SICHERHEIT UND DIGITALE SOUVERÄNITÄT IM CLOUD COMPUTING

GLIEDERUNG

- ▶ Cloud: IaaS Layer
- ▶ Beispiel OpenStack
- ▶ Sicherheit
  - Möglichkeiten zur Absicherung
  - Entwicklung anhand von Angriffsvektoren
- ▶ Digitale Souveränität
  - Was ist das?
  - Wie kann man digitale Souveränität erreichen?

CLOUD & HEAT

STARTPUNKT:

WAS IST CLOUD?

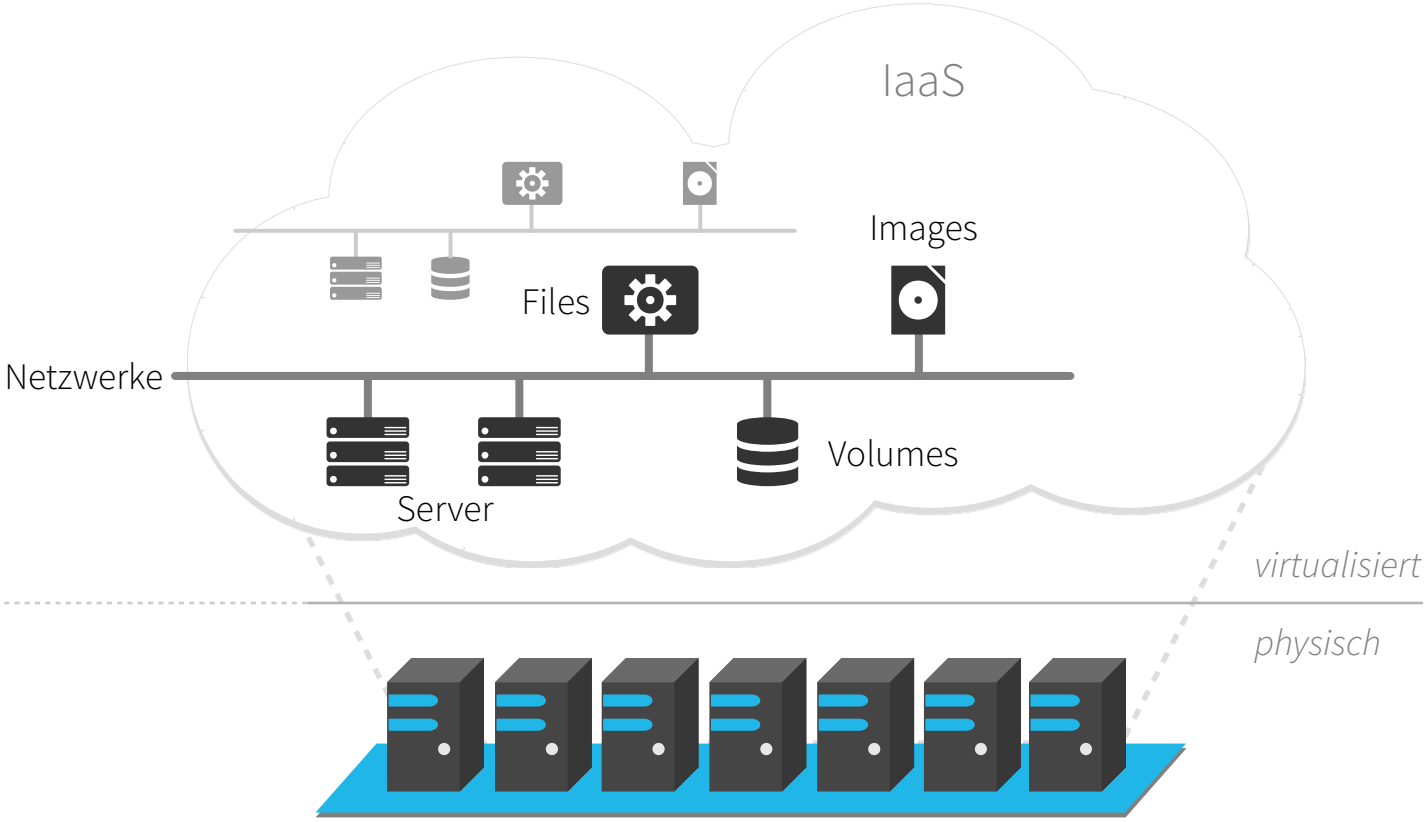
CLOUD - IAAS

“ There is no cloud, it's just someone else's computer ”

