

Red Hat Portfolio im Kontext der Datenschutzgrundverordnung

Dipl.-Ing. Dr. techn. Markus Löschnigg, MBA
Geschäftsführer

Ansatz und Idee



- **~~Geheimhaltungspflicht~~**
personenbezogener Daten Datenverarbeitung ist nur ausnahmsweise erlaubt
- **~~Rechtfertigungspflicht~~**
Datenverarbeitung darf nur aufgrund rechtlich sanktionierter Interessen erfolgen
- **~~Zweckbindung~~**
Die Zwecke müssen von den Rechtsgrundlagen getragen sein und im Vorhinein feststehen
- **Datensparsamkeit**
- **Transparenz**
Die Personen deren Daten verarbeitet werden sind zu informieren.
- **Datensicherheit**
Das Sicherheitsniveau muss zur jeweiligen Datenverarbeitung angemessen sein.
- **Privacy by design & Privacy by default**
Technische und organisatorische Maßnahmen zur Umsetzung der Prinzipien sind vorzusehen. Die genauen technischen Leitlinien wurden bis dato noch nicht beschlossen.

- ~~Informationsrecht~~
- **Auskunftsrecht**
- ~~Kontrollrecht~~
- ~~Widerspruchsrecht gegen Datenverarbeitungen~~
- **Recht auf Vergessen**
- **Recht auf Datenübertragbarkeit**

SIND MEINE SYSTEME INTEGER?

Einfache Schritte zuerst – Hostintegrität

RED HAT ENTERPRISE LINUX

Installieren

```
yum install aide
```

Initialisieren

```
aide --init
```

Zyklisches Prüfen

```
aide --check
```

Updates

```
aide --update
```

Archivieren

Nach Ihren Unternehmensvorgaben



MOBILE GERÄTE

Daten auf Devices verschlüsseln

RED HAT ENTERPRISE LINUX

dm-crypt & Linux Unified Key Setup

Verschlüsseln von

- gesamten Festplatten
- Wechselmedien
- Partitionen
- Software RAIDs
- Logical Volumes
- Dateien

1. Block Device erstellen
2. Device mit Zufallsdaten beschreiben
3. Device als dm-crypt/LUKS formatieren
4. Device-Mapper Mapping erstellen
5. Dateisystem am Device erstellen
6. Eintrag in /etc/crypttab
7. Eintrag in /etc/fstab



Privacy by design

DATENMISSBRAUCH VON INNEN

USB Devices stark unterschätzt

RED HAT ENTERPRISE LINUX

USBGuard

Whitelisting

Blacklisting

USB Events

1. Installieren
`yum install usbguard`
2. Ruleset erstellen
`usbguard generate-policy > /etc/usbguard/rules.conf`
3. Service starten
`start usbguard.service`
4. USB Devices listen
`usbguard list-devices`
5. Erlauben / Blockieren
`usbguard allow-device 6`
`usbguard block-device 6`
6. Regeln erstellen

DATEN AUF STORAGES

Datensicherheit im Storage Bereich

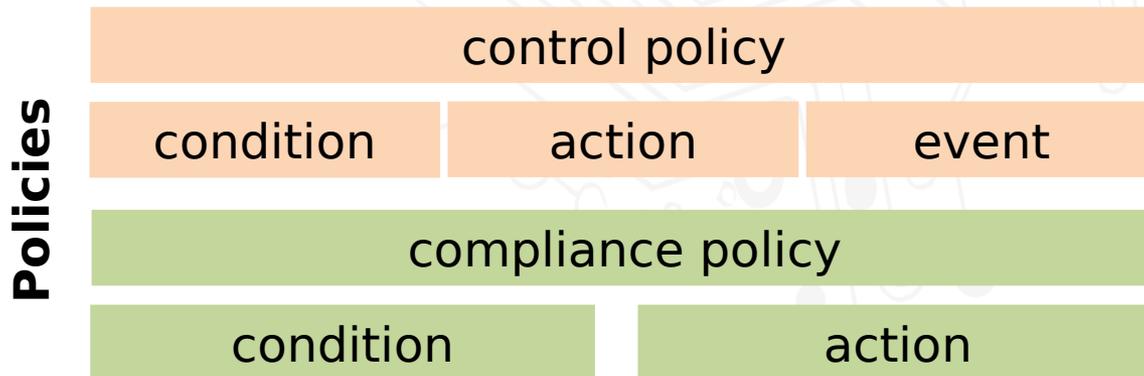
RED HAT STORAGE

- Red Hat Gluster Storage
 - Data-at-rest encryption
 - Data-in-motion encryption
- Red Hat Ceph Storage
 - Customer-provided keys
 - Key management service
 - Automatic encryption
 - Data-at-rest encryption

