Segmentierung ist einfach?

Stephan Verbücheln
Zürich, 9. September 2020

cnlab

Agenda

- Einführung Container
- Netzwerk mit Containern
- Segmentierung mit Containern
- Policy Enforcement Point als Container betreiben

Was ist Docker?

- Anwendungen in **Images** paketieren
- Images als **Container** ausführen
- Container sind voneinander isolierte Prozesse
- Jeder Container sieht eigene Linux-Umgebung (Filesystem, System Calls)
- Basiert auf elementaren Funktionen des Linux-Kernels

Image für Anwendungen erzeugen

1. Basis-Image auswählen, z.B. Ubuntu
2. Dockerfile definieren
3. Image generieren

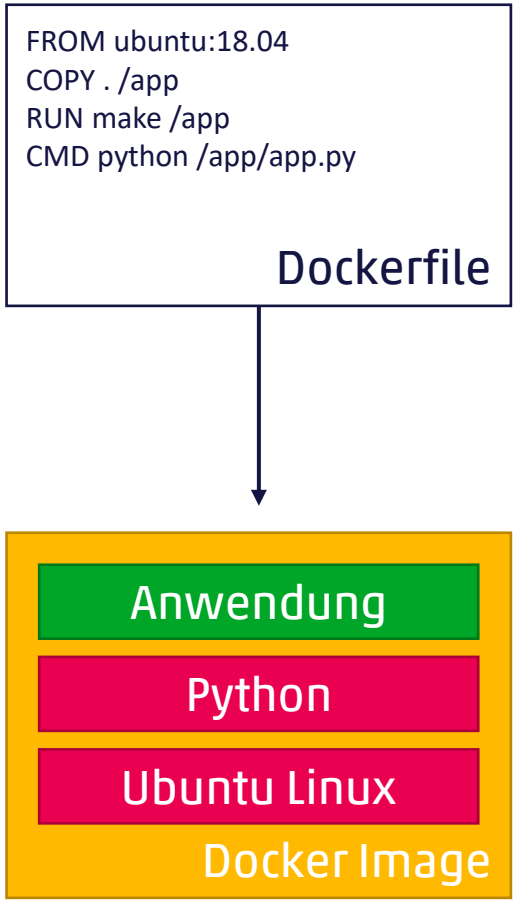
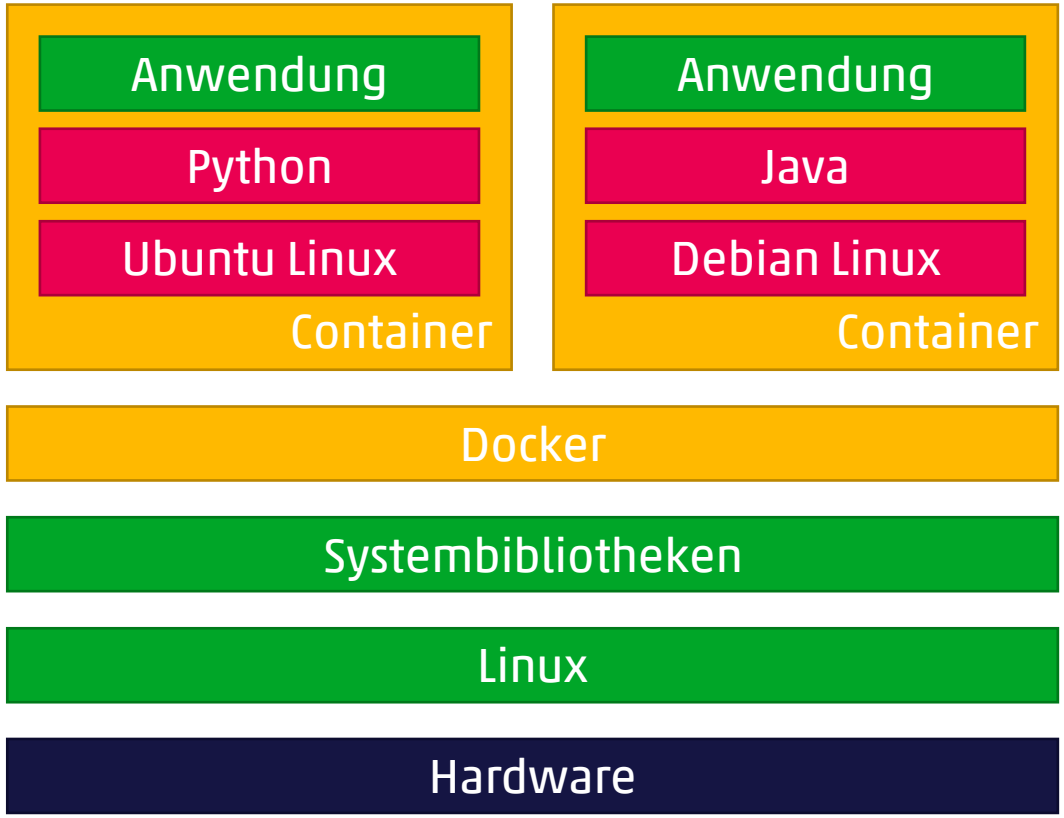


