



BEHÖRDENCLOUD ZUGELASSEN FÜR GEHEIM MIT L4RE

Dr.-Ing. Michael Hohmuth | Geschäftsführer Kernkonzept GmbH

In meinem Talk

- 01** Über Kernkonzept
- 02** Vorteile einer Cloud
- 03** Geheime Cloud unmöglich mit klassischem Hypervisor
- 04** Neue Architektur für geheime Cloud
- 05** Mehrere Informationsräume ohne Neuverkabeln

Wer ist Kernkonzept?

Inhabergeführt,
Sitz in Dresden

Gegründet 2012,
stetig wachsend

Spin-off der TU
Dresden

Internationales
Team von 30+

Umfassende
Erfahrung seit
1996

Forschungsnah
und innovativ

Betriebssystem-
Spezialisten

Reifes L4Re
Operating System
Framework

Adressierte Märkte



**AUTO-
MOTIVE**



**HIGH
ASSURANCE**



**CYBER
SECURITY**



**SECURE
ENDPOINT**



**SMART
HOME**



**SECURE
CLOUD**



**INDUSTRIAL
IOT**



AVIONICS

Vorteile der Cloud

Kosten-
ersparnisse

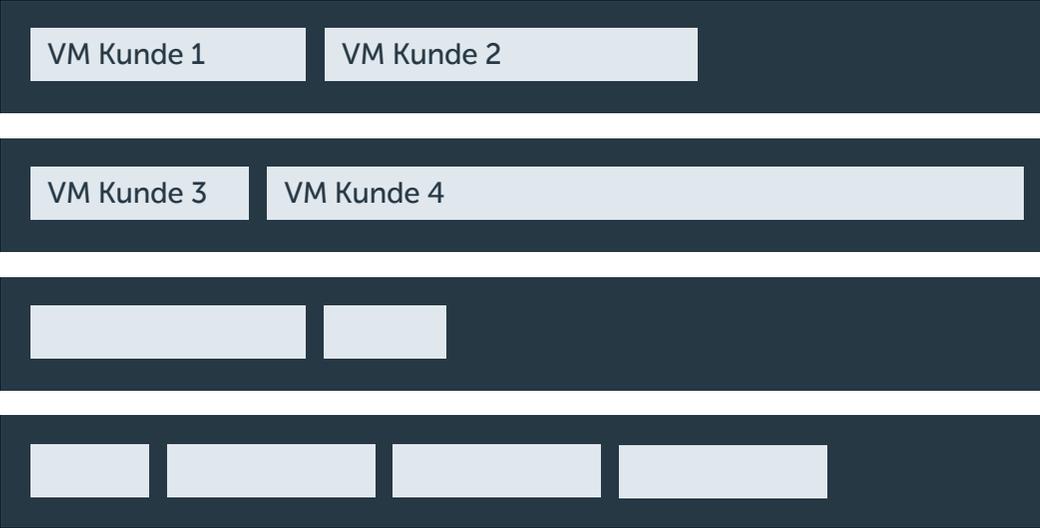
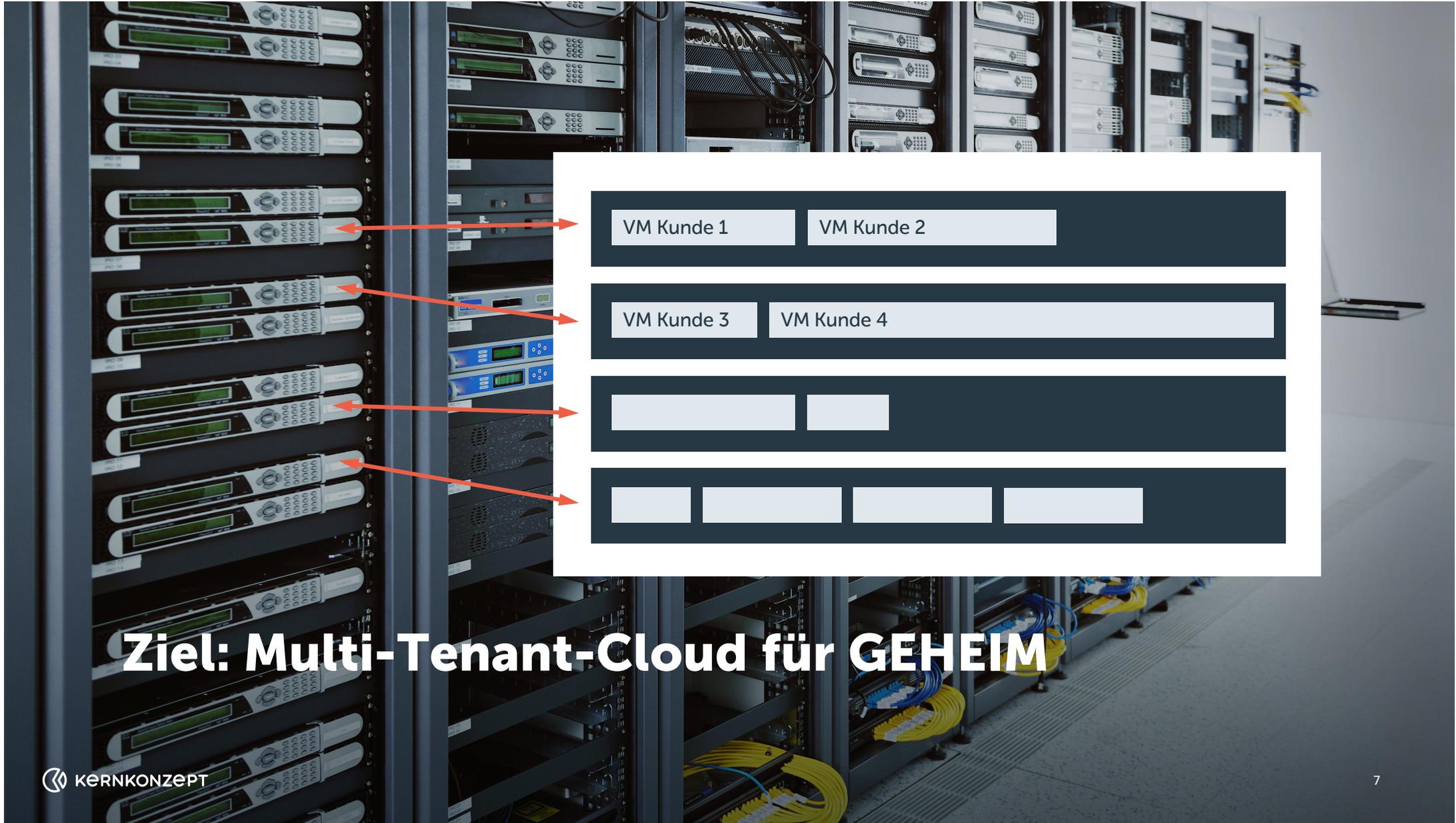
Zentrale
Administration