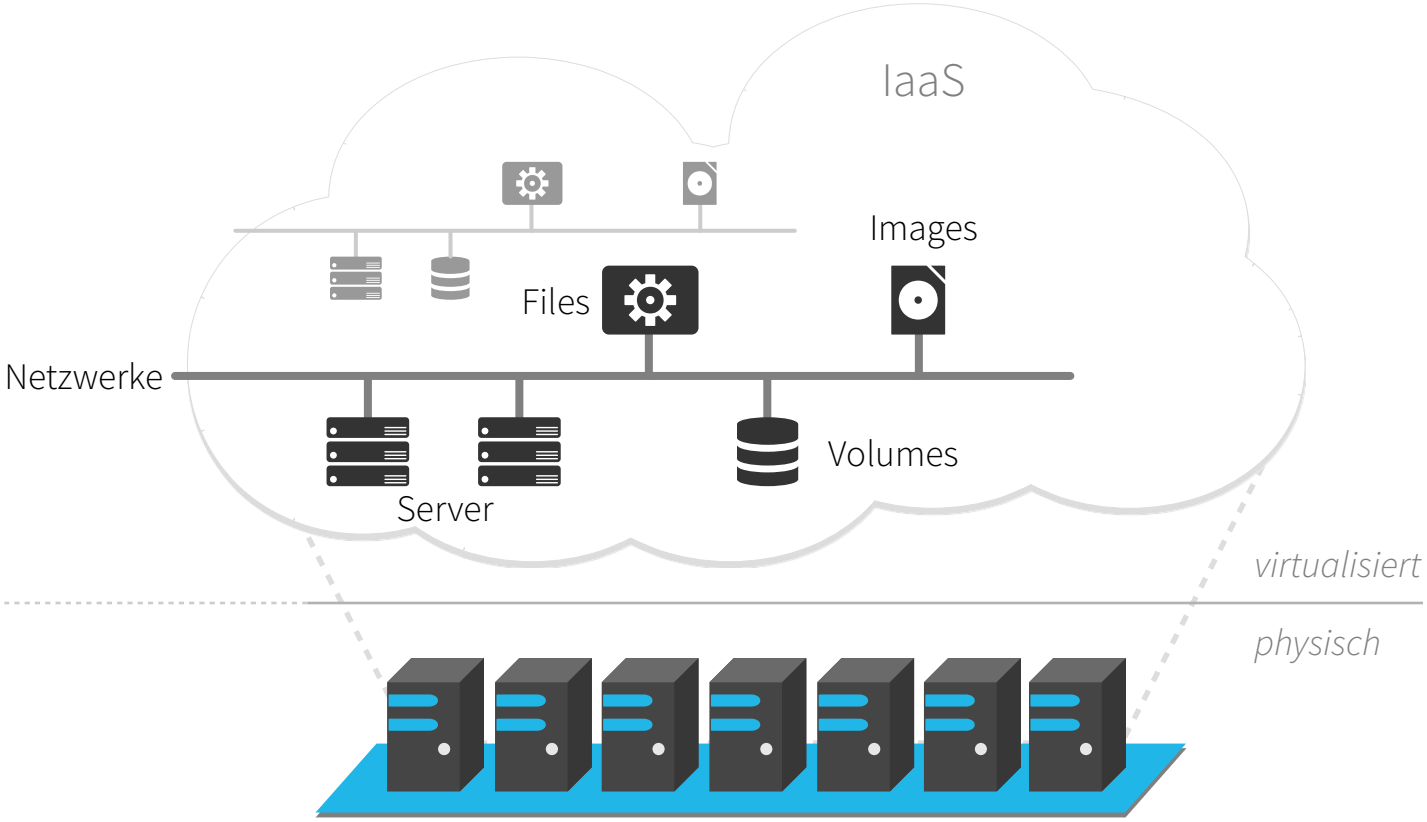
CLOUD - IAAS

Welche Objekte existieren im IaaS und müssen geschützt werden?