Image als Container ausführen

Parameter übergeben

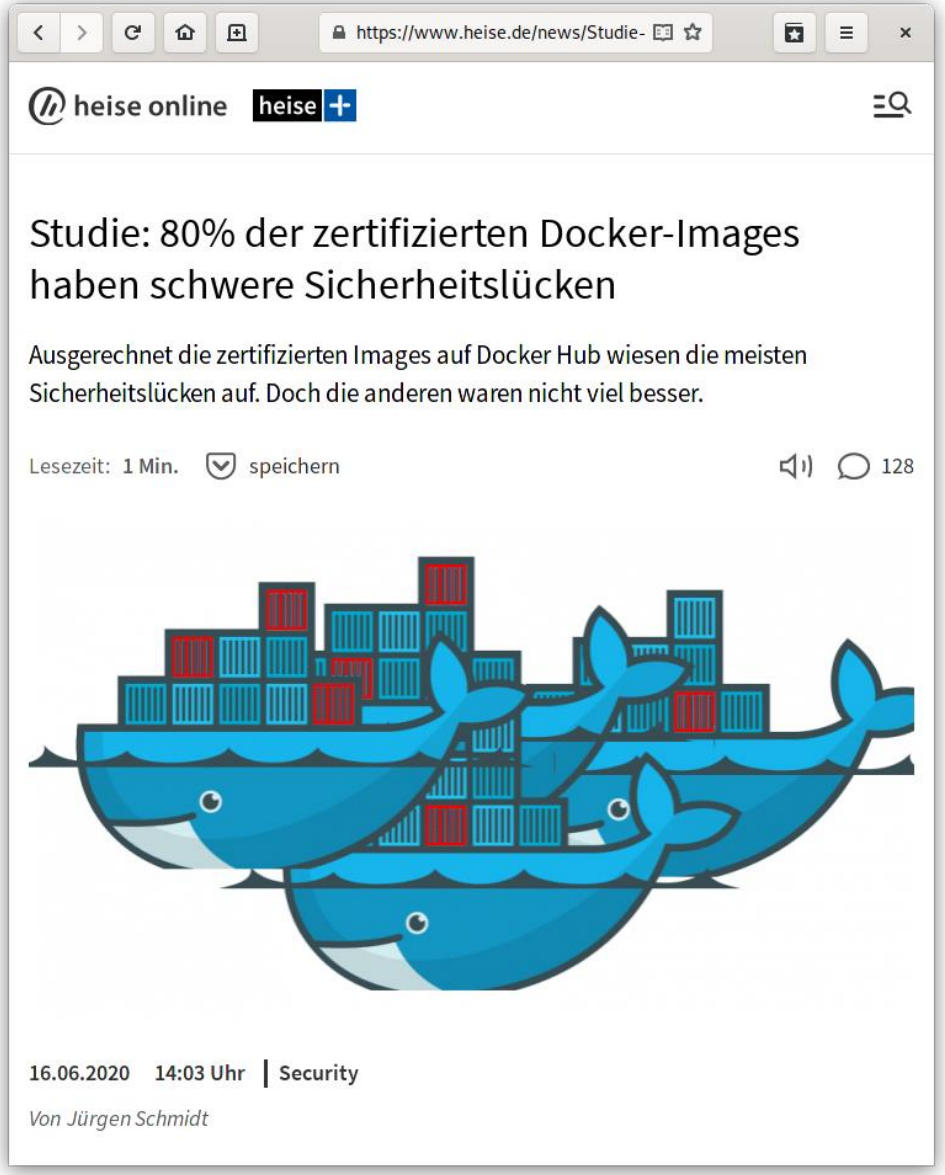
- Konfiguration
- Passwörter und Schlüssel
- Mounts