Flexible
Reaktion auf
Lastensituation

Höhere
Sicherheit

Ausfallsicherheit

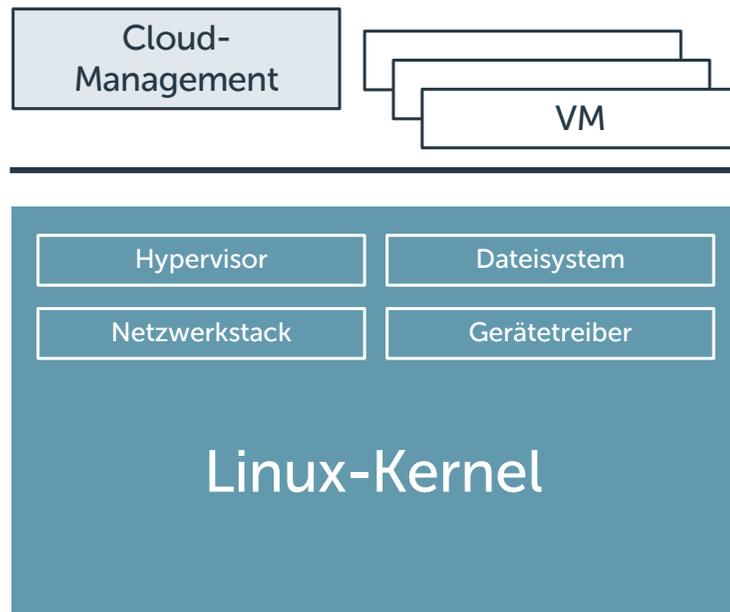
State of the Art



Ziel: Multi-Tenant-Cloud für GEHEIM

Monolithischer Hypervisor

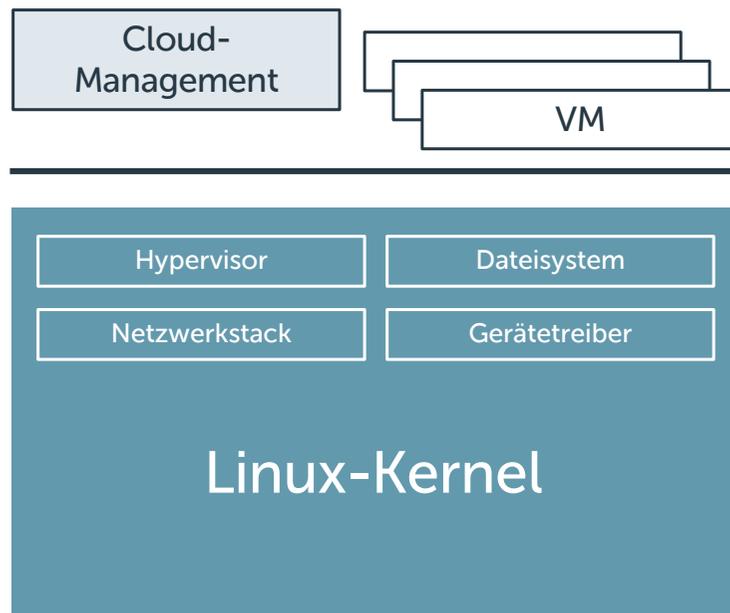
+ Klassische Cloud



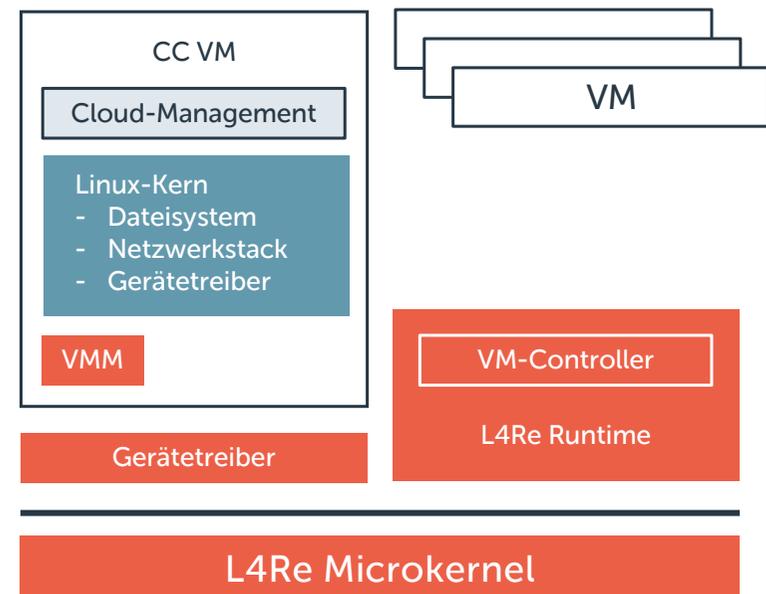
- + Zu große Trusted Computing Base
- + Isolation kann nicht verlässlich durchgesetzt werden
- + Nicht zulassungsfähig

