WITSTOR
SYSTEMLÖSUNGEN . SERVICE

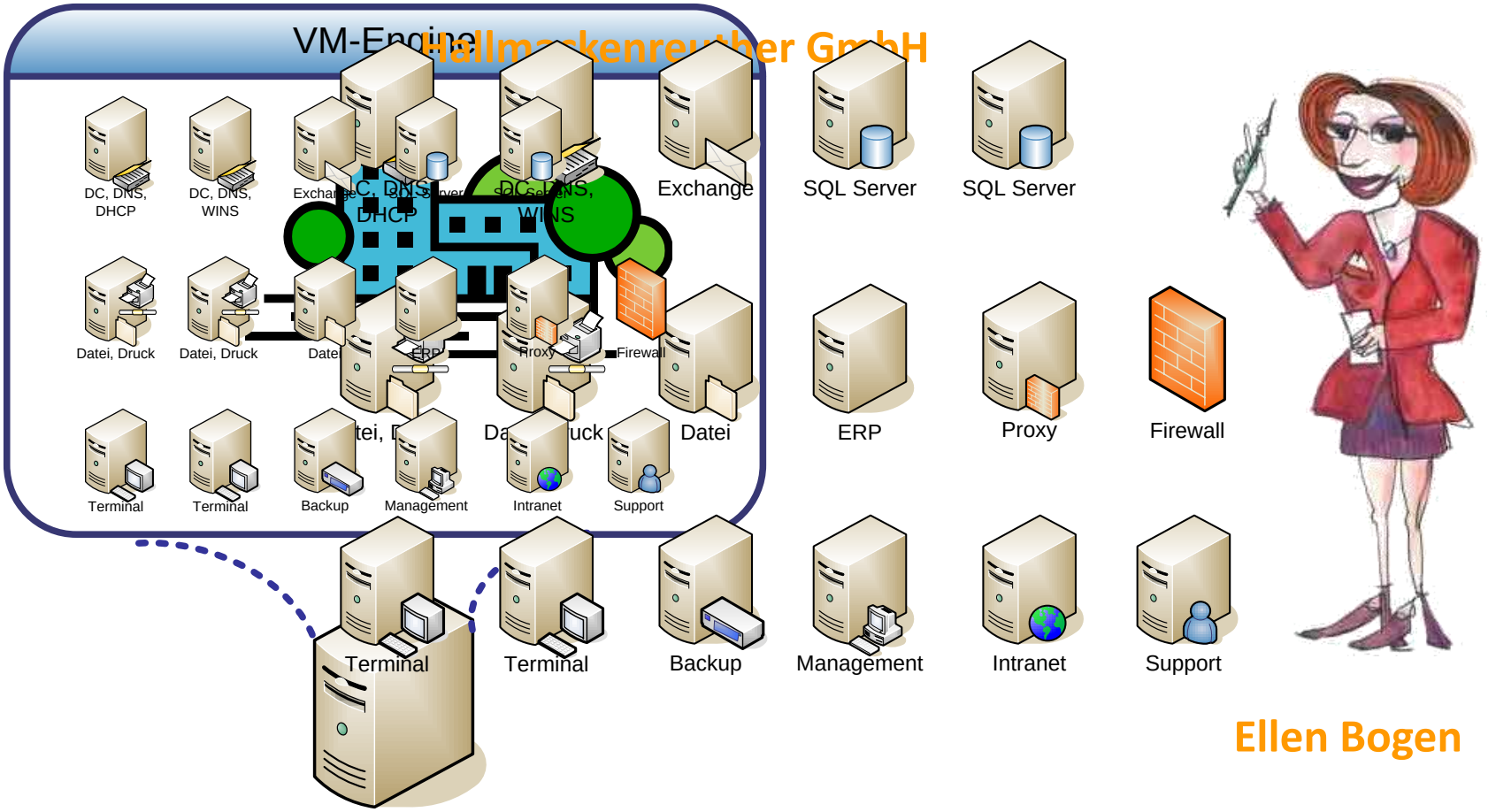
» Sicherheit in virtualisierten Umgebungen

Sandkästen, Klone und Mythen

» Nils Kaczenski
Leiter Consulting & Support, WITstor

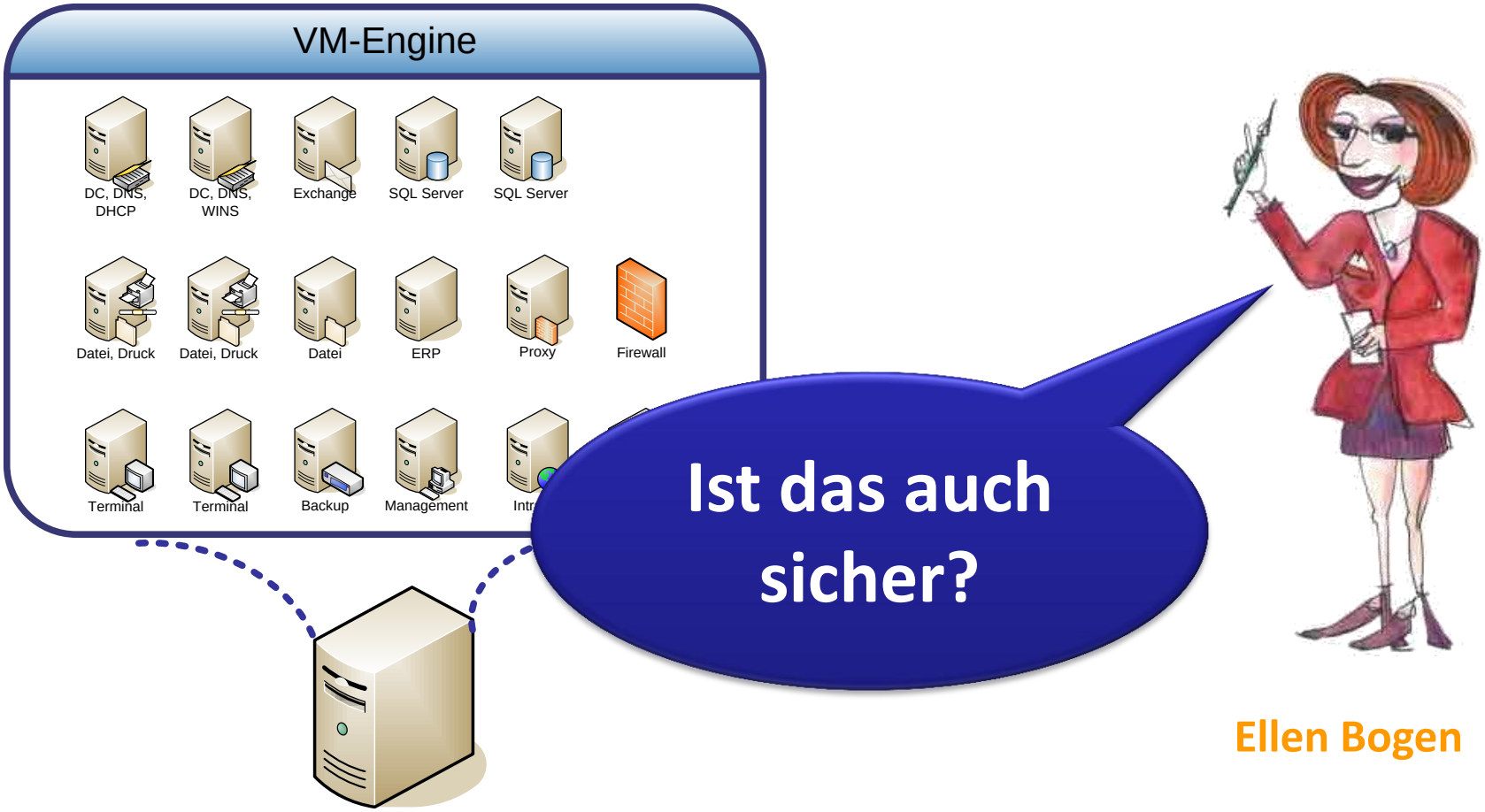
WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Frau Bogen virtualisiert.



WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Frau Bogen fragt sich:



WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Wer vor Ihnen steht

- **Nils Kaczenski**
- **Leiter Consulting & Support**
  WITstor Hannover
  - Strategische Beratung
  - Projektleitung
  - Windows, Exchange, SQL
  - Virtualisierung, Verfügbarkeit, Sicherheit
- **Fachautor Windows**
  - Microsoft Press
  - iX, c't, heise Security, heise Netze …
- **Nils.Kaczenski@witstor.de**

FAQ-O-MATIC.NET

MVP
Microsoft®
Most Valuable
Professional

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

WITstor: Systemlösungen. Service

Network & Applications

Windows
Active Directory
Exchange
Security
Switching/Routing
Firewall
WAN-Optimierung

Data Center

Storage
Server
Virtualisierung
Recovery
Verfügbarkeit

IT Services

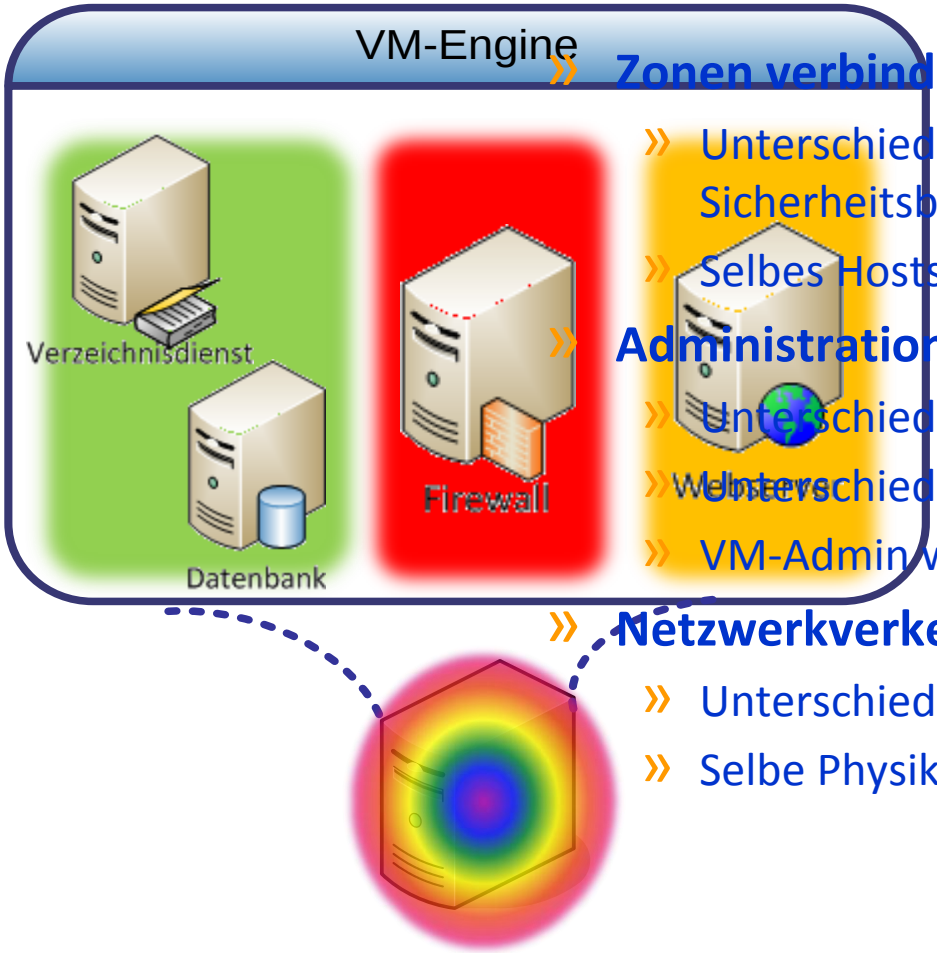
Rollout
Managed Services
Client Services
Helpdesk
Operating

NetApp Gold Partner
FUJITSU QUALIFIED PARTNER
vmware enterprise PARTNER
Cisco Systems
riverbed Think fast.
WatchGuard
CITRIX
Microsoft Partner Gold Server Platform
commvault GOLD PARTNER
hp invent
IBM Business Partner