Sicherheit von Containern

Fettnäpfchen

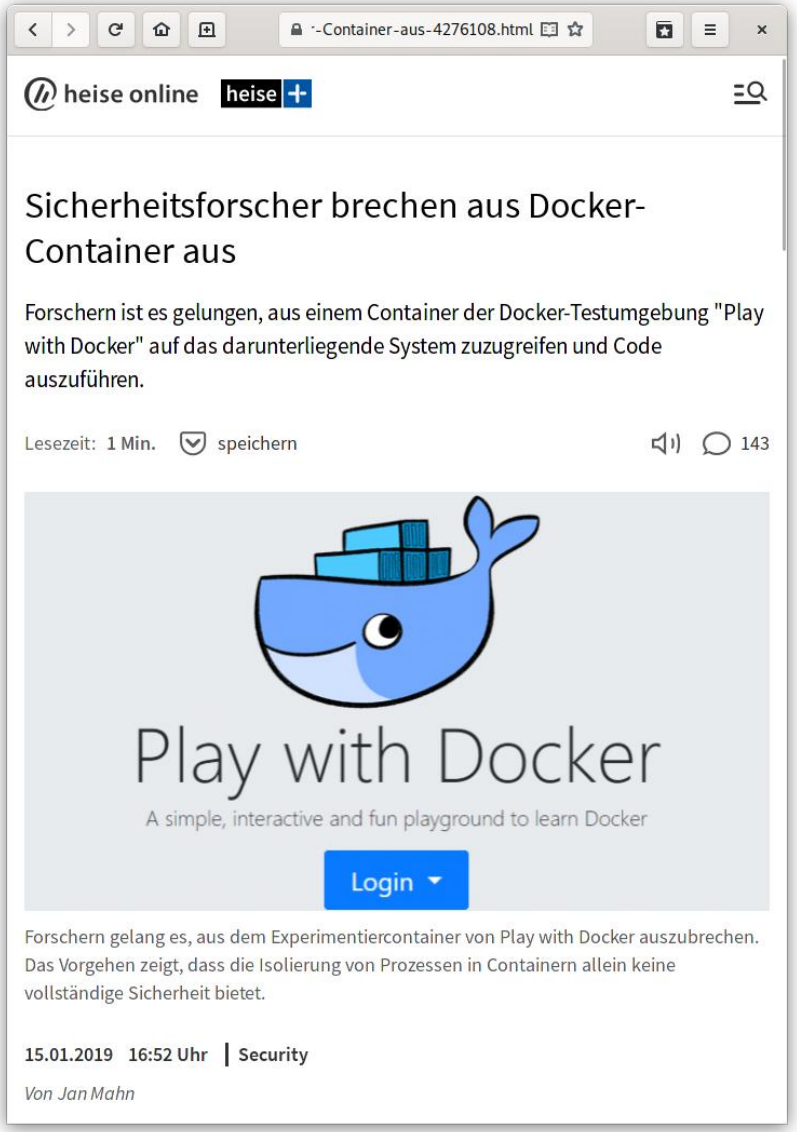
- veraltete Libraries mit bekannten Lücken
- Passwörter und Schlüssel im Image
- Berechtigungen auf Host-Dateisystem



Ausbruch aus Containern

Sandbox ist nicht perfekt

- kompetente Angreifer können ausbrechen
  - Sicherheitslücken
  - Fehlkonfiguration
- kritische Anwendungen sollten separat betrieben werden



Was sind Kubernetes und OpenShift?