Vertrauenswürdige Isolation

+ Klassische Cloud

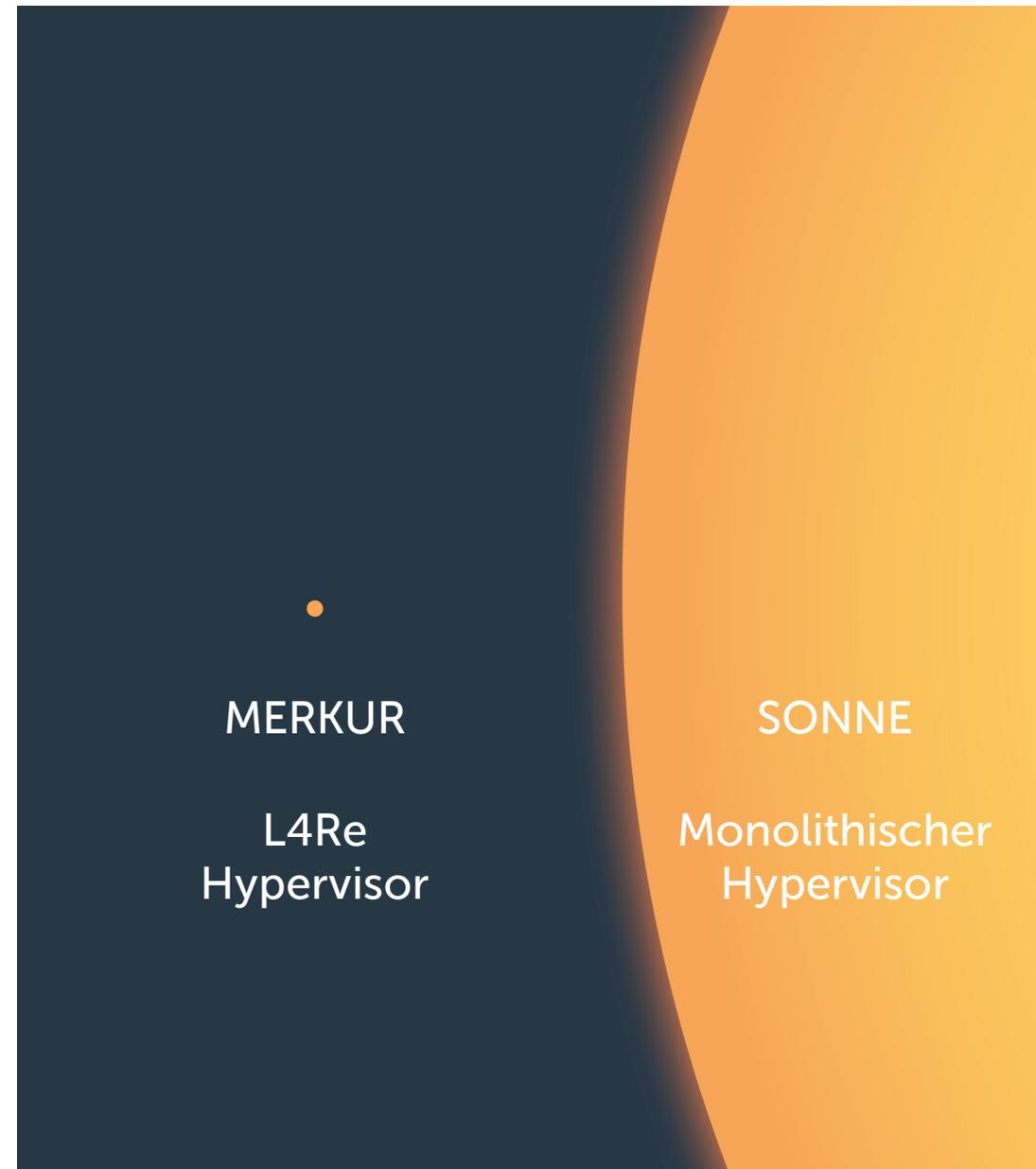


+ L4Re-Cloud



TCBs im Vergleich

- + **Monolithischer Hypervisor: viele Mio. Zeilen Code**
- + **L4Re: 30.000 Zeilen Code**

