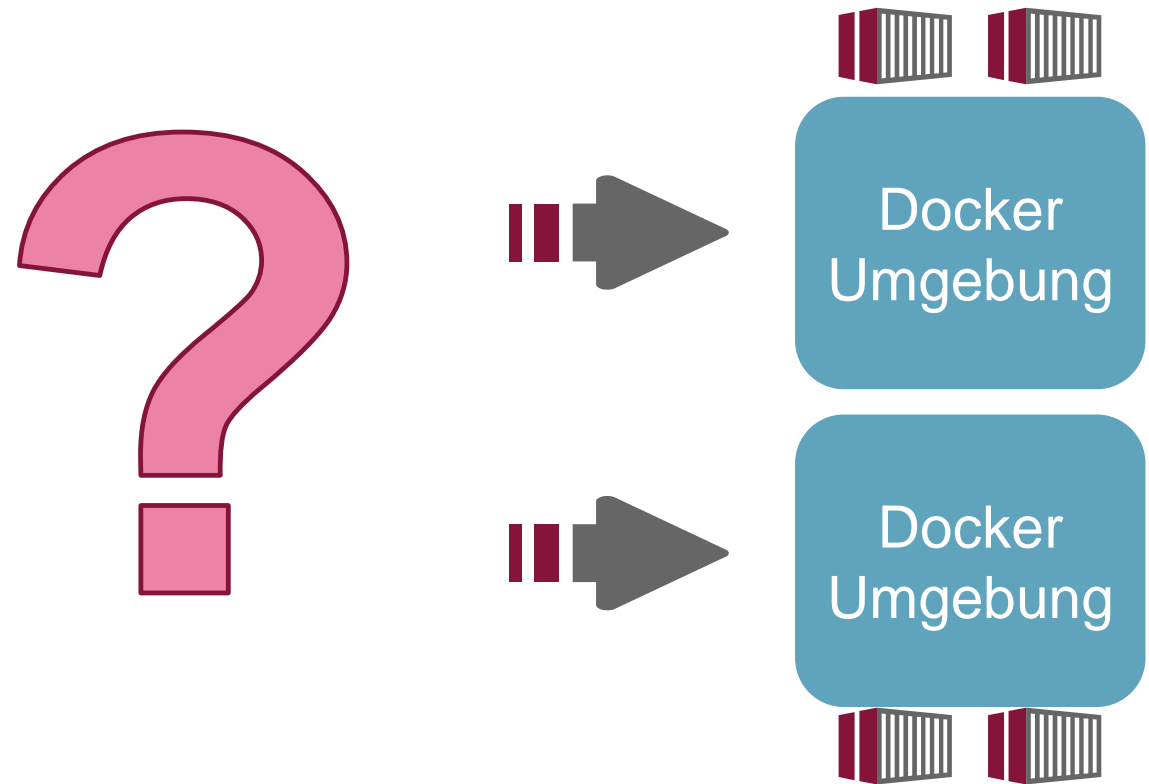
minimale Berechtigungen erteilen

Angepasst als Container-Host-System

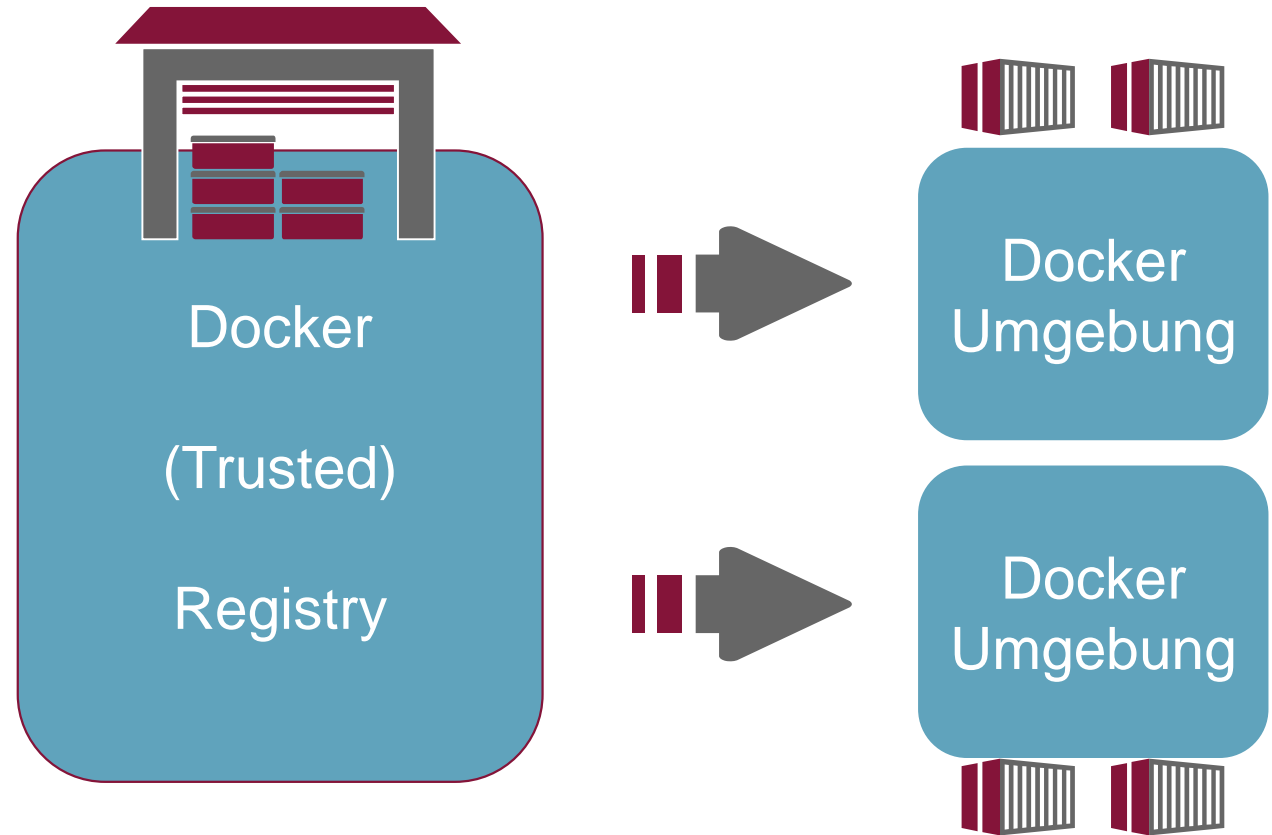
Docker (Trusted) Registry