Was Sie erwartet

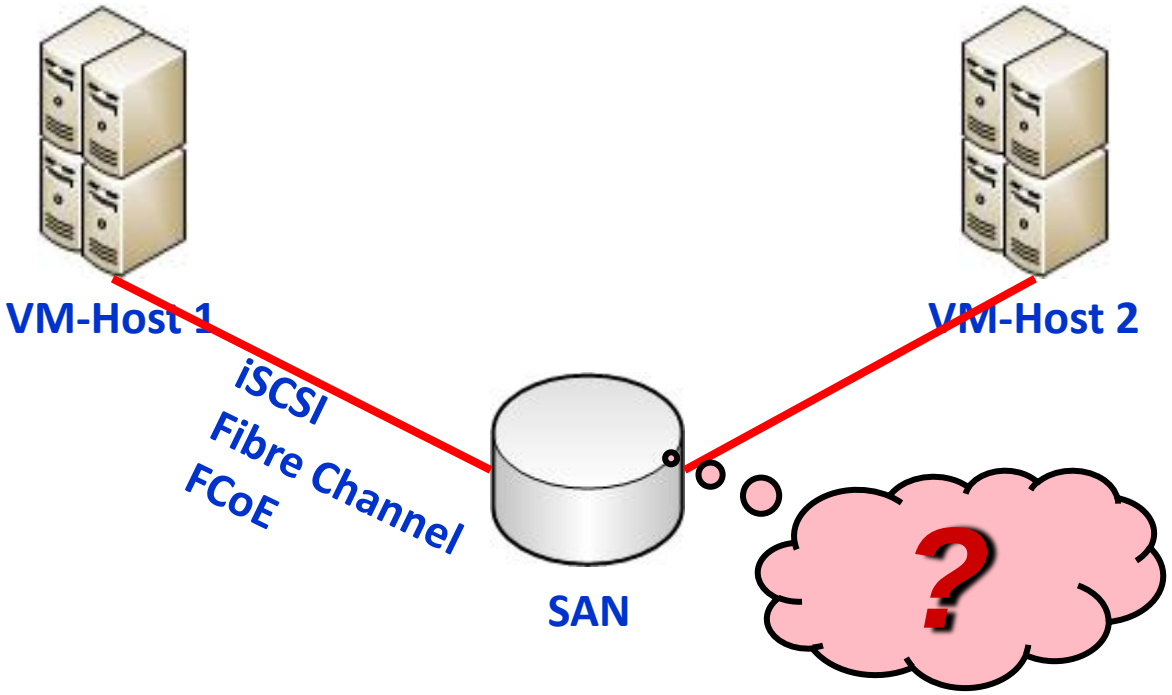
- Innen, außen und dazwischen: VMs und Netzwerke
- Sandkästen und Klone: VMs sind keine Spielplätze
- Mythen und Irrtümer: Katastrophe statt Rettung
- Virtuelle Systeme: Reale Gefahren

Kuschlig beieinander

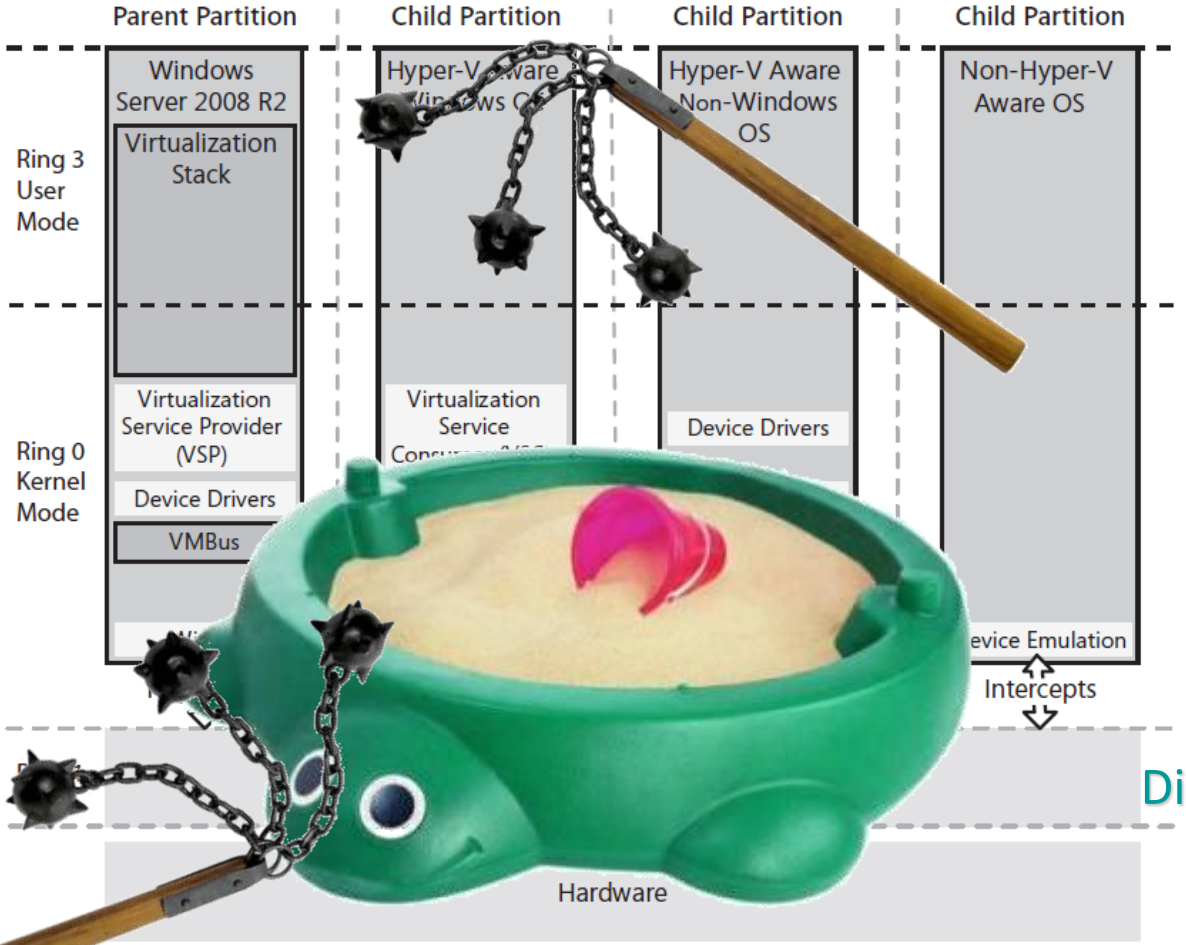


- **Zonen verbinden**
  - Unterschiedliche Sicherheitsbereiche
  - Selbes Hostsystem
- **Administration verbinden**
  - Unterschiedliche Admins
  - Unterschiedliche Richtlinien
  - VM-Admin wird Master-Admin
- **Netzwerkverkehr verbinden**
  - Unterschiedlicher Traffic
  - Selbe Physik