CLOUD - IAAS

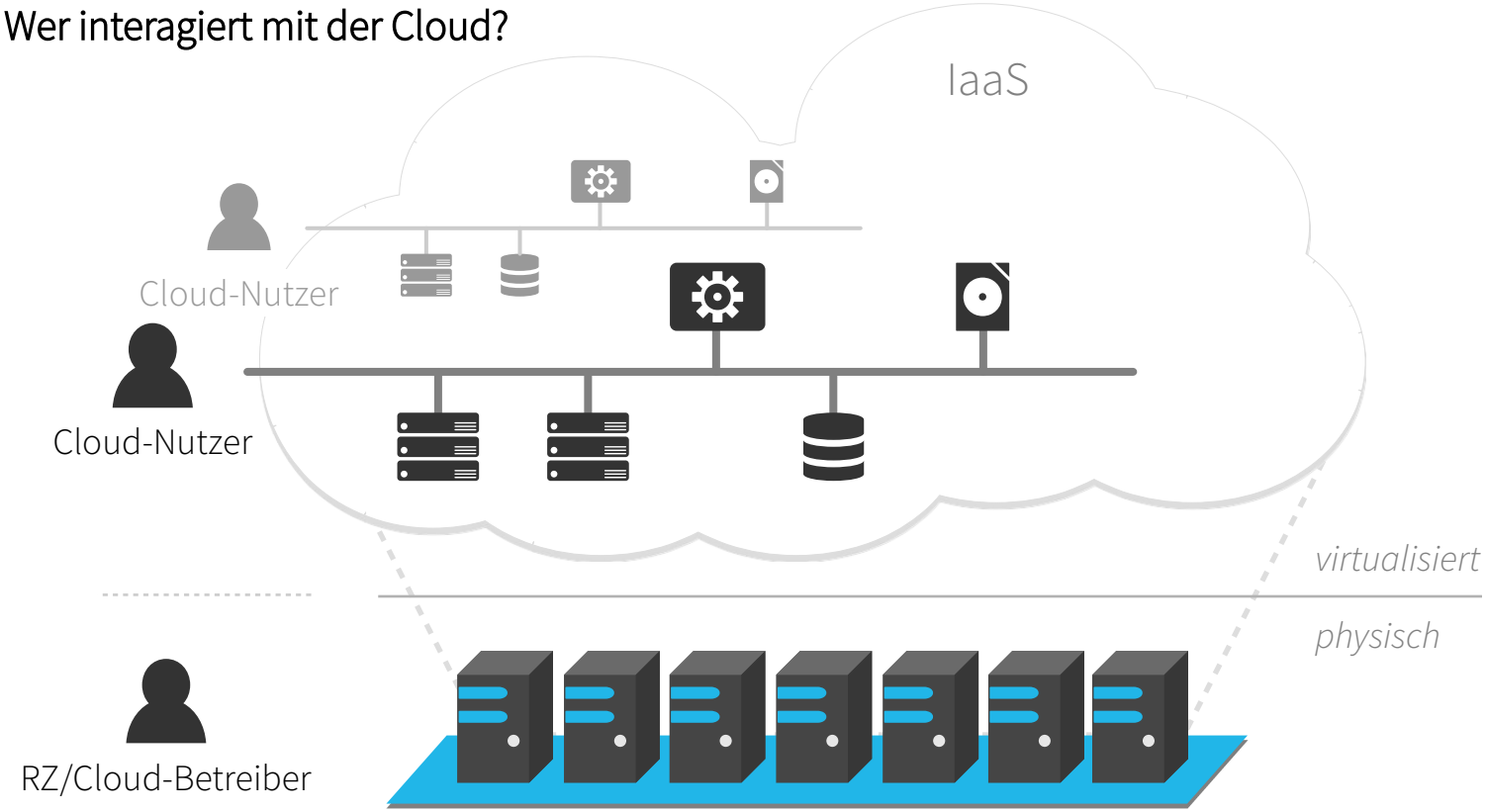

IaaS
Images
Files
Netzwerke
Volumes
Server
virtualisiert
physisch

CLOUD - IAAS


IaaS
Images
Files
Netzwerke
Volumes
Server
virtualisiert
physisch

CLOUD - IAAS

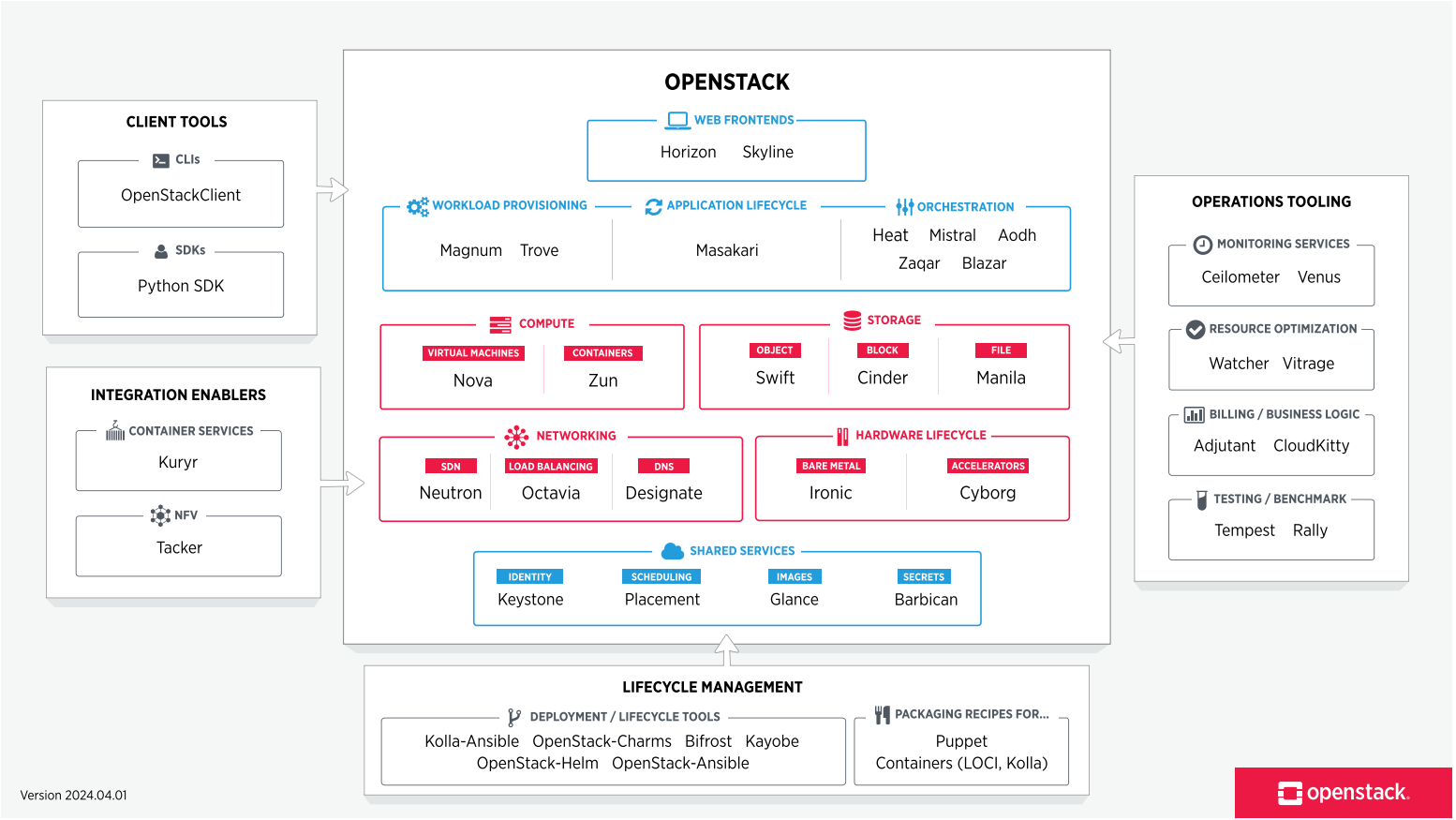
Wer interagiert mit der Cloud?