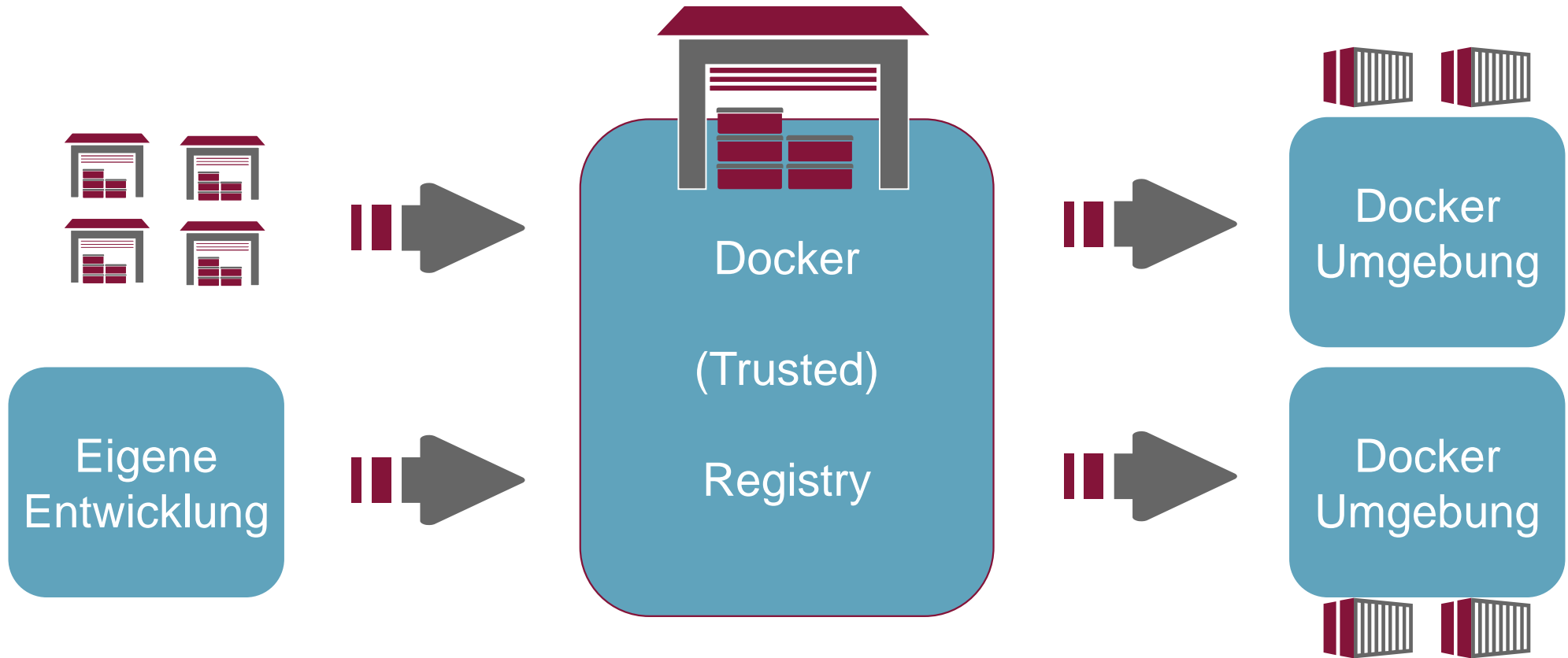
Docker (Trusted) Registry



Docker (Trusted) Registry



Docker (Trusted) Registry



Docker Trusted Registry



Anforderungen an Orchestrator