SAN: Steal All Network



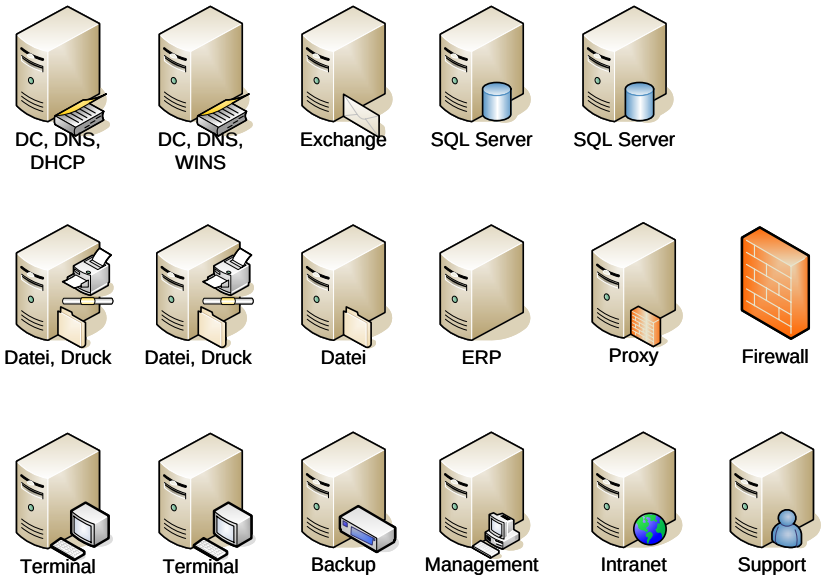
Die VM im sicheren Sandkasten

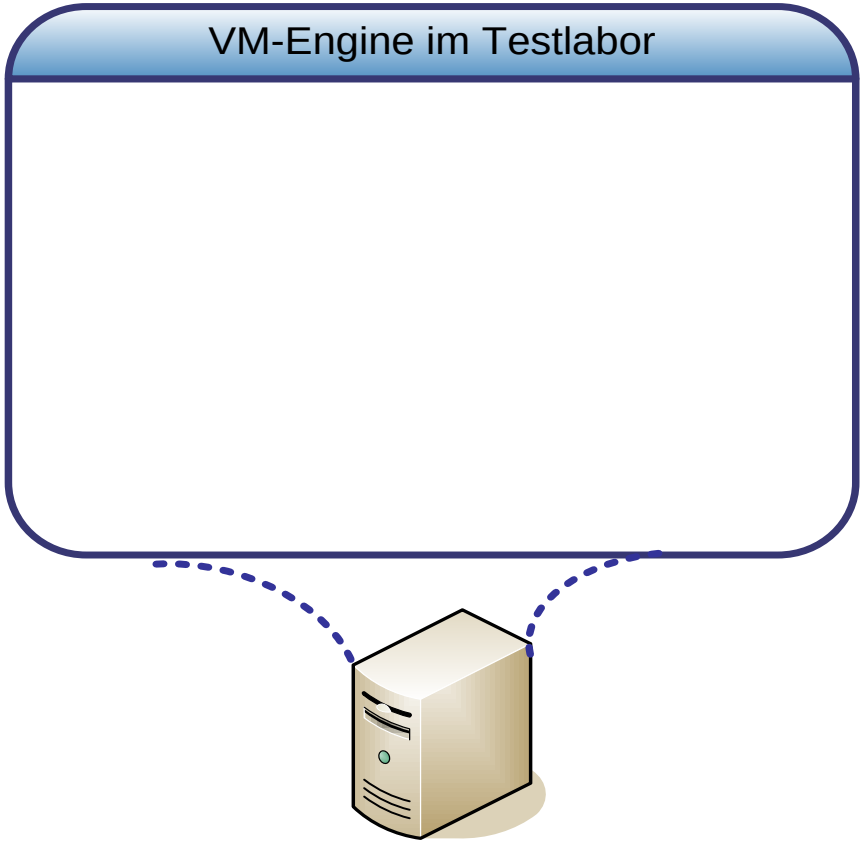


Dietrich Salpeter

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Sicherheitsloch auf Knopfdruck