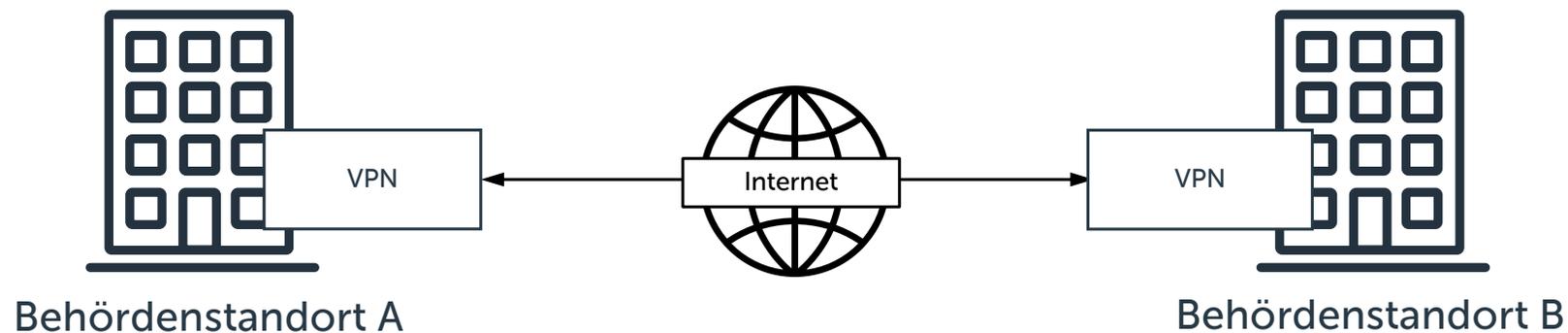


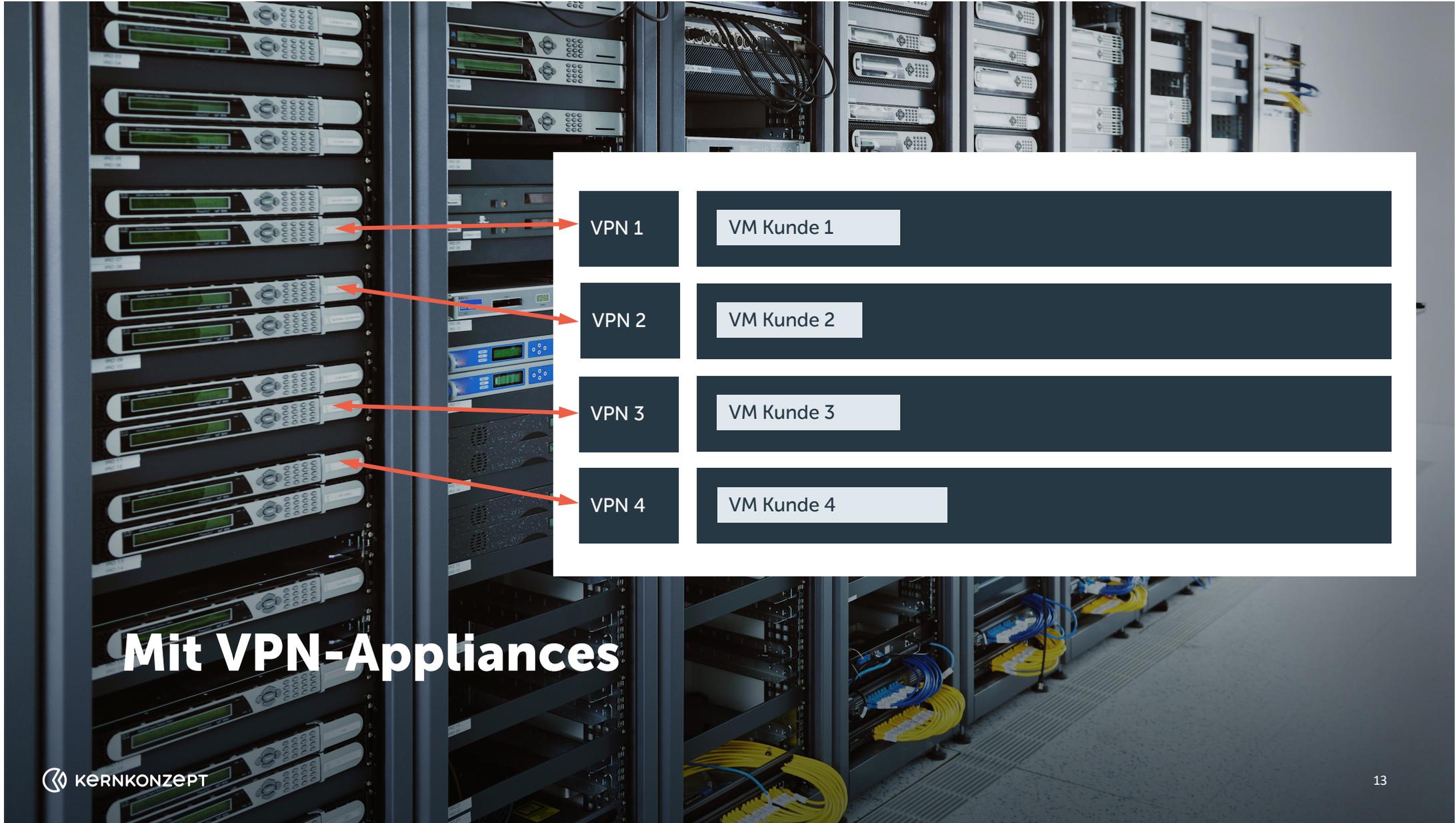
Problemstellung

- + Für eine Behörde muss die sichere Kommunikation mit der VM sichergestellt sein**

Virtual Private Network (VPN)

- + Überbrückt nicht vertrauenswürdige Netze mit Crypto
- + VPN-Geräte sind zugelassen und am Markt





VPN 1

VM Kunde 1

VPN 2

VM Kunde 2

VPN 3

VM Kunde 3

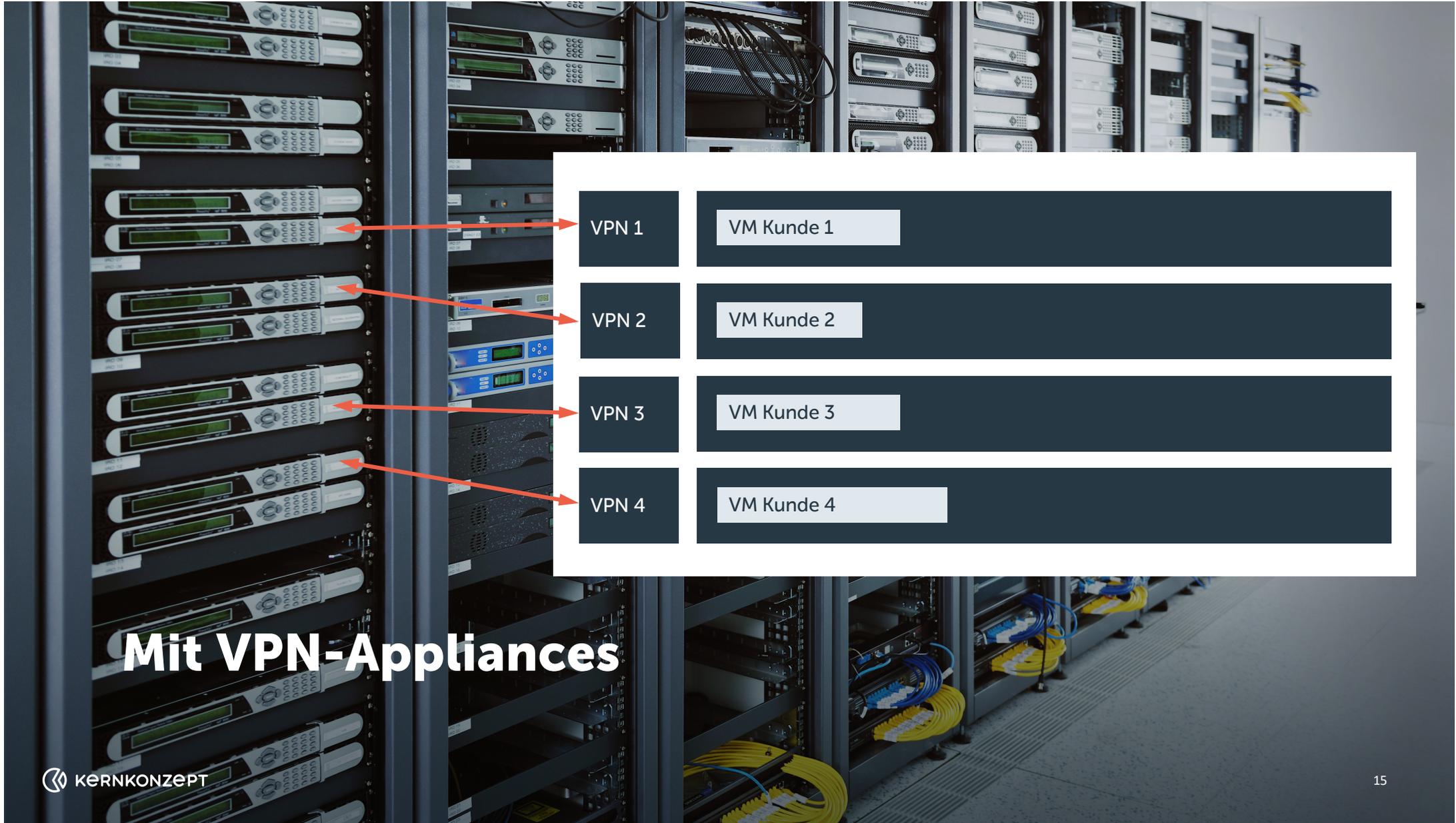
VPN 4

VM Kunde 4

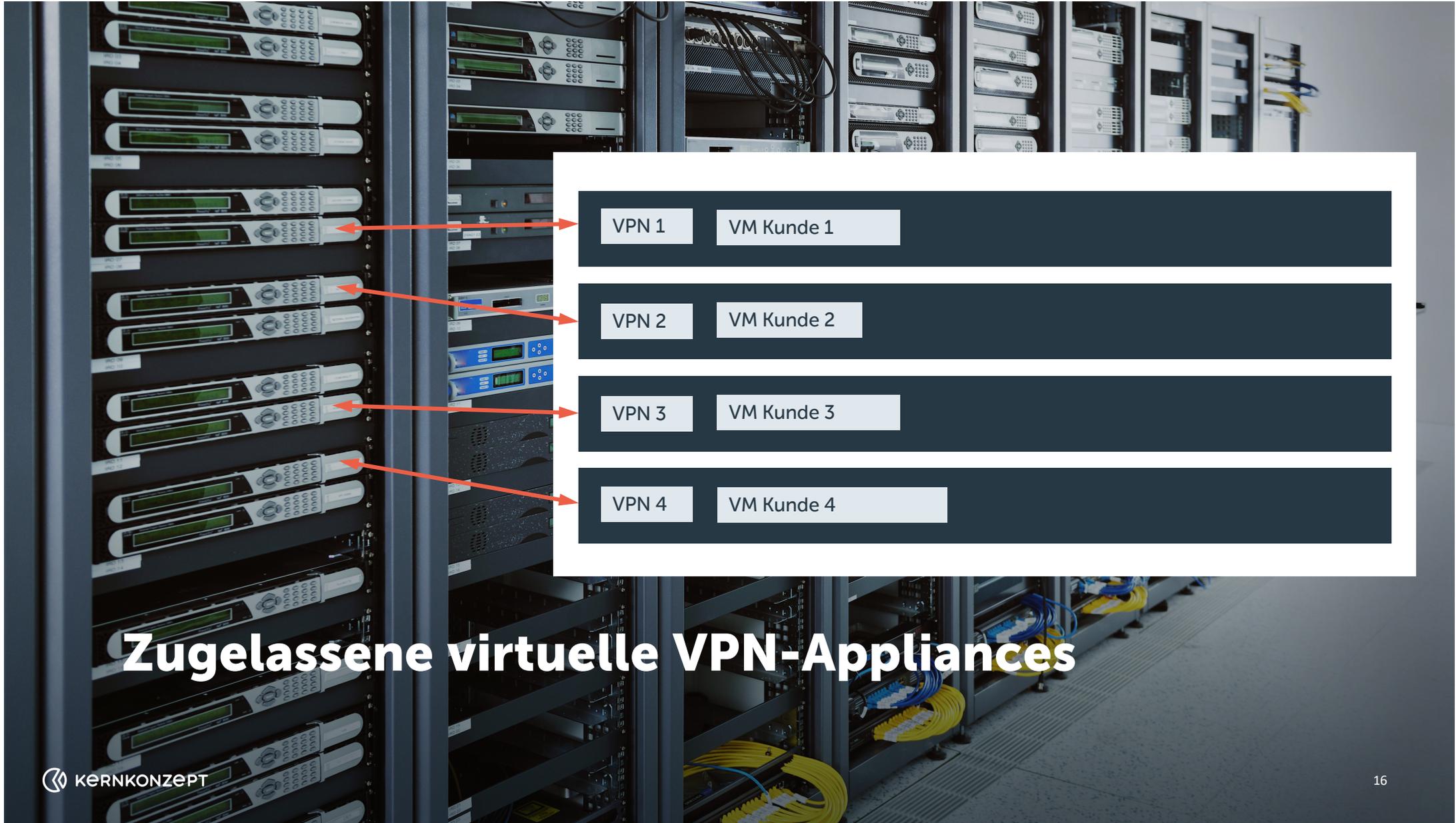
Mit VPN-Appliances

A man with short brown hair and a beard, wearing a black t-shirt and blue suspenders, is looking down at a silver laptop in a server room. He is surrounded by rows of server racks filled with orange and blue cables. The lighting is dim, with a blueish tint. The text 'Verkabelung – Fehleranfälligkeit' is overlaid in white on the bottom left of the image.

Verkabelung – Fehleranfälligkeit



Mit VPN-Appliances



Zugelassene virtuelle VPN-Appliances

Schlüsseltechnologie: Virtueller VPN-Endpunkt

+ Zugelassener L4Re-Separationkernel

- Verschiebt zugelassenen VPN-Endpunkt aus separatem Gerät in virtuelle Maschine
- Separation durchgesetzt durch Microkernel
- Zulassungserhaltend

VISION: DATACENTER / CLOUD FÜR GEHEIM

Vision: Skalierbarer Cloud-/Datacenter-Betrieb für VS

+ Heute: Keine gemeinsame Ressourcennutzung

- Neues Datacenter für neue Domäne
- Cloud-Skalierung nur innerhalb einer Domäne möglich

+ Vision: Mehrere Domänen auf einer Infrastruktur

- Geteilte CPU-Blades / Netzwerktopologie
- Co-Hosting mehrerer Domänen, z. B. GEHEIM-VS-NfD oder VS-NfD-NATO-RESTRICTED
- Skalierbarkeit über Domänengrenzen
- Domänenübergreifende Anwendungen

Vision: Zugelassene Software-Appliances

+ Heute: GEHEIM-Zulassung nur als Hardware-Appliance

- Internet Exchange Gateways (IEGs), VPNs, Firewalls

+ Vision: GEHEIM-Zulassung für „Software-Appliances“

- Dynamische Instanziierung, beliebig oft
- Basis: GEHEIM-zugelassene Datacenter-Plattform

Vision: Security Domain as a Service

+ Heute: Riesiger Aufwand, wenig Skalierbarkeit

- Neues Datacenter für neue Domäne
- Neue Appliances, Neuinstallation, neu verkabeln
- „Monate“

+ Vision: Security Domain auf Knopfdruck

- Neue Domäne dynamisch erfassen
- Software-Appliances, VPN zwischen Knoten
- „Minuten“

Zugelassene Datacenter-Plattform

+ **Zugelassenes Hardware-Profil**

- Off the Shelf – soweit möglich
- Secure Boot, Hardware-Anker, Netzwerkbeschleunigung

+ **Zugelassener Separation Kernel**

- Erweiterung der L4Re-Zulassung

+ **Zugelassene Infrastrukturkomponenten**

- IEG, VPN, vHSM, Storage, vNet

+ **Erlaubt zulassungskonformen Plattformbetrieb**

- Container, Middleware usw.

Dynamisches Ausfassen einer neuen Sicherheitsdomäne

+ L4Re beherrscht isolierte Domänen

+ Herausforderungen

- Domäne darf keine Residuen früherer Nutzung enthalten
- Isolation muss unerwünschte Kanäle unterbinden

+ Erster Ansatz

- Bereitstellung von vorgehaltenen leeren Domänen
- GEHEIM: Vorerst keine Freigabe von Domänen
- Unerwünschte Kanäle je nach Hardware-Profil durch physische Separation unterbinden

Instanziierung von zugelassenen Software-Appliances

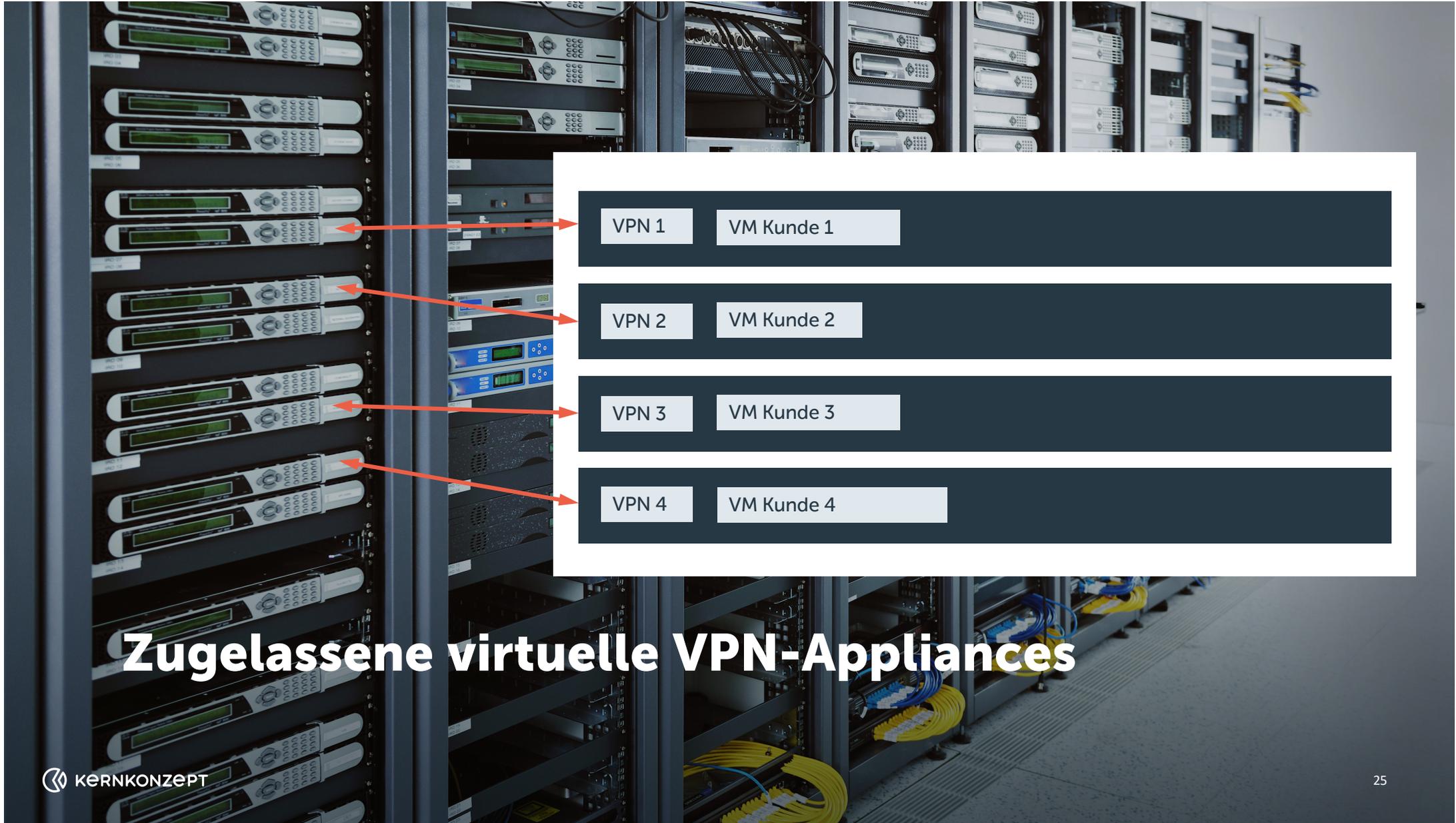
+ App-Store / Warenkorb

- IEGs, VPNs, Firewalls usw.

+ Manifest deklariert funktionale/Sicherheitsanforderungen

- Gerätezugriff
- Isolationsanforderungen / Domänen
- Virtuelles Netzwerk
- Zugriffsrechte

+ Infrastruktur setzt Anforderungen um – konformer Betrieb



VPN 1 VM Kunde 1

VPN 2 VM Kunde 2

VPN 3 VM Kunde 3

VPN 4 VM Kunde 4

Zugelassene virtuelle VPN-Appliances

NSC: National Secure Cloud

- + **Cloud-Technologiestack für Infrastrukturbetreiber**
- + **Multi-Domain, Security Domain as a Service**
- + **Partner: IABG + Infodas + Kernkonzept + weitere Partner**
- + **SaaS – PaaS – IaaS**
- + **Kubernetes in L4Re-Domänen, Cloud Management Platform, IEG, Network Acceleration, HSM-Virtualisierung**



ZUSAMMENFASSUNG

GEHEIM-Cloud mit dem L4Re Hypervisor

- + L4Re Hypervisor ermöglicht vertrauenswürdige Netzwerkverschaltung direkt im Hypervisor**
 - Vertrauenswürdige Trennung von VMs
 - Vertrauenswürdige Netzwerkanbindung der VMs
- + Vision: Zugelassene GEHEIM-Cloud-Plattform**
 - Security Domains / Software Appliances per Knopfdruck
- + Realisierung einer zulassungsfähigen geheimen Cloud**
 - National Secure Cloud



VIELEN DANK!

Bitte besuchen Sie uns an unserem Stand!

www.kernkonzept.com