Netz
segmentieren

Netz
verschlüsseln

ausreichend
Ressourcen
bereitstellen

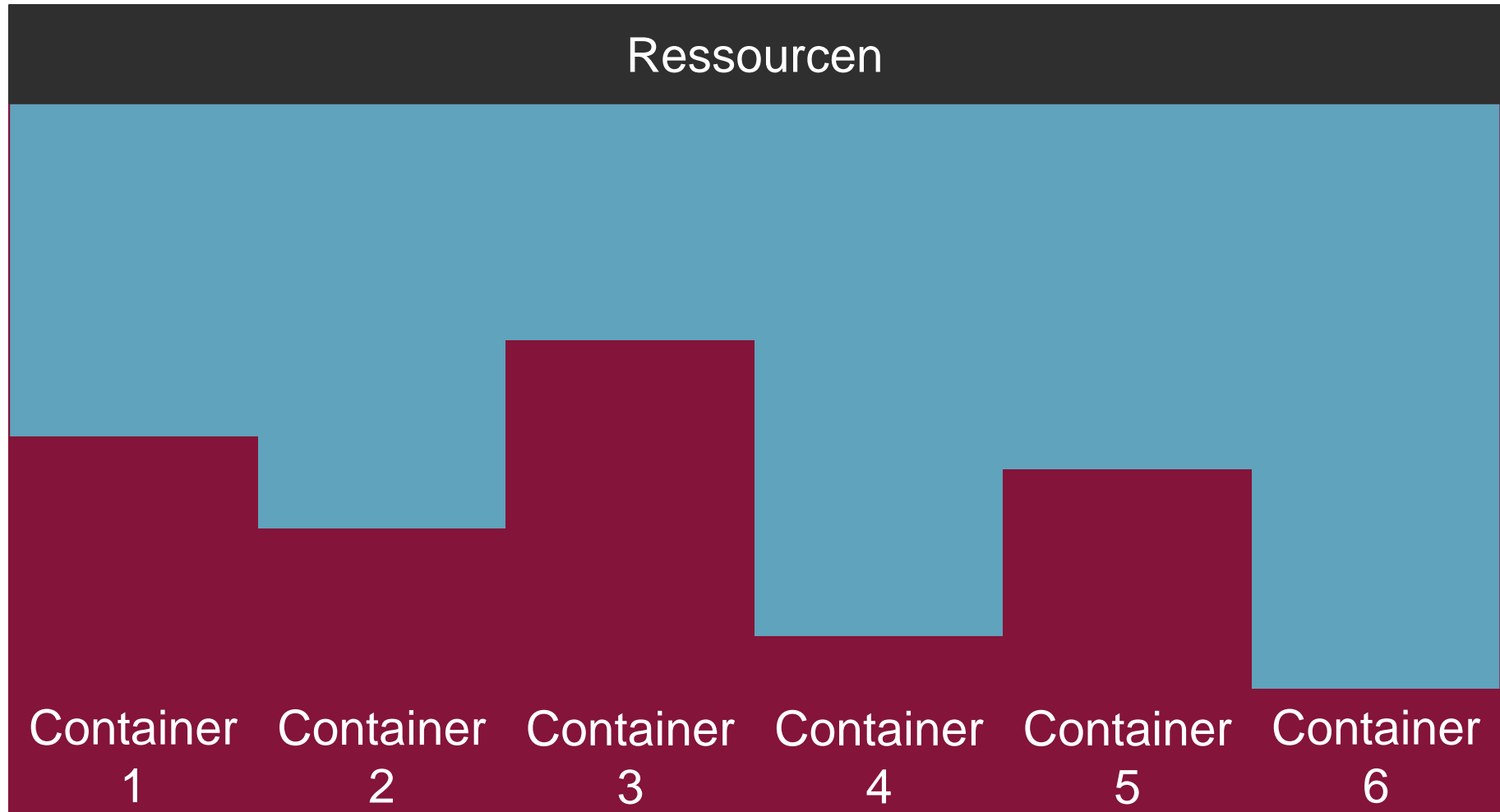
Konfiguration
von Minimal-
sowie
Maximal-
Ressourcen

