

15:55 – 16:15 Uhr

**KubeOps Compliance:  
Souveräne Kubernetes-Lösungen  
für kritische Infrastrukturen**

**Marius Biedermann**

# Agenda

1. **Vorstellung**
2. **Was bedeutet IT-Souveränität?**
3. **Success Stories**
4. **KubeOps**
5. **Fazit**



Vorstellung

 bechtle

# Marius Biedermann

**Key Account Manager BMDS und ITZBund @KubeOps  
GmbH**

- Vormals Gesamtprojektleiter BundID, ZBP, MJP
- Schwerpunkte:
  - Projekte in der Onlinezugangsgesetz- Umsetzung
  - Digitale Souveränität
- [Marius.biedermann@arwinet.com](mailto:Marius.biedermann@arwinet.com)

# KubeOps GmbH

## Key Facts



9,5 Millionen EUR  
Umsatz (2024)



~95 Mitarbeiter



Team von ~70  
Kubernetes  
Experten  
In Projekten seit 2015



Höchste  
IT Security  
Standards

## Highlights

- ✓ Langjährige Erfahrung im öffentlichen Sektor mit restriktiven IT-Umgebungen (hohe Sicherheit, Compliance, Datenschutz, kritische Infrastrukturen)
- ✓ Betrieb von Kubernetes-Clustern und containerisierten Anwendungen
- ✓ On-Premise, Cloud, Multi-Cloud – jeweils souverän
- ✓ Kubernetes-Betriebsplattform basierend auf Open-Source-Komponenten ohne Vendor-Lock-in
- ✓ Zertifizierter Trainingspartner mit eigener Akademie
- ✓ Seit 2024 Teil der Bechtle



# Strategische Perspektive

IT-Souveränität =  
mehr als technische  
Selbstbestimmung

Kontrolle über IT-  
Systeme & Daten

Geopolitische  
Relevanz

Vorteile für  
Organisationen

Sicherheits- und  
Datenschutzaspekte

# Technische Perspektive

Security by  
Design

Offene  
Standards

Open Source

Multi-Cloud

air-gapped  
Betrieb

Automatisierung

Stabilität

# Projektanforderungen KRITIS & sensible Umgebungen

Sicherheits- & Compliance-Vorgaben

Einhaltung gesetzlicher Leitlinien: **BSI, BACS, NIS2, ISO 27001**

**Resilienz:** Störungen erkennen und sich schnell erholen

**Ausfallsicherheit:** kontinuierlicher Betrieb auch bei Teilfehlern

keine Abhängigkeit von einzelnen Anbietern oder geopolitischen Einflüssen

Vermeidung proprietärer Lizenzmodelle und politischer Risiken

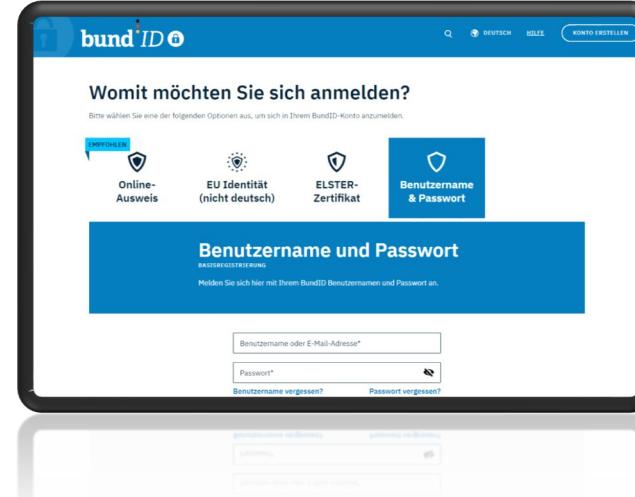
sichere Einbindung von **Legacy-Systemen** in moderne Plattformen

Unterstützung von **Multi-Cloud-** und **air-gapped-Umgebungen**

Installationen und Updates müssen **reproduzierbar, stabil und revisionssicher** sein

Compliance muss jederzeit **nachweisbar** bleiben

# Betrieb BundID



## Betrieb der BundID

- zentrales Projekt im Rahmen des **Onlinezugangsgesetzes (OZG)**
- Ziel: **digitale Verfügbarkeit aller Verwaltungsleistungen** für Bürgerinnen und Bürger

## Funktion der BundID

- zentrale Plattform zur **Authentifizierung** im digitalen Verwaltungsverfahren
- ermöglicht sichere Anmeldung über **eID, eIDAS, ELSTER** oder **Benutzername/Passwort**
- **BundID-Postkorb**: direkte Zustellung von Bescheiden an Bürgerinnen und Bürger

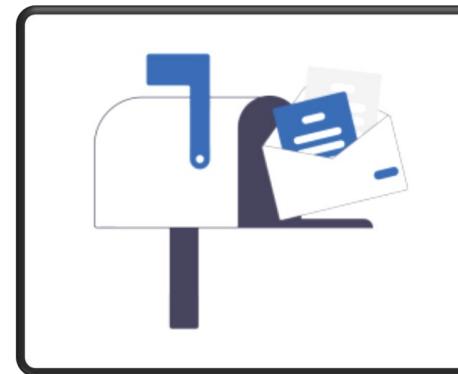
## Entwicklung & Zweck

- gezielt für die **Digitalisierung der Verwaltung** entwickelt
- dient als **zentrale Identitäts- und Kommunikationsschnittstelle** zwischen Bürgern und Behörden

## Unser Beitrag & Verantwortung

- **Betrieb der Anwendung und Plattform seit 2019**
- Umsetzung **gemäss den Anforderungen des BSI**
- **Leistungsumfang**:
  - Projekt- und ITIL-Management
  - Applikations- und Plattformbetrieb
  - über **14.000 Personentage Erfahrung**

# Betrieb ZBP



## Betrieb des Zentralen Bürgerpostfachs (ZBP)

- mehrjähriges Projekt für eine zentrale Kommunikationsplattform
- bündelt die Kommunikation zwischen Bürgerinnen und Bürgern, Bundesländern, Kommunen und Fachverfahren an einem Ort

## Entstehung & Zielsetzung

- entstand durch die Migration der bestehenden Postfächer aus der BundID
- ersetzt das dort zuvor integrierte Postfach
- bietet einen sicheren, zentralen Ort für den Empfang amtlicher Bescheide

## Technischer Betrieb & Umsetzung

- Betrieb der Anwendung und Kubernetes-Infrastruktur seit 2022
- Zusammenarbeit mit einem Partnerunternehmen
- Umsetzung gemäss den BSI-Vorgaben

## Ausblick & Weiterentwicklung

- künftig bidirektionale Kommunikation möglich
- Bürgerinnen und Bürger können direkt mit Behörden in Kontakt treten

# Betrieb MJP

## Praxisbeispiel 3: „Mein Justizpostfach“ (MJP)

- digitale Plattform für **verschlüsselte Kommunikation** zwischen
  - Bürgerinnen und Bürgern
  - Organisationen
  - der **Justiz** (Gerichte, Anwälte, Notare)

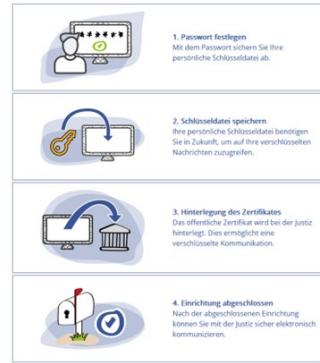
### Funktion & Nutzen

- ermöglicht sicheren Austausch sensibler Informationen
- stärkt **Vertraulichkeit und Integrität** in der digitalen Justizkommunikation



### Integration mit BundID

- Zugang über das **BundID-Konto**
- sorgt für einen **nahtlosen Übergang** zwischen BundID und MJP



### Betrieb & Verantwortung

- Betrieb und Plattformmanagement seit dem **Rollout 2023**
- Umsetzung **gemäss BSI-Vorgaben**
- Fokus auf **Sicherheit, Stabilität und Souveränität**

# Gemeinsame Erfolgsfaktoren der Projekte

## Praxis zeigt: souveräne, sichere und skalierbare Plattformen funktionieren

- nicht nur theoretisch, sondern **bewährt in realen Projekten**
- alle Systeme laufen auf **Kubernetes, BSI-konform** und **hochverfügbar**
- mehrere Jahre **zuverlässiger Betrieb**

## Grundlage für Stabilität & Sicherheit

- sorgfältiges Zusammenspiel von **Technologie, Compliance und operativer Erfahrung**

## Übertragung auf KubeOps Compliance

- praxisnahe Erfahrungen aus BundID, ZBP und MJP **direkt integriert**
- alle Anforderungen, Prüfverfahren und Sicherheitsmassnahmen in **wiederverwendbare Plattform** überführt

## Ergebnis der Plattform

- **vollständig auditierte, souveräne und cloud-agnostische Lösung**
- entspricht höchsten **Sicherheits- und Compliance-Standards**

## Nutzen für Organisationen

- Erfahrungen aus erfolgreichen KRITIS-Projekten **direkt auf neue Anwendungen und Infrastrukturen übertragen**
- ermöglicht **verlässlichen, sicheren und unabhängigen Betrieb**

# Wie können Sicherheits- und Compliance-Anforderungen in souveränen IT-Infrastrukturen erfüllt werden?

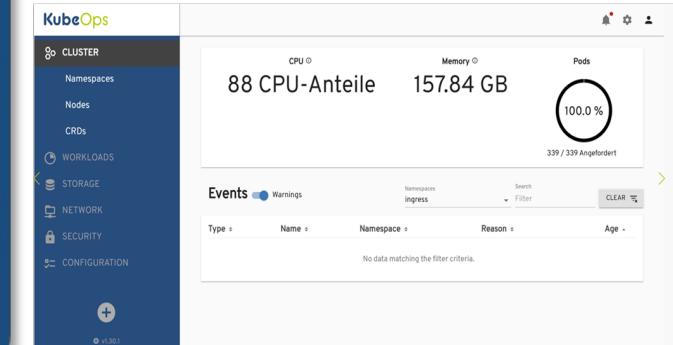
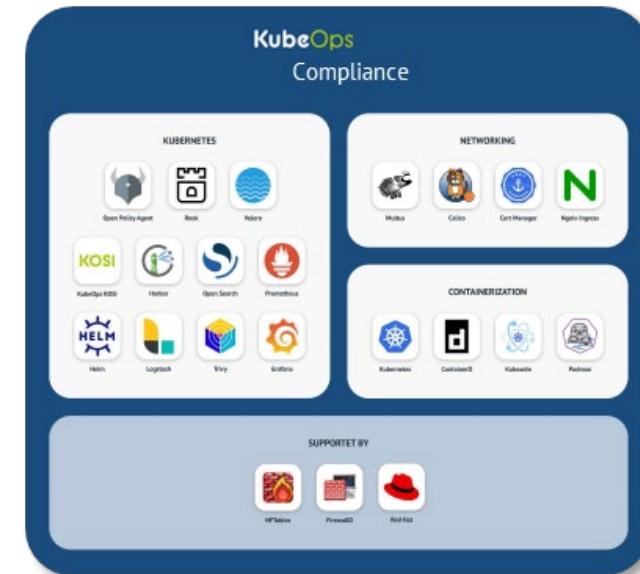
Security-by-Design:  
gehärtete Images  
& überprüfbare  
Herkunft

Durchgängiges  
Policy Enforcement  
für Compliance

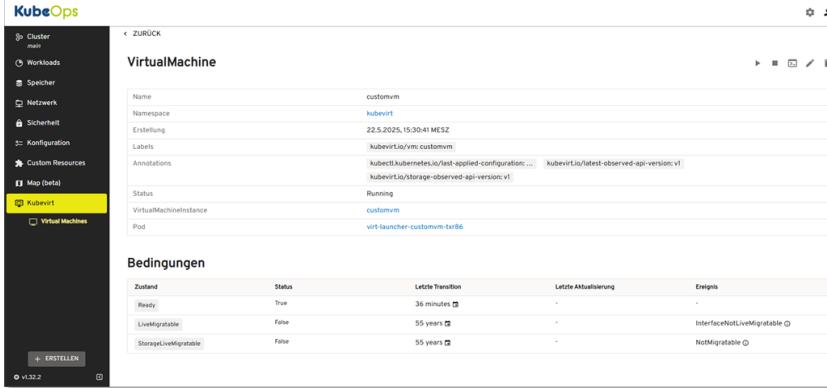
Multi-Cloud- und  
On-Premises-  
Unterstützung

Offene Architektur,  
kein Vendor  
Lock-in

Aufbau vollständig  
souveräner IT-  
Umgebungen  
möglich



# Wie können virtuelle Maschinen souverän in einer Kubernetes-Umgebung betrieben werden?



VM-Orchestrierung innerhalb derselben Kubernetes-Umgebung wie Container

Migration bisheriger Anwendungen von VMware & anderen Virtualisierungslösungen

Automatisierte Verwaltung von Infrastruktur & Anwendungen via GitOps

Kombination aus souveränem Ansatz & Zukunftsfähigkeit

# Wie kann in restriktiven IT-Umgebungen die Integrität und Nachvollziehbarkeit von Softwareinstallationen sichergestellt werden?