VERTEILTE WORKLOADS

RED HAT CLOUDFORMS

Management Engine



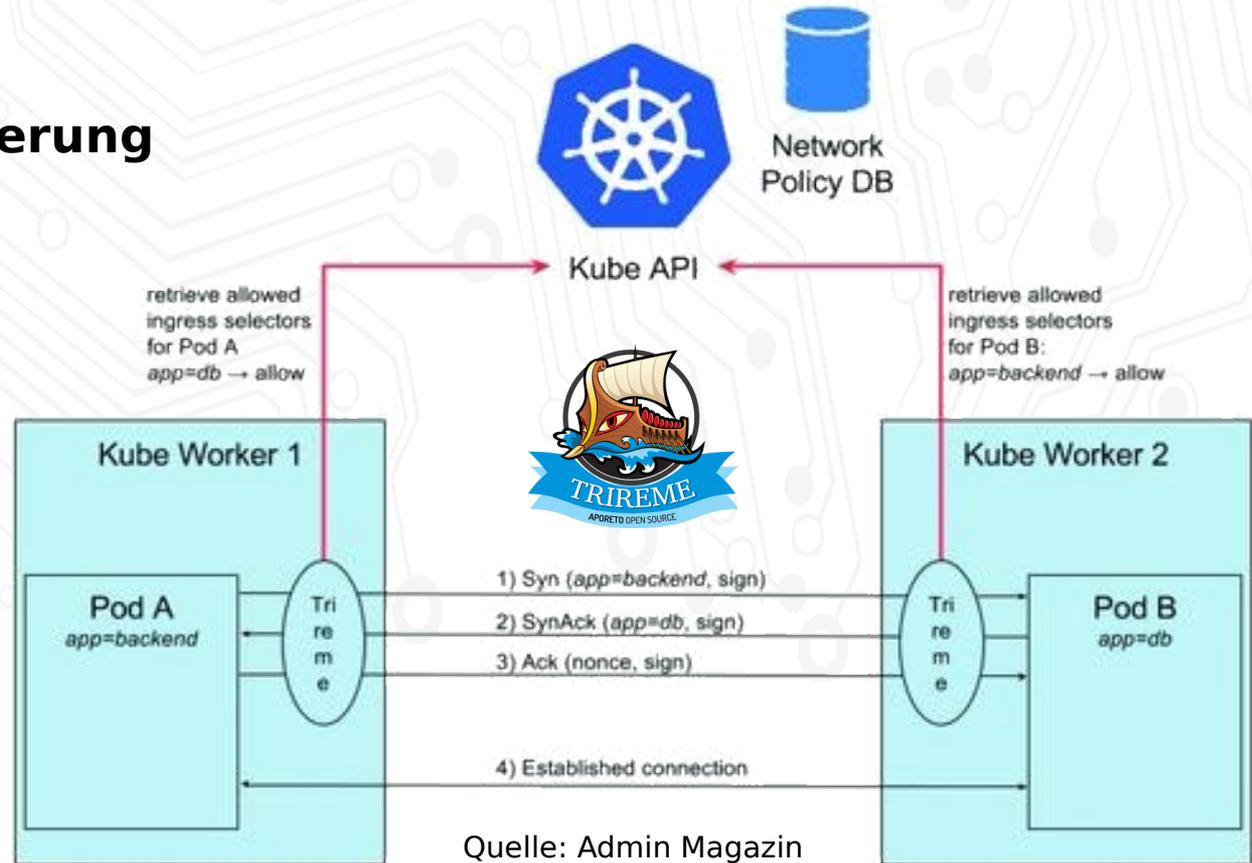
SmartState Analysis

CONTAINER ISOLIEREN

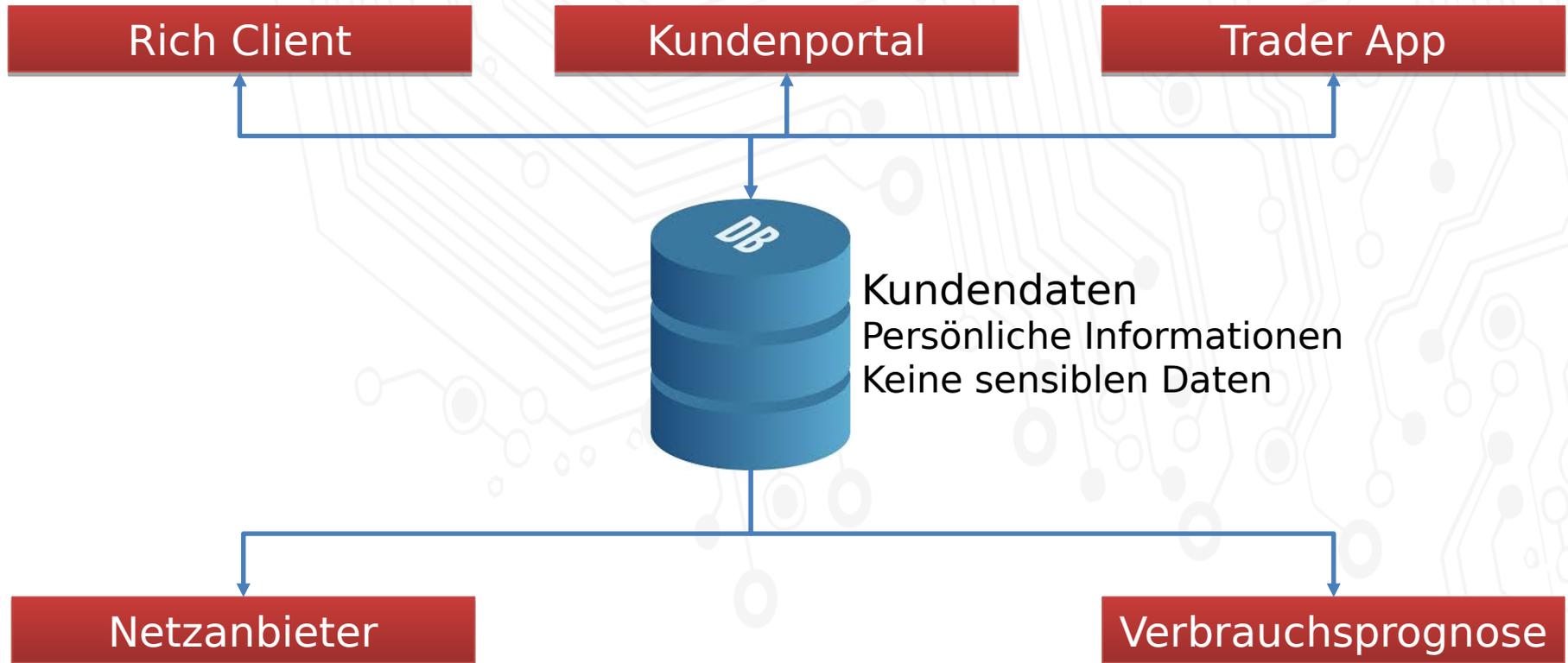
Sicherheit auf Netzwerkebene

RED HAT OPENSIFT

Container Segmentierung Aforeto Tirmere



DATENFLUSS & KONTROLLE



Energieanbieter

Rich Client

Kundenportal

Trader App

Netzanbieter

Mobile App

Verbrauchsprognose

Energy Management System - API



Kundendaten
Persönliche Informationen
Keine sensiblen Daten

Energieanbieter

Rich Client

Kundenportal

Trader App

Netzanbieter

Mobile App

Verbrauchsprognose

3SCALE BY RED HAT

Energy Management System - API



Kundendaten
Persönliche Informationen
Keine sensiblen Daten

3SCALE BY RED HAT API Management



- Schaffen Sie Bewusstsein
- Aktiv technisch SINNVOLL vorbereiten
- Red Hat Portfolio bietet einige unterstützende Komponenten
- Unbedingt an Prozessen arbeiten

**DANKE FÜR IHRE
AUFMERKSAMKEIT**