Minimal- und Maximalressourcen

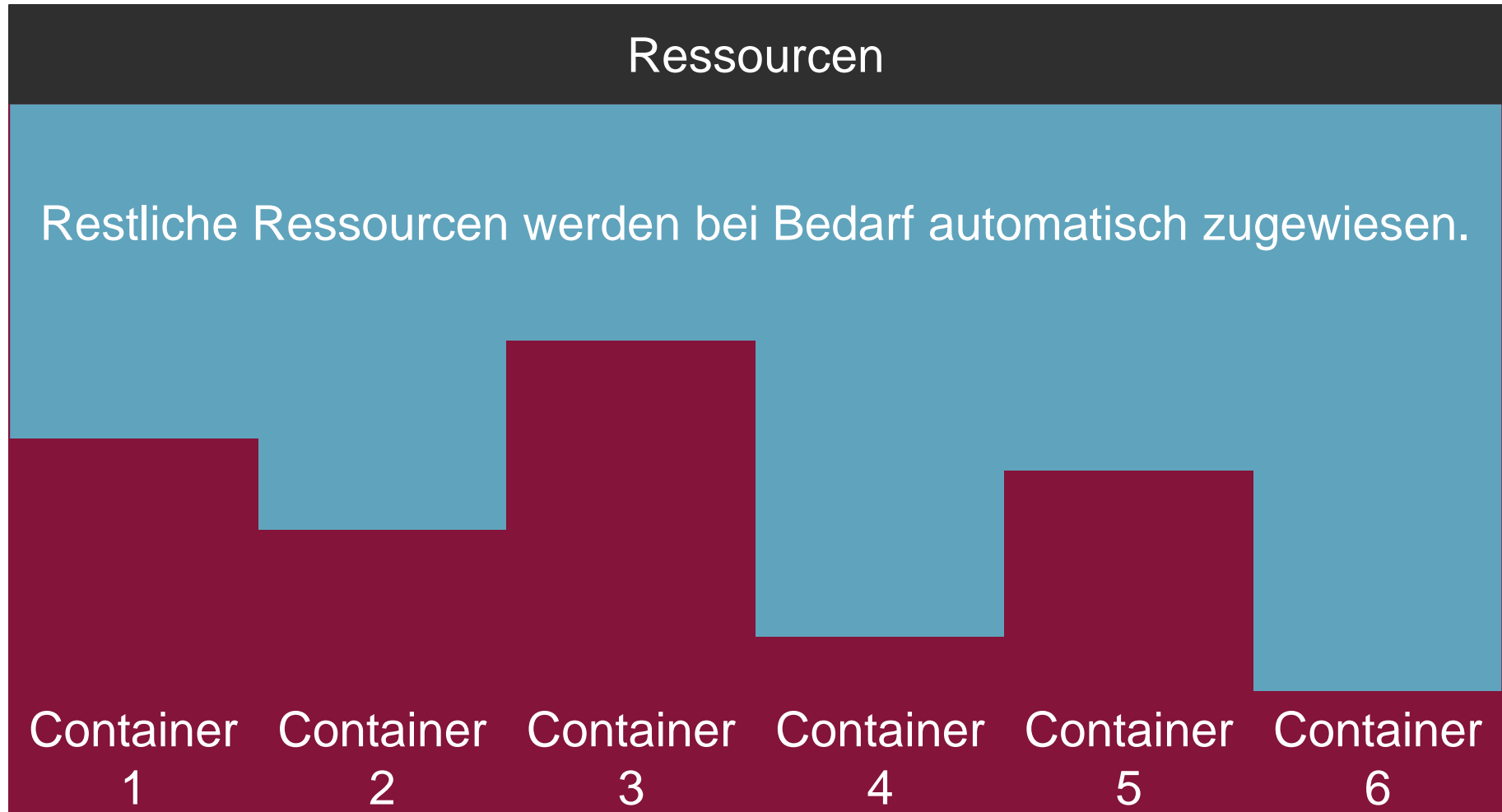
Ressourcen



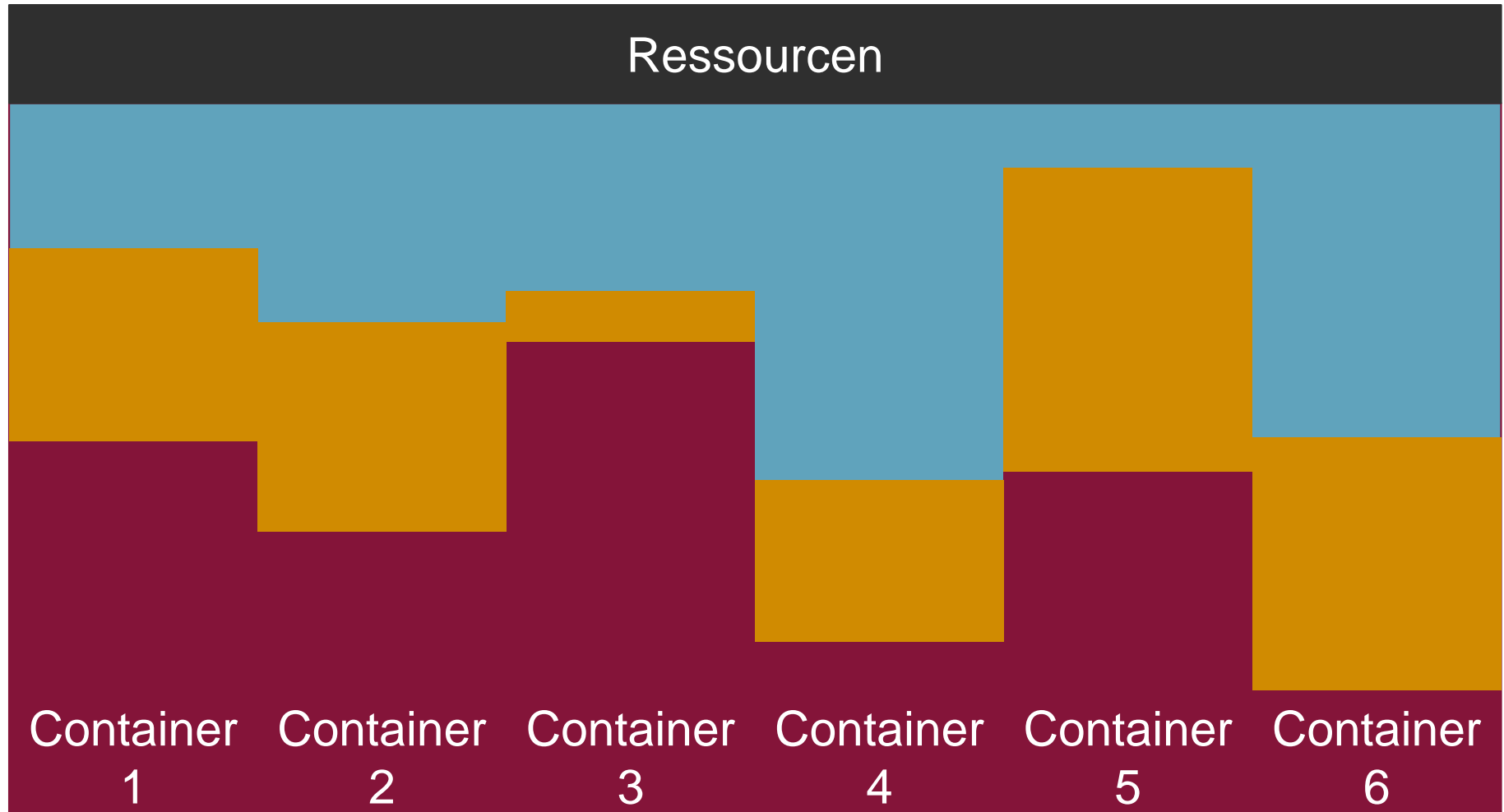
Minimal- und Maximalressourcen