CLOUD - IAAS

Beispiel OpenStack

CLOUD - IAAS


CLIENT TOOLS
CLIs
OpenStackClient
SDKs
Python SDK
INTEGRATION ENABLERS
CONTAINER SERVICES
Kuryr
NFV
Tacker
OPENSTACK
WEB FRONTENDS
Horizon Skyline
WORKLOAD PROVISIONING
Magnum Trove
APPLICATION LIFECYCLE
Masakari
ORCHESTRATION
Heat Mistral Aodh
Zaqar Blazar
COMPUTE
VIRTUAL MACHINES
Nova
CONTAINERS
Zun
STORAGE
OBJECT
Swift
BLOCK
Cinder
FILE
Manila
NETWORKING
SDN
Neutron
LOAD BALANCING
Octavia
DNS
Designate
HARDWARE LIFECYCLE
BARE METAL
Ironic
ACCELERATORS
Cyborg
SHARED SERVICES
IDENTITY
Keystone
SCHEDULING
Placement
IMAGES
Glance
SECRETS
Barbican
OPERATIONS TOOLING
MONITORING SERVICES
Ceilometer Venus
RESOURCE OPTIMIZATION
Watcher Vitrage
BILLING / BUSINESS LOGIC
Adjutant CloudKitty
TESTING / BENCHMARK
Tempest Rally
LIFECYCLE MANAGEMENT
DEPLOYMENT / LIFECYCLE TOOLS
Kolla-Ansible OpenStack-Charms Bifrost Kayobe
OpenStack-Helm OpenStack-Ansible
PACKAGING RECIPES FOR...
Puppet
Containers (LOCI, Kolla)
Version 2024.04.01
openstack.

CLOUD - IAAS

OPENSTACK

▶ Baukastenprinzip:

- Auswahl von benötigten Services: Keystone, Barbican, Cinder, Nova, Glance, Placement, …
- Aufbau / Zusammenbau muss von Betreiber geleistet werden

▶ Zusätzliche erforderliche Infrastrukturkomponenten:

- Datenbank (Speichern der Zustände von Hosts, VMs, Informationen zu Nutzern, Projekten, …)
- Message-Dienst (z.B. RabbitMQ) zum Übermitteln von RPC-Nachrichten
- Cache (z.B. memcached)

▶ Life-Cycle-Management für Installation, Konfiguration, Updates, Zertifikatsmanagement

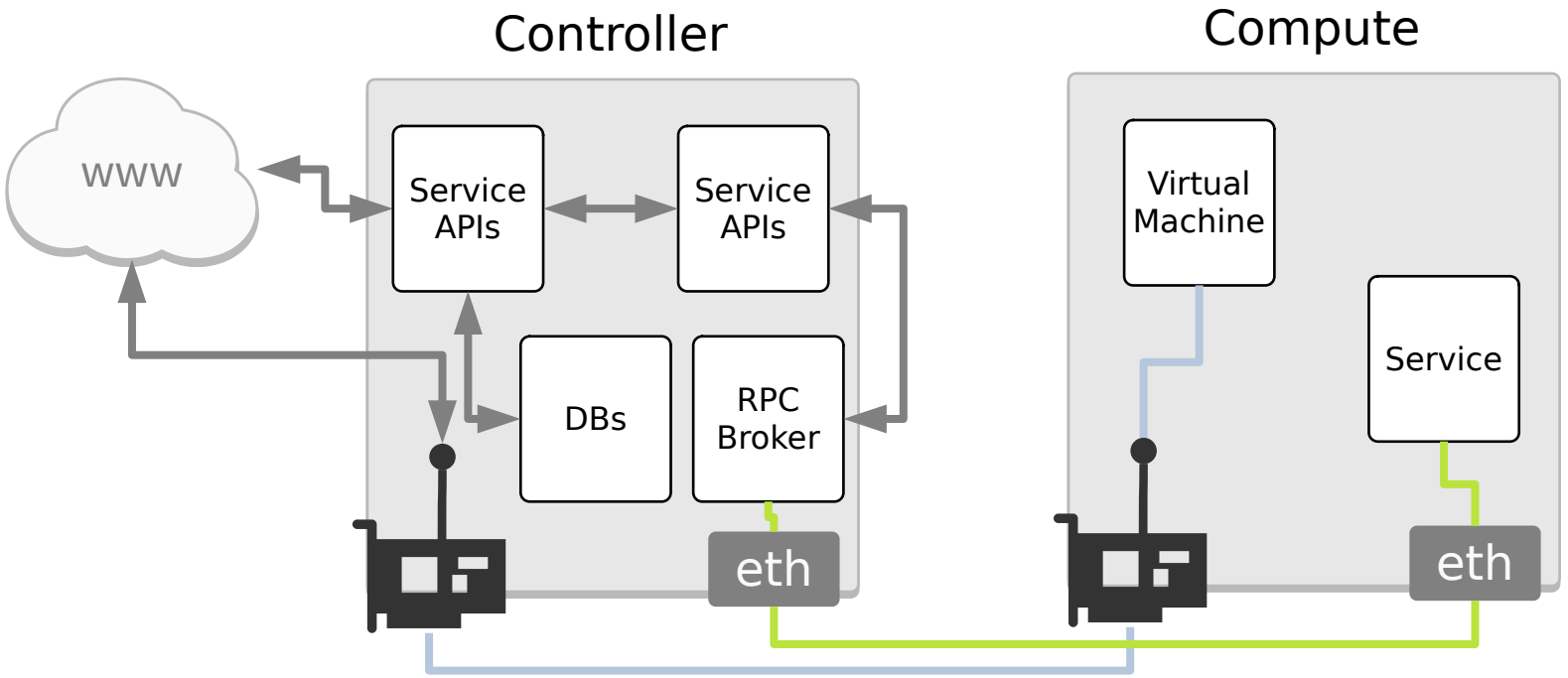
BEISPIEL NETZWERK

- Welche verschiedenene Verbindungen existieren?

CLOUD - NETZWERKVERBINDUNGEN

BEISPIEL

▶externe Netzwerke, APIs, RPC, Datenbank



CLOUD & HEAT

SICHERHEIT

- Welche Schutzziele gibt es?
- Was ist ein Angriffsvektor

SICHERHEIT

SCHUTZZIELE

- Vertraulichkeit
  - Daten/Informationen können nicht von Ungefugten gelesen werden
- Integrität
  - Daten wurden nur von autorisierten Nutzern verändert
- Verfügbarkeit
  - Daten sind zugänglich
- Authentizität
  - Ein Nutzer ist der, der er vorgibt zu sein
- Autorisierung
  - Einschränkung des Zugriffs auf Daten

SICHERHEIT

ANGRIFFSVEKTOR

Wer kann **wo** und **wie** (und **wann**) angreifen?

SICHERHEIT

ANGRIFFSVEKTOR

Wer kann **wo** und **wie** (und **wann**) angreifen?

Betreiber
Admin
Nutzer

SICHERHEIT

ANGRIFFSVEKTOR

Schnittstellen

Wer kann **wo** und **wie** (und **wann**) angreifen?

Betreiber
Admin
Nutzer

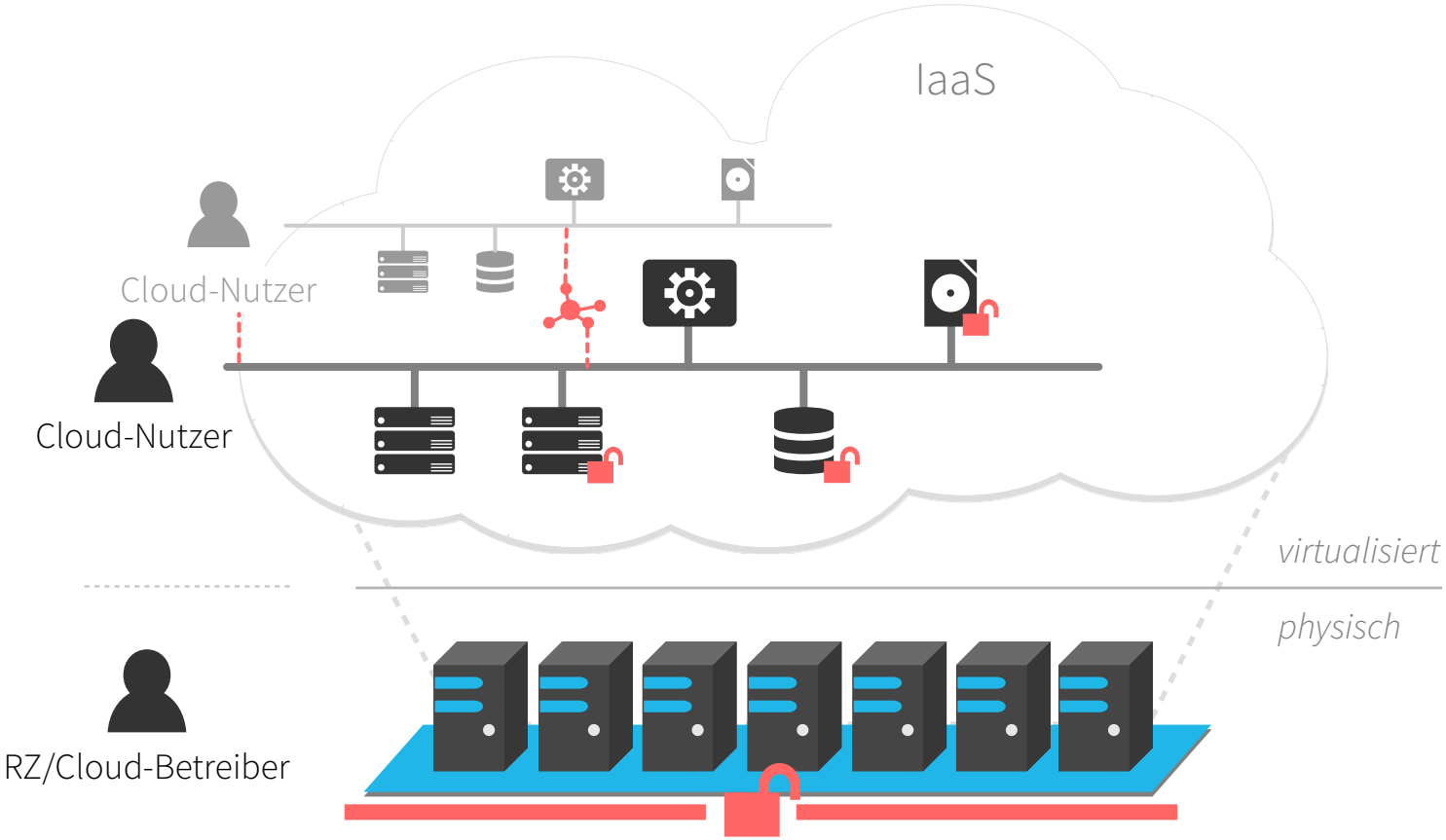
SICHERHEIT

ANGRIFFSVEKTOR

SICHERHEIT

ANGRIFFSVEKTOR

CLOUD - ANGRIFFSVEKTOREN



SICHERHEIT

IDEEN

- ▶ Absicherung der Nutzerdaten
  - Verschlüsselung aktivieren oder einbauen
- ▶ Sicherer Zugang zur Cloud
  - VPN(aaS)
- ▶ Separation von Projekten und Domänen
  - Ermöglicht Nutzerselbstverwaltung
- ▶ Härtung und Absicherung der OpenStack Infrastruktur
  - Physische Absicherung
  - Absicherung der IaaS-Services

Möglichkeiten zur Absicherung

MÖGLICHKEITEN ZUR ABSICHERUNG

IDEEN

- Hardwareanpassung:
  - Nutzung von HSMs
  - Nutzung spezifischer Hardware (Netzwerkkarten, CPUs)
- Konfigurationsanpassungen:
  - TLS everywhere
  - Verschlüsselte Datanbankverbindung
  - Absicherung von RPC
  - Aktivierung von Barbican
  - Aktivierung verschlüsselter Volumes

MÖGLICHKEITEN ZUR ABSICHERUNG

IDEEN

▶ Codeanpassung:

- Verschlüsselung
- Zugangsbeschränkungen

▶ Neue Konzepte:

- Mandantentrennung

CLOUD & HEAT

ENTWICKLUNG UND KONFIGURATION

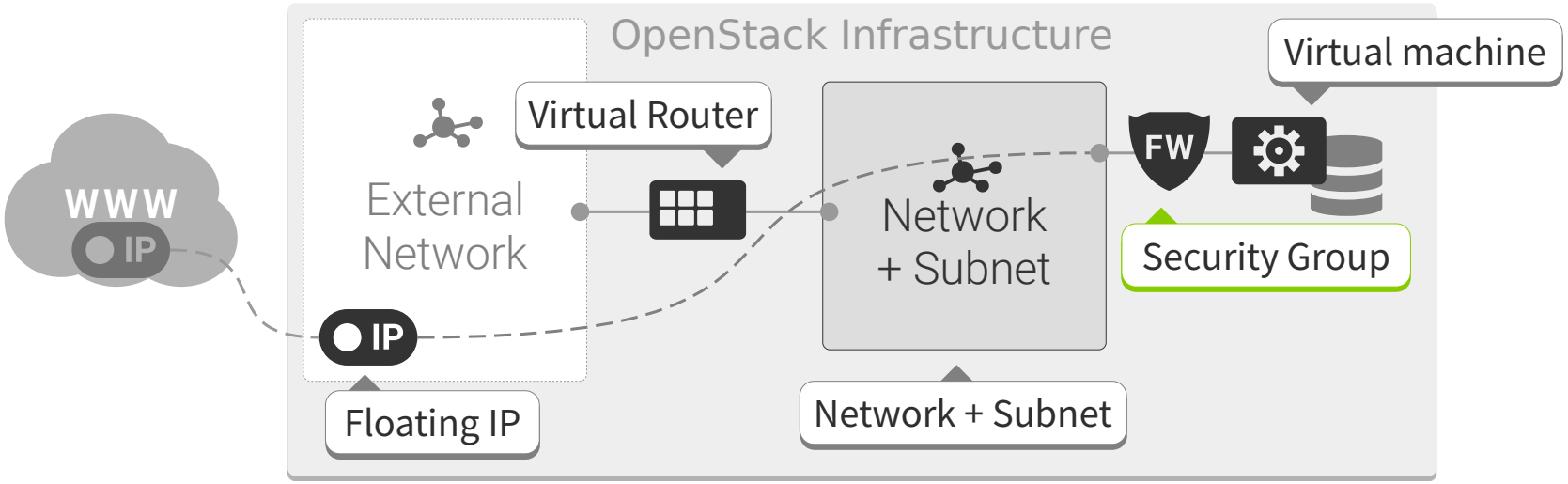
- Anhand von Angriffsvektoren

1. Kommunikationsabsicherung
AV: Man in the Middle

1. KOMMUNIKATIONSABSICHERUNG

NETZWERKE

- ▶VPN zwischen Client und Infrastruktur
- ▶Netzwerkverschlüsselung für Traffic innerhalb der Infrastruktur
- ▶Security Groups (Sicherheitsgruppen) sind Sets an ip-table Regeln, die auf Ports angewendet werden



2. Verschlüsselung von Nutzerdaten
AV: Lesen / Verändern der Daten durch Dritte

VERSCHLÜSSELUNG VON RESSOURCEN

AKTUELLER STAND UND AUSBLICK

▶Verschlüsselte Volumes sind implementiert und nutzbar

▶Es gibt Einzelfälle, in denen verschlüsselte Images existieren

▶VM verschlüsselung wird zur Zeit überarbeitet

Volumes

- **verschlüsselbar durch volume type**
- **Implementation ist nutzbar seit Einigen Jahren**

Images

- **nur verschlüsselt, wenn durch Volume erstellt oder hoch-geladen***
- **Upstream patches zur verschlüsselung vorhanden**

VMs

- **bisher wird ein dmcrypt device auf dem Host permanent geöffnet**
- **neue Version wird z.Z. entwickelt**

* verschlüsselte images können hochgeladen werden, aber benötigte Parameter können dabei noch nicht gesetzt werden.

SICHERHEIT

IDEEN

Mehr Interesse an Sicherheit im Cloud Computing?

ES GIBT GUIDES, RICHTLINIEN UND DOKUS

WO?

- Security Guide von OpenStack
  - Link: https://docs.openstack.org/security-guide/
  - Für Betreiber von OpenStack Infrastrukturen
- Guides des SCS Projekts
  - Link: https://docs.scs.community/docs/iaas/guides/
  - z.B. Guide für die Erstellung von Sicherheitsgruppen
  - Für Betreiber und Nutzer von Cloud (auch über IaaS hinaus)
- Allgemeine Informationen zu Sicherheit im Cloud Computing
  - das BSI hat viele Guides und Richtlinien zu Availibility, Risikoanalysen, Fehlerfälle, etc…
  - Für Betreiber

DIGITALE SOUVERÄNITÄT

▶ Was ist das?

DIGITALE SOUVERÄNITÄT

DEFINITION

Digitale Souveränität gibt Unternehmen sowie Individuen die Möglichkeit im digitalen Raum selbstbestimmt, selbstständig und sicher Handeln bzw. Entscheiden zu können.

DIGITALE SOUVERÄNITÄT

BEISPIEL

Ein Unternehmen entwickelt eine kritische Software für die Verwaltung eines Krankenhauses.