Tools zum Verwalten von Containern

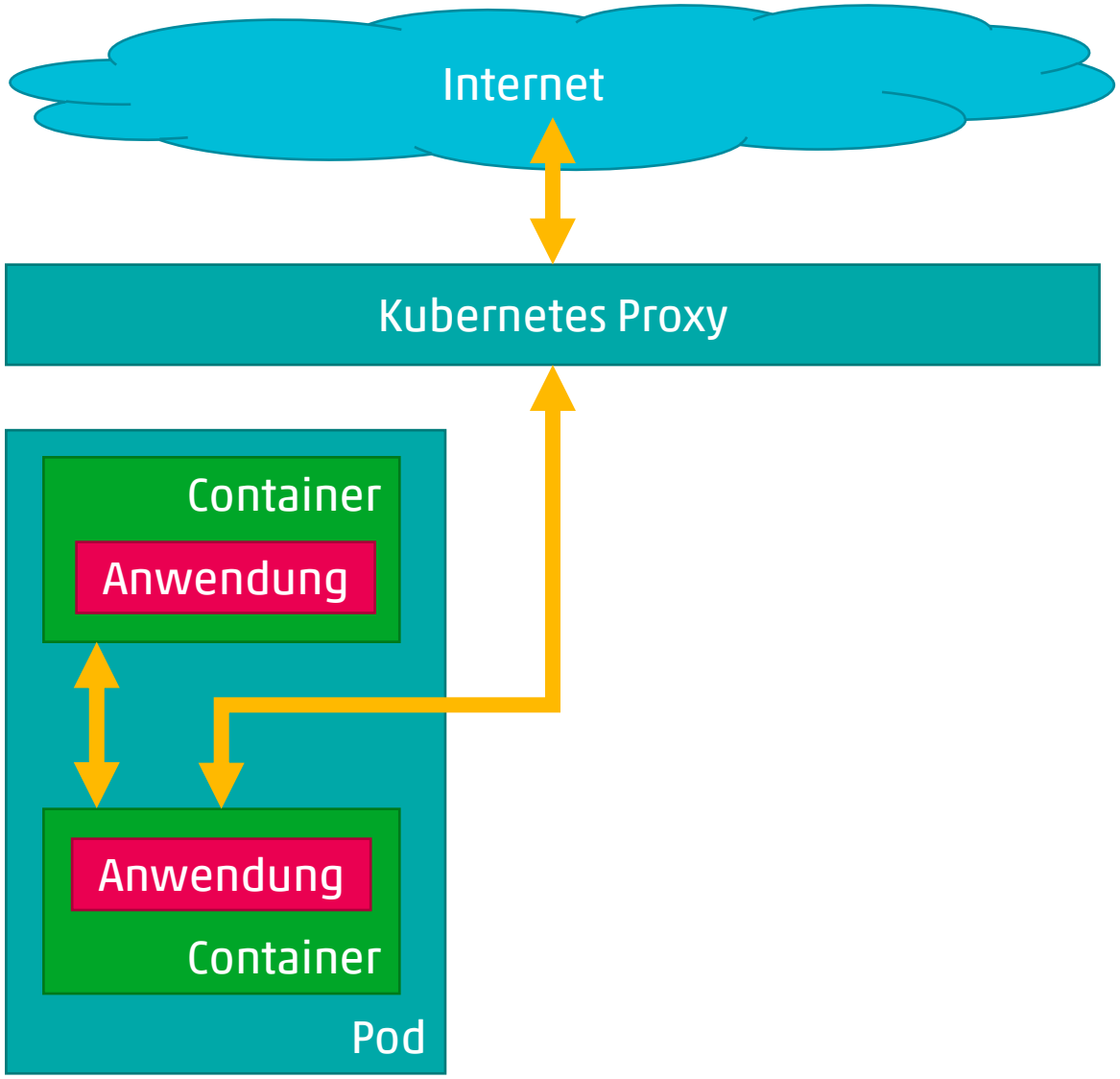
- Gruppierung (Pods, Namespaces)
- Konfiguration
- Verwaltung von Credentials
- Automatisierung
- Orchestration
- Redundanz
- Verteilung auf verschiedene Cluster