KOSI bündelt alle Installationsartefakte (Helm-Charts, RPMs, software-spezifische Dateien) in einem Paket

Unterstützt air-gapped bzw. abgeschottete Umgebungen

Unveränderlichkeit & Wiederholbarkeit gewährleisten Sicherheit und Stabilität

Integrierte Batch-Engine ermöglicht vollständige Automatisierung

Sichert stabile Update-Prozesse für alle KubeOps-Produkte

Ermöglicht souveräne, wartbare und zukunftssichere IT-Systeme



# Fazit

## IT-Souveränität ist gelebte Realität

- nicht nur theoretisches Konzept, sondern **bewährt in Praxisprojekten**

## Praxisbeispiele bestätigen die Umsetzbarkeit

- **BundID, ZBP, MJP** zeigen souveräne, sichere und skalierbare Infrastrukturen

## KubeOps-Produkte basieren auf diesen Erfahrungen

- **KubeOps Compliance**: BSI-konforme, auditierte Kubernetes-Plattform
- **KubeOps VM**: Verwaltung von **VMs und Containern Side-by-Side**
- **KOSI**: hocheffiziente, sichere Softwareinstallation, auch in restriktiven Umgebungen

## Gesamtbild

- alle Lösungen zusammen bilden eine **offene, sichere und zukunftsfähige digitale Infrastruktur**

# KubeOps Compliance: Souveräne Kubernetes-Lösungen für kritische Infrastrukturen

## Ihr Feedback zählt

*Jetzt in der App*

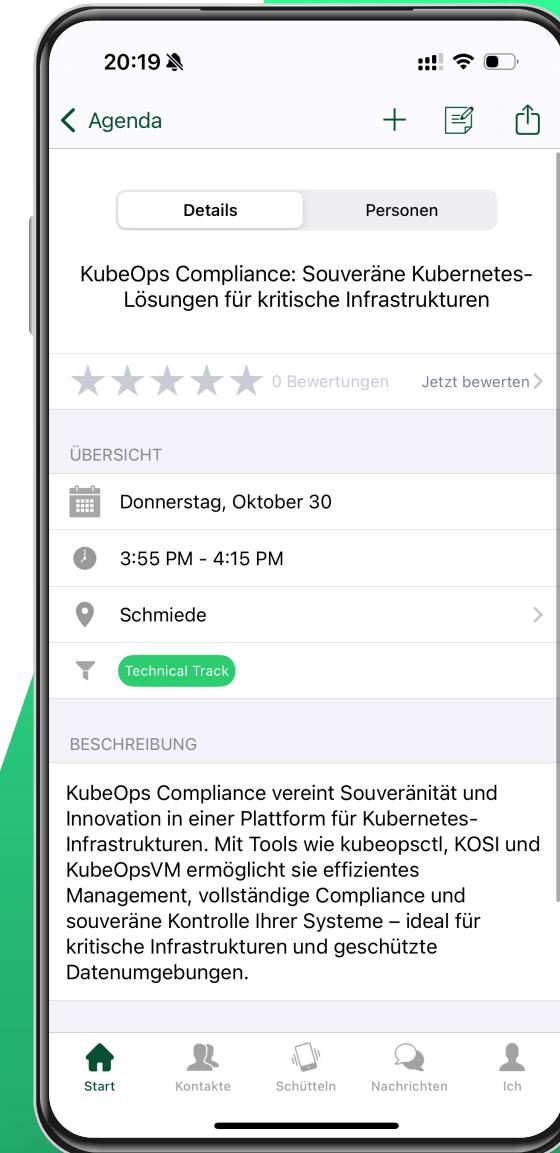
*bewerten.*



App Store



Play Store



16:20 bis 16:50 Uhr

Kaffeepause

# 16:50 - 17:10 Uhr

## SCHMIEDE



### Kundenreferenz Coop Pronto Shop

*Andreas Weidner (Bechtle  
Schweiz)*

*Hasan Akzorba (Coop Pronto)  
Beat Sommerhalder (HPE  
Aruba)*

## OFENHALLE

### Cyberattacke: Was passiert, wenn der Ernstfall eintritt

*Chris Bregenzer (Hawa Sliding  
Solutions AG)*

## STUBE

### Quantencomputer und die Auswirkungen auf die digitale Sicherheit

*Filip Vukadin (IBM Schweiz AG)*

## EVENTLOUNGE

### Modern Meeting Demo- Center

*Die neusten Lösungen,  
Trends & Technologien*