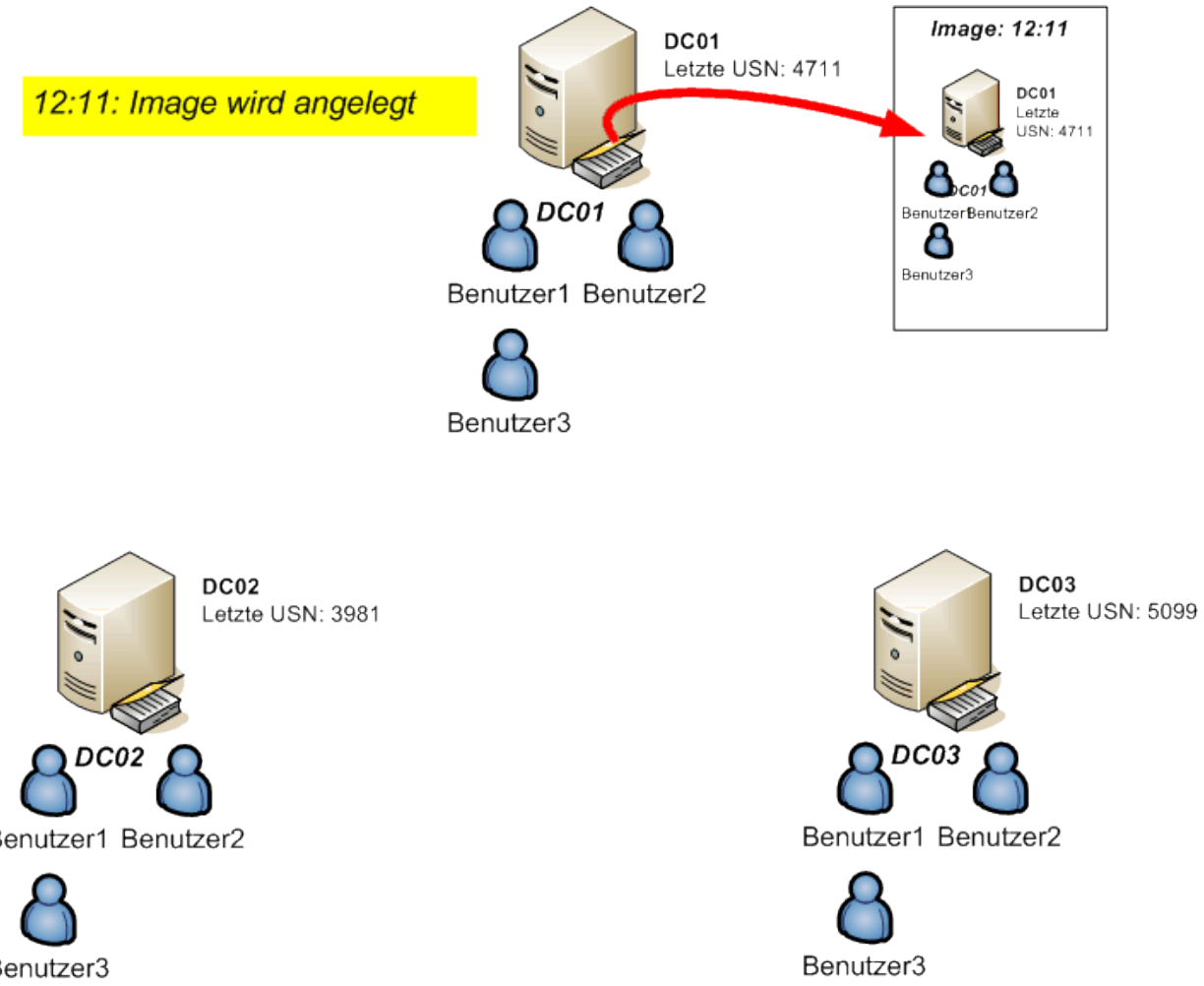




Mythen, Irrtümer und Irrwege

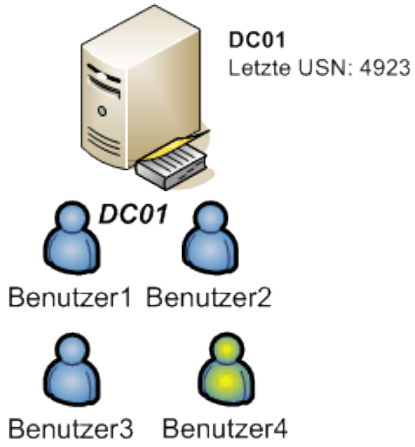
- **Live Migration (bzw. VMotion bzw. XenMotion)**
  - Vermeidet *geplante* Downtime – aber auch nicht jede
  - Dient zur dynamischen Lastverteilung
  - Hilft *nicht* bei Server-Ausfällen
- **Live-Spiegelung von Maschinen (Fault Tolerance, Marathon)**
  - VMware FT: Prinzipbedingt nur für eine CPU geeignet (bis vSphere 5)
  - High-End-Dienste scheiden damit aus
  - Hyper-V kann das (noch) nicht
- **Snapshots von VMs**
  - Frieren historischen Zustand ein
  - Zerstören Konsistenz bei komplexen Applikationen (z.B. Active Directory)

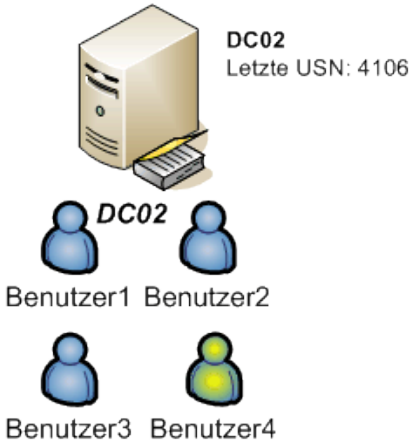
USN Rollback: Katastrophe statt Rettung

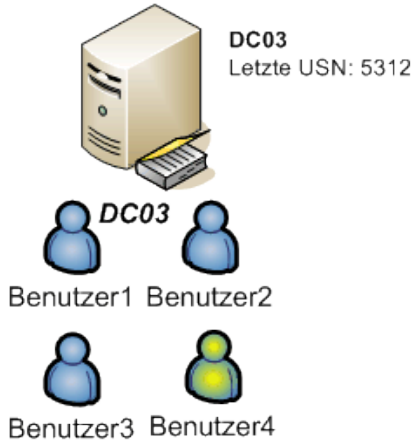


USN Rollback: Katastrophe statt Rettung

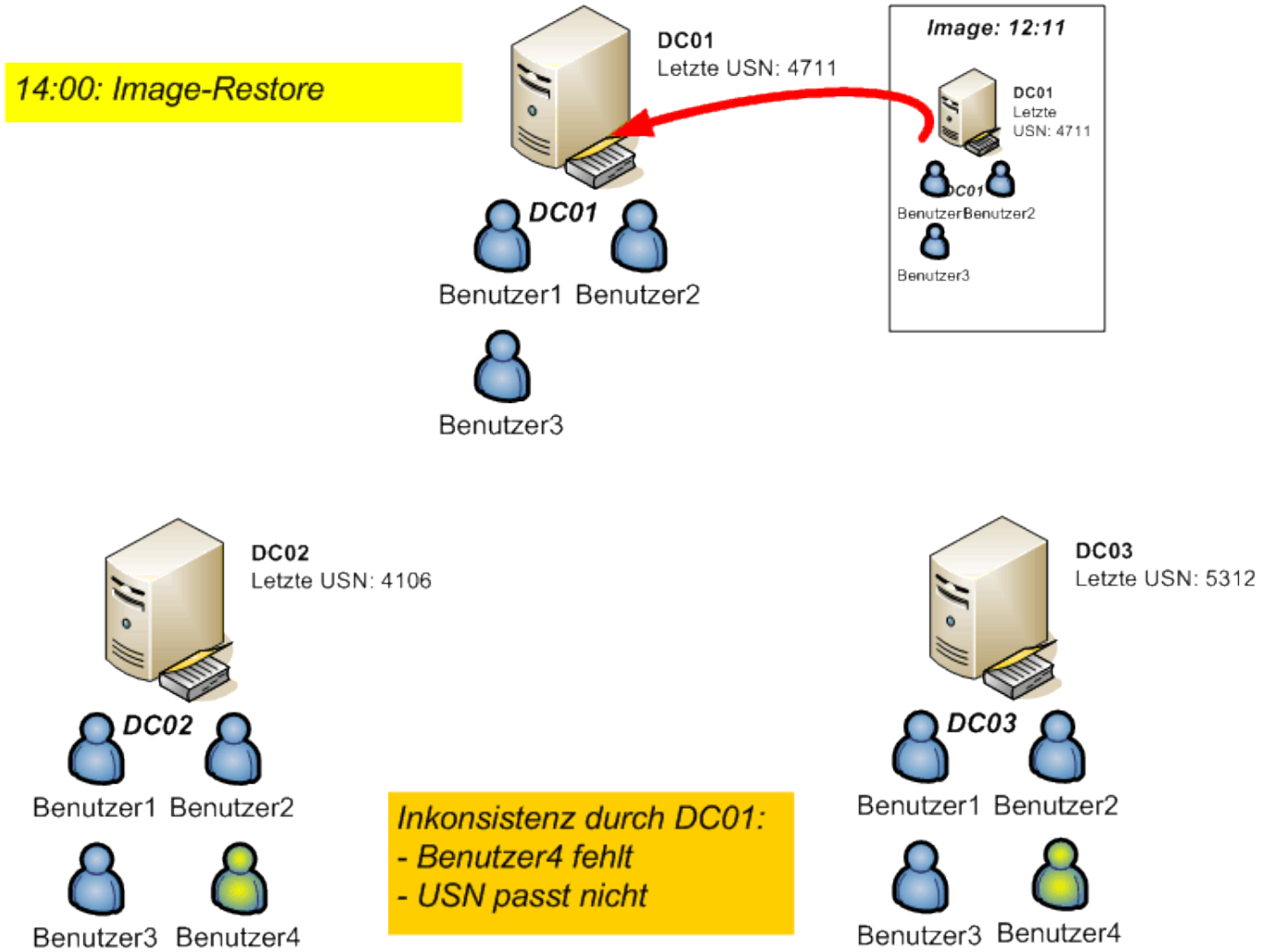
13:24: Neue Daten



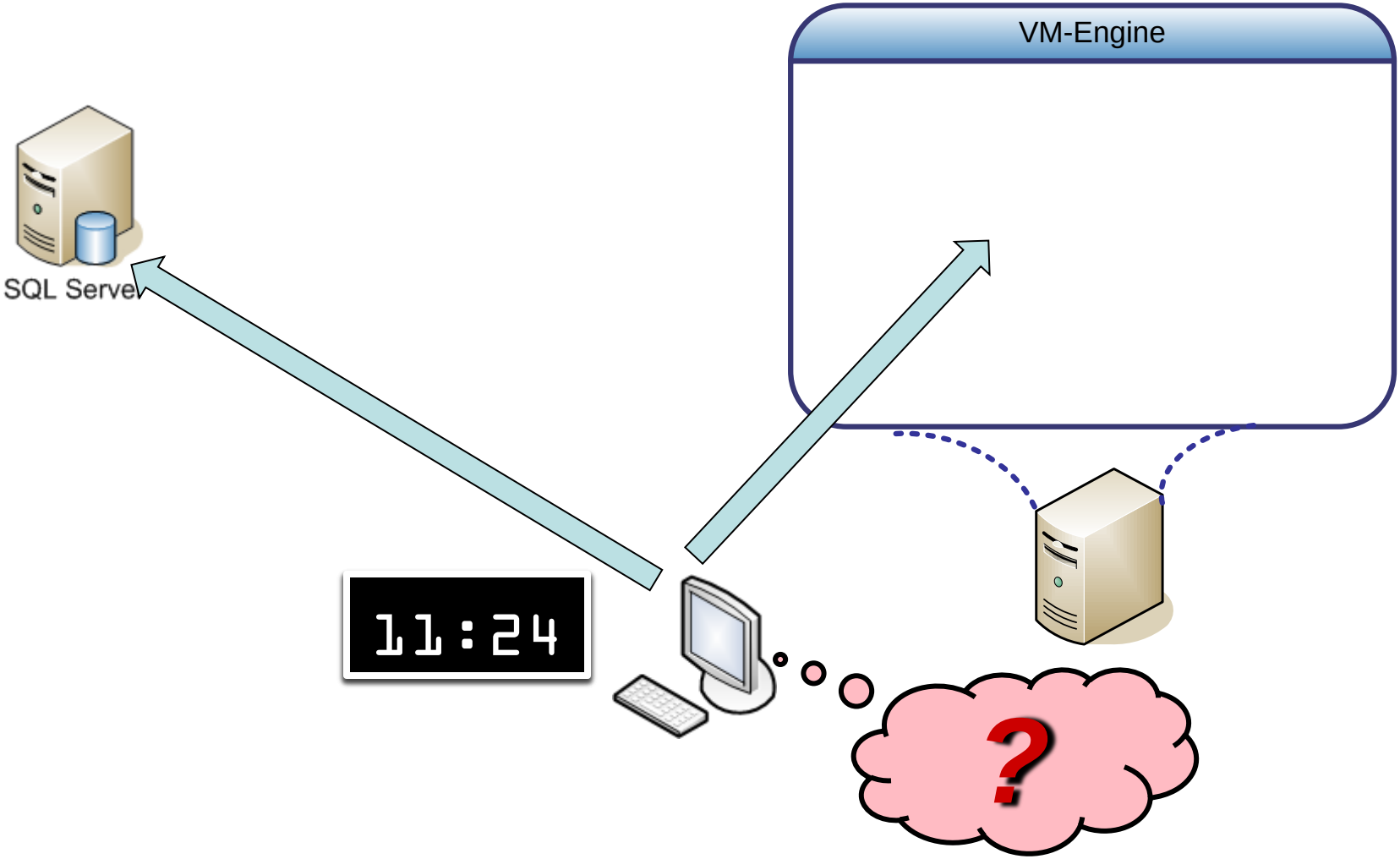




USN Rollback: Katastrophe statt Rettung



P2V: Alles andere als schmerzlos



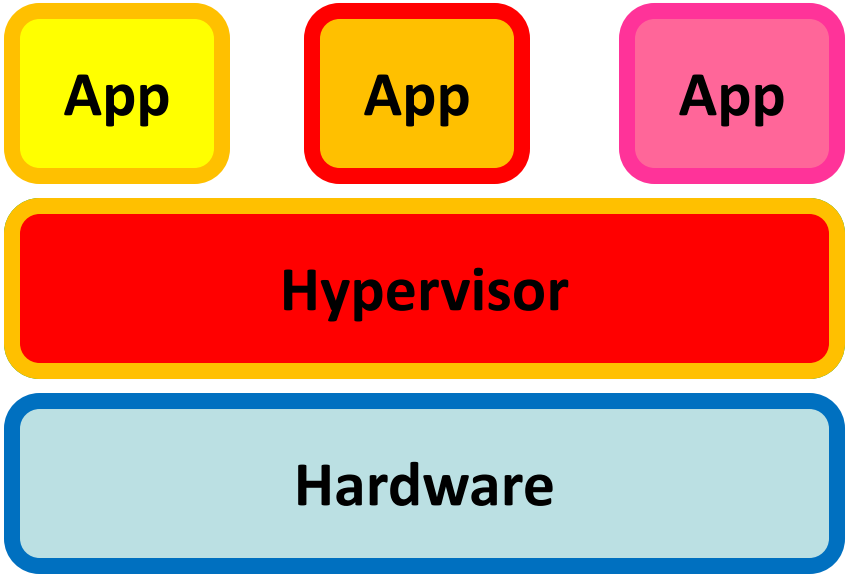
Virtuelle Systeme – reale Gefahren

- **Patch-Management**
  - Mehr, nicht weniger