- **Wer** stellt eine Versionierungssoftware bereit? (z.B. Gitlab) → Wahl eines Anbieters oder Selbstverwaltung
- **Wo** wird der Softwarestand versioniert? → physischer Host
- **Was** wird dort gespeichert? → Einordnung kritischer Dokumente
- **Wer** hat Zugriff? → Zugriffskontrolle über eigene Mitarbeiter bis hin zum Provider plus Möglichkeiten zur Verschlüsselung

DIGITALE SOUVERÄNITÄT

BEISPIEL

Ein Unternehmen entwickelt eine kritische Software für die Verwaltung eines Krankenhauses.

- Hier bedeutet digitale Souveränität die Möglichkeit zur freien **Auswahl** eines Möglichen Providers einer Gitlab-Instanz.
- Des Weiteren bringt es die **Möglichkeit** zum Wechsel des Providers.

DIGITALE SOUVERÄNITÄT

VORRAUSSETZUNGEN

- Möglichkeit zur Auswahl (z.B. Provider von IaaS / PaaS)
  - Ist gegeben wenn ausreichend verschiedene Wettbewerber vorhanden sind
- Möglichkeit zum Wechsel eines Dienstleisters (von IaaS Provider A zu IaaS Provider B)
  - Bedingt ähnliche oder gleiche Struktur des IaaS → kein Vendor Lock-In
  - Wird teilweise ermöglicht durch Nutzung von Open Source
  - Verbesserung durch Standardisierung möglich

DEFAULT SECURITY GROUP RULES STANDARD

BEISPIEL STANDARDISIERUNG

- In OpenStack gibt es Sets von IP-Table rules = Security Groups
- Wenn eine VM ohne Security Group erstellt wird, bekommt sie automatisch die “default Security Group”
- Die Regeln innerhalb dieser Gruppen werden vom Betreiber vorab bestimmt

```
stack@devstack:~/devstack$ openstack default security group rule list --max-width 100
+----------+-------------+----------+----------+------------+-----------+-----------------------+---------------------+-------------------------------+-------------------------------+
| ID       | IP Protocol | Ethertype | IP Range | Port Range | Direction | Remote Security Group | Remote Address Group | Used in default Security Group | Used in custom Security Group |
+----------+-------------+----------+----------+------------+-----------+-----------------------+---------------------+-------------------------------+-------------------------------+
| 2b82f187 | None        | IPv6     | ::/0     |            | egress    | None                  | None                | True                          | True                          |
| -b385-   |             |          |          |            |           |                       |                     |                               |                               |
| 4fae-    |             |          |          |            |           |                       |                     |                               |                               |
| 9142-    |             |          |          |            |           |                       |                     |                               |                               |
| 6a72ace7 |             |          |          |            |           |                       |                     |                               |                               |
| 2fac     |             |          |          |            |           |                       |                     |                               |                               |
| 315c216b | None        | IPv4     | 0.0.0.0/ |            | ingress   | PARENT                | None                | True                          | False                         |
| -05ef-   |             |          | 0        |            |           |                       |                     |                               |                               |
| 42a4-    |             |          |          |            |           |                       |                     |                               |                               |
| a0ca-    |             |          |          |            |           |                       |                     |                               |                               |
| 84f73582 |             |          |          |            |           |                       |                     |                               |                               |
| 08c2     |             |          |          |            |           |                       |                     |                               |                               |
| 44700fc3 | None        | IPv4     | 0.0.0.0/ |            | egress    | None                  | None                | True                          | True                          |
| -d576-   |             |          | 0        |            |           |                       |                     |                               |                               |
| 4dce-bf7 |             |          |          |            |           |                       |                     |                               |                               |
| f-       |             |          |          |            |           |                       |                     |                               |                               |
| b530b9ef |             |          |          |            |           |                       |                     |                               |                               |
| 1074     |             |          |          |            |           |                       |                     |                               |                               |
| e66c8e2c | None        | IPv6     | ::/0     |            | ingress   | PARENT                | None                | True                          | False                         |
| -8d42-   |             |          |          |            |           |                       |                     |                               |                               |
| 4a0f-    |             |          |          |            |           |                       |                     |                               |                               |
| a84d-    |             |          |          |            |           |                       |                     |                               |                               |
| deb7e9c3 |             |          |          |            |           |                       |                     |                               |                               |
| 7b6b     |             |          |          |            |           |                       |                     |                               |                               |
+----------+-------------+----------+----------+------------+-----------+-----------------------+---------------------+-------------------------------+-------------------------------+
```

ZUSAMMENFASSUNG

- ▶Angriffsvektoren bestimmen: Wer, Wo, Was?
- ▶Absicherung durch Hardware-, Konfigurations- und Codeanpassungen
- ▶auch Kombinationen von Anpassungen nötig
- ▶Vorgestellte Sicherheitsmaßnahmen sind präventiv
- ▶Zusätzlich wichtig sind detektive und reaktive Maßnahmen
- ▶Überblick über digitale Souveränität
- ▶Beispiel zu Standardisierung