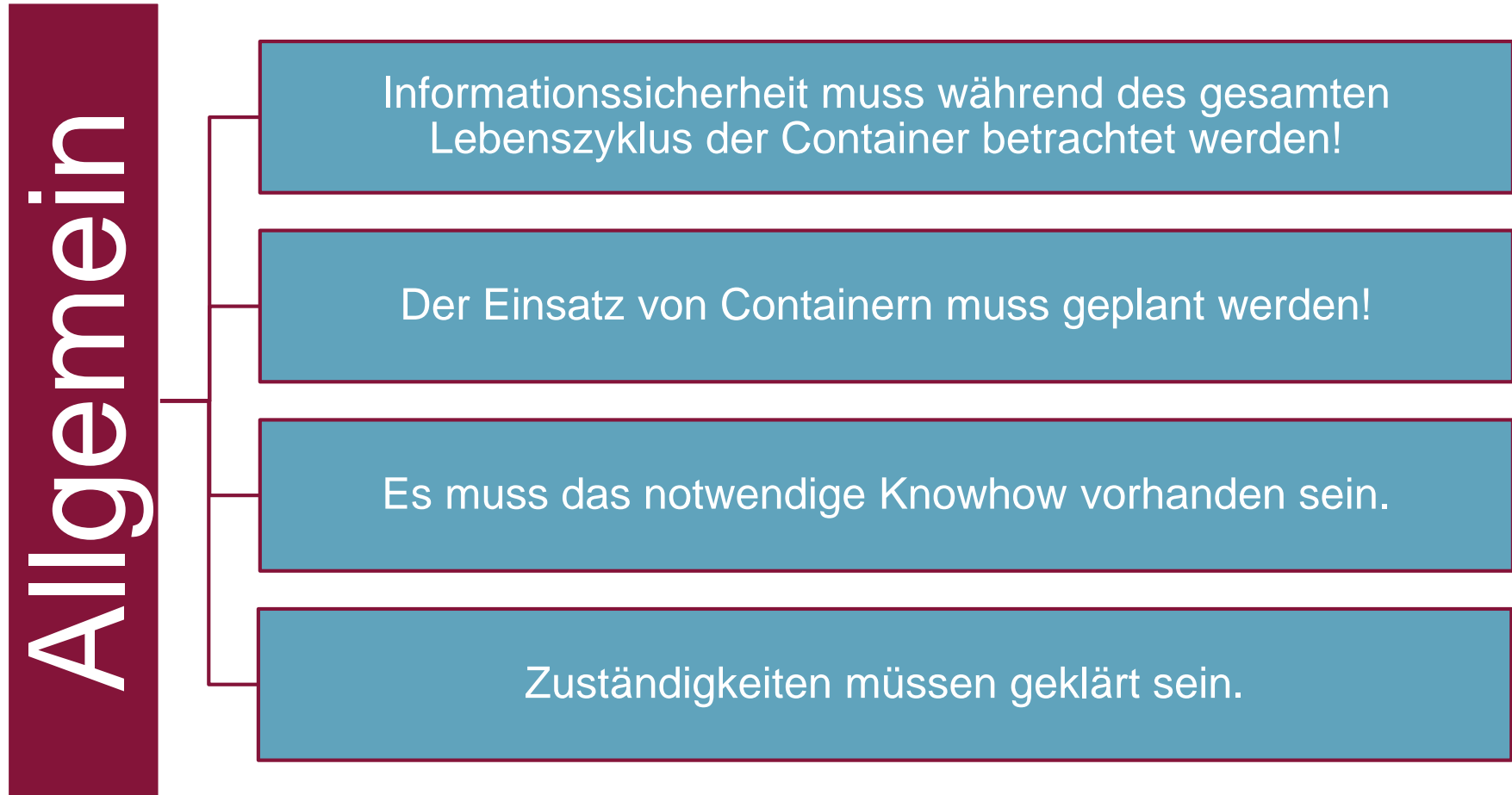
Minimal- und Maximalressourcen



Minimal- und Maximalressourcen



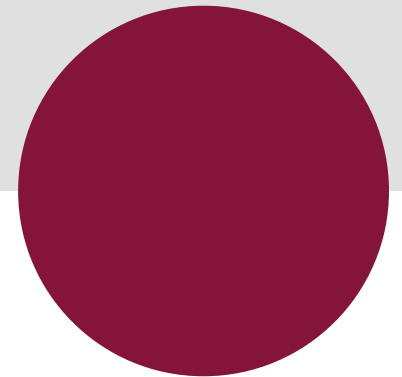
Grundsätzliches





Jan Eltner
Business Consultant Public Sector

0172 / 950 44 91
jan.eltner@msg.group



Besuchen Sie uns auf Stand 10.0-202

msg .consulting .solutions .partnership