Red Hat

OPENSHIFT

Netzwerk mit Containern

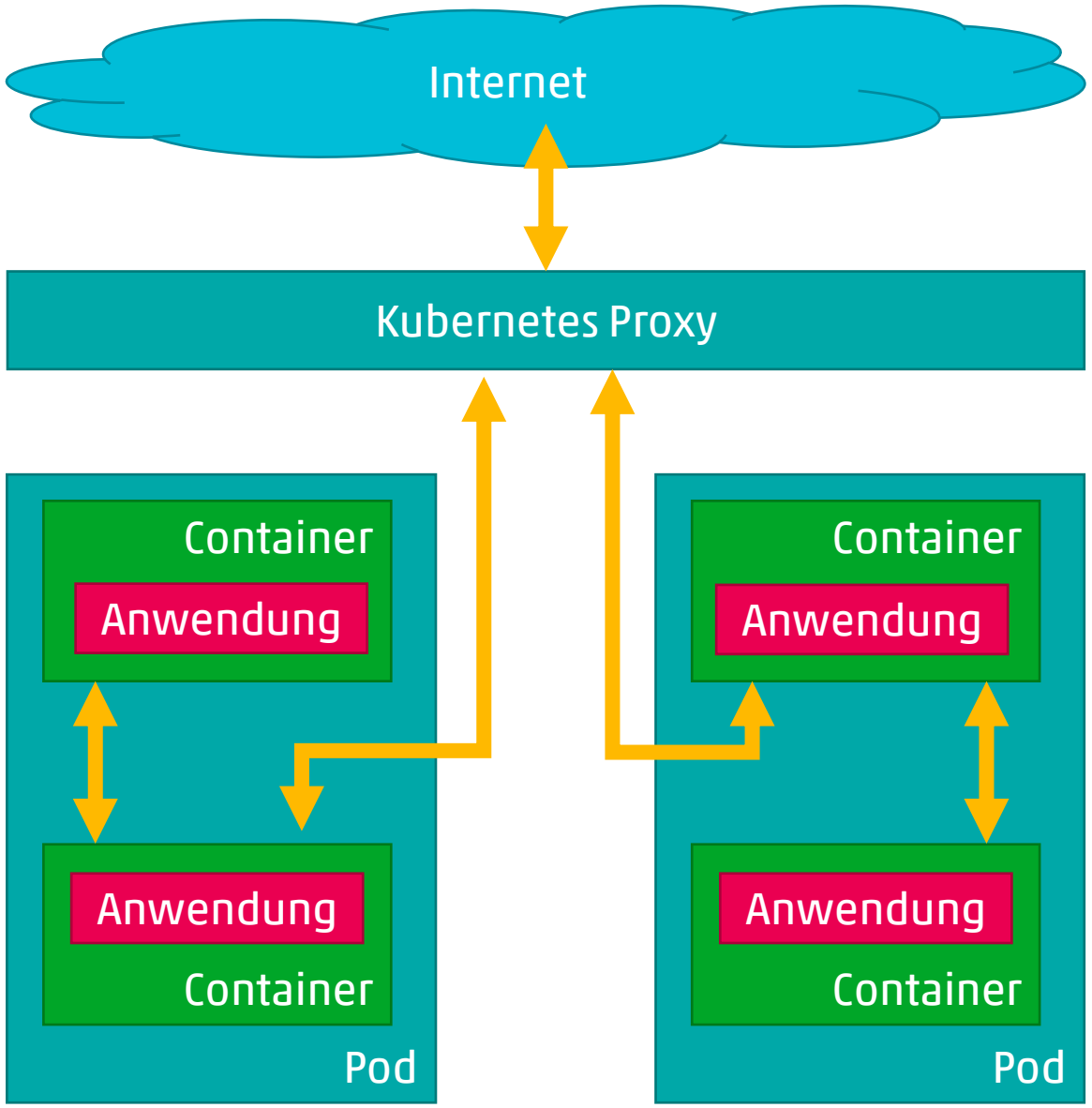
- Jeder Container sieht eine virtuelle Netzwerkkarte
- Pods sind Gruppen von Containern
- Pods haben eine IP-Adresse
- Container in einem Pod können über Localhost kommunizieren



Segmentierung mit Containern

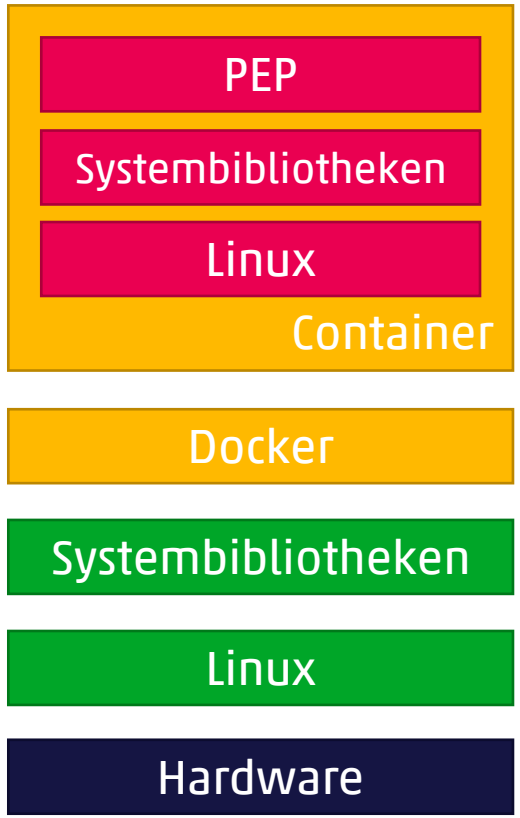
Kubernetes-Proxy

- verwaltet Kommunikation zwischen Pods
- verwaltet Kommunikation über externe Netzwerke
- verwaltet Kommunikation über Internet