  - Komplexe Host-Updates
- **Administrative Sünden**
  - Laxe Kennwortvergabe
  - Backups, die nicht zum Restore taugen
- **Unkontrollierte VM-Landschaften**
  - VM-Wucherung
  - Undefinierte Admins
  - Sorglose Ablage von VM-Images
  - Nicht angepasste Standardinstallationen

SubVirt und Blue Pill: Modell „Perfektes Verbrechen“

SubVirt

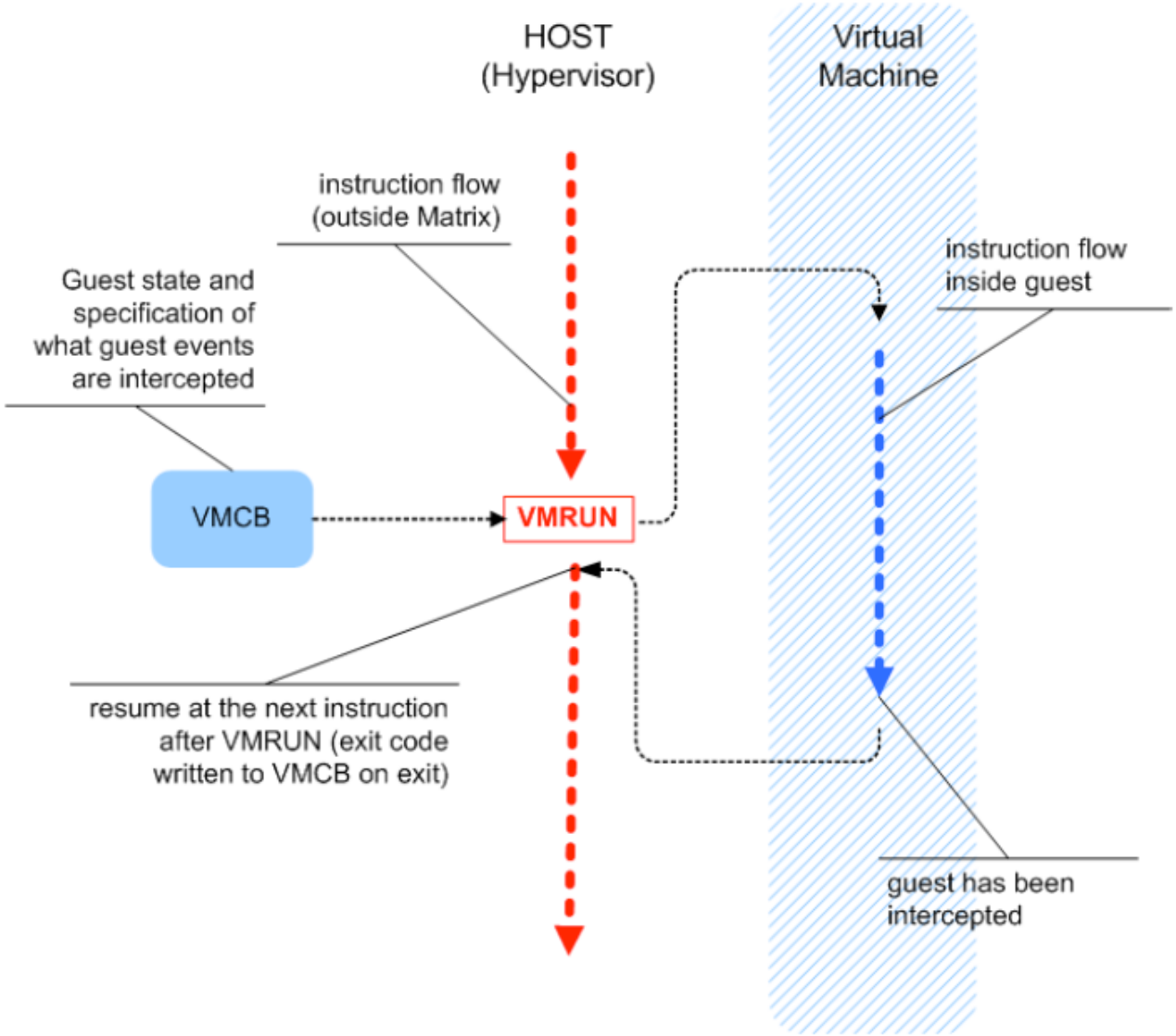
- Fest installiert
- Überlebt Reboot
- Nachweisbar
- PoC: Microsoft Research



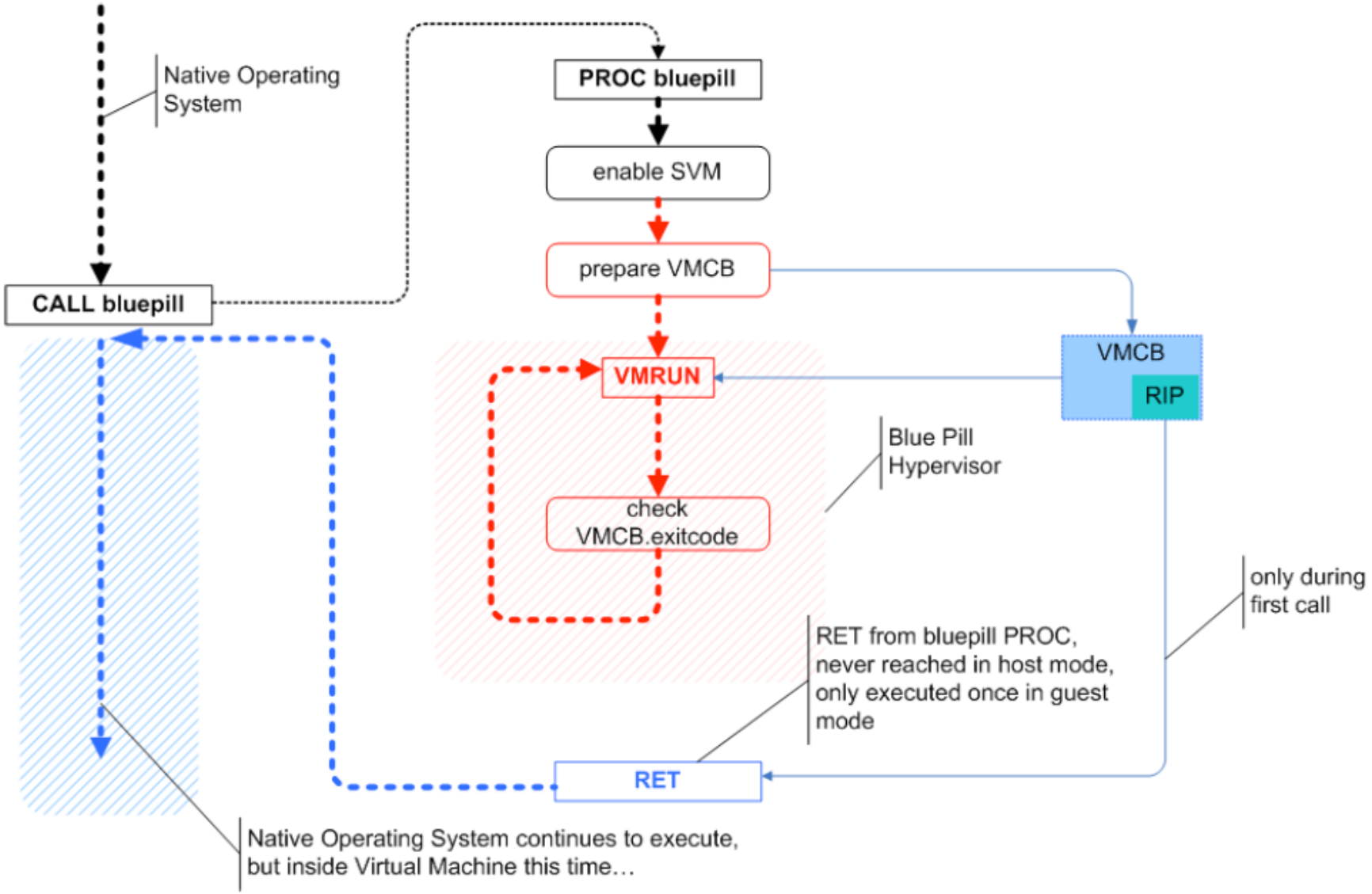
Blue Pill

- On-the-Fly
- Vermeidet Reboot
- Nicht nachweisbar
- PoC: Joanna Rutkowska

The heart of SVM: VMRUN instruction

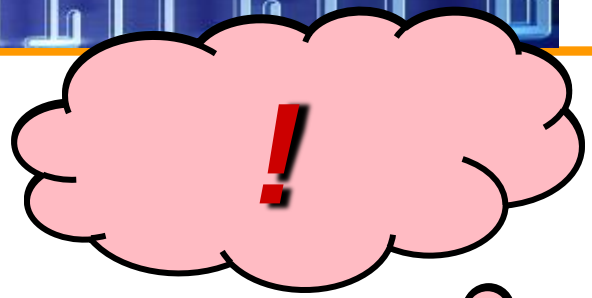


Blue Pill Idea (simplified)



WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Was Sie erwartet



- Innen, außen und dazwischen: VMs und Netzwerke
- Sandkästen und Klone: VMs sind keine Spielzeuge
- Mythen und Irrtümer: Katastrophe statt Realität
- Virtuelle Systeme: Reale Gefahren

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

Mehr …

» www.witstor.de

» Nils.Kaczenski@witstor.de

» twitter.com/WITstor