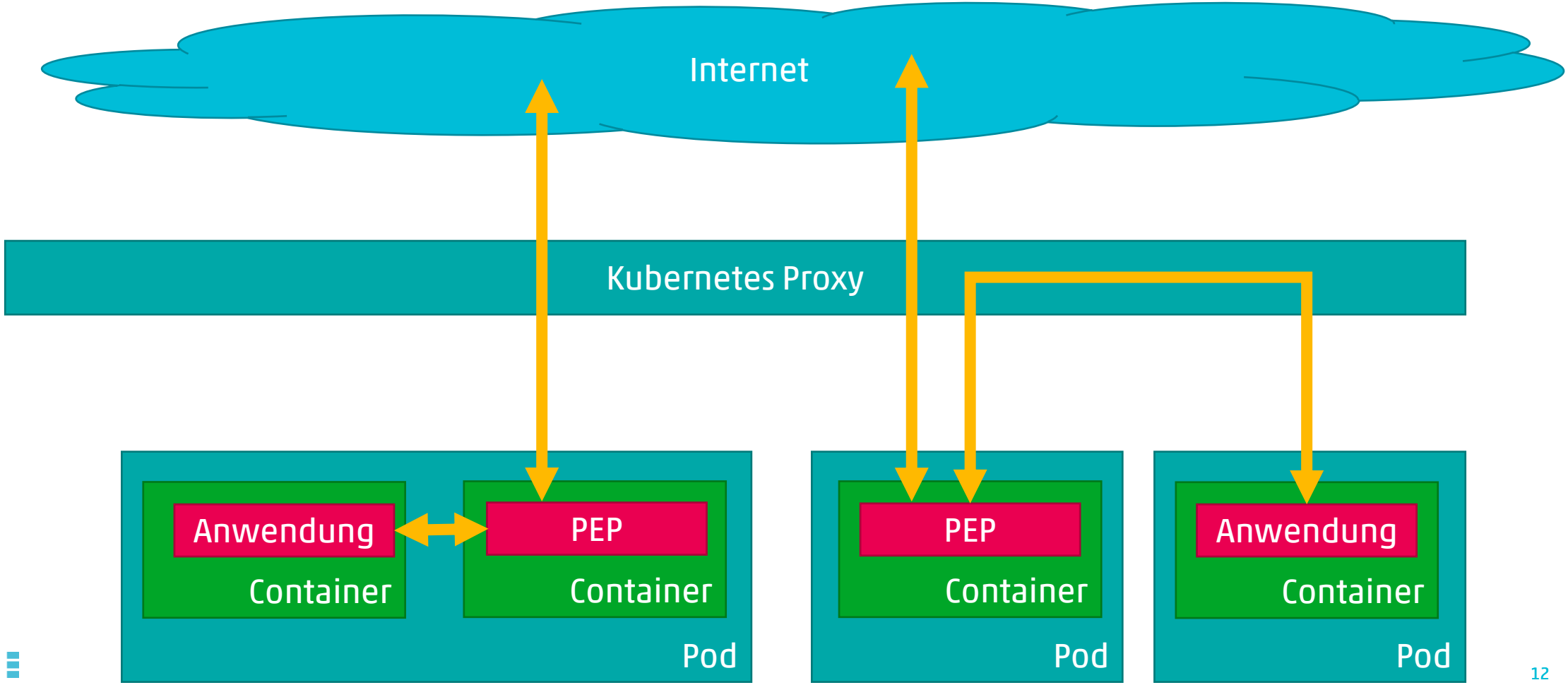


Policy Enforcement Point (PEP) als Container

- Einfach aufzusetzen
- Wiederverwendbares Image kann mit angepasster Konfiguration gestartet werden
- Isolation von der eigentlichen Anwendung
- Kann im selben Pod betrieben werden
  - Enforcement sehr nah an Anwendung



Gesamtansicht: Zero Trust mit Containern



Fazit

- Container erleichtern das Deployment.
- Nicht automatisch sicher, Fettnäpfchen beachten.
- Konfigurationsmöglichkeiten sind nützlich für Segmentierung.

Vielen Dank für Ihre Aufmerksamkeit_

info@cnlab-security.ch
+41 55 214 33 33

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab