FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-Forensik in cloudbasierten Systemen

Martin Kuen

IT Forensik
FH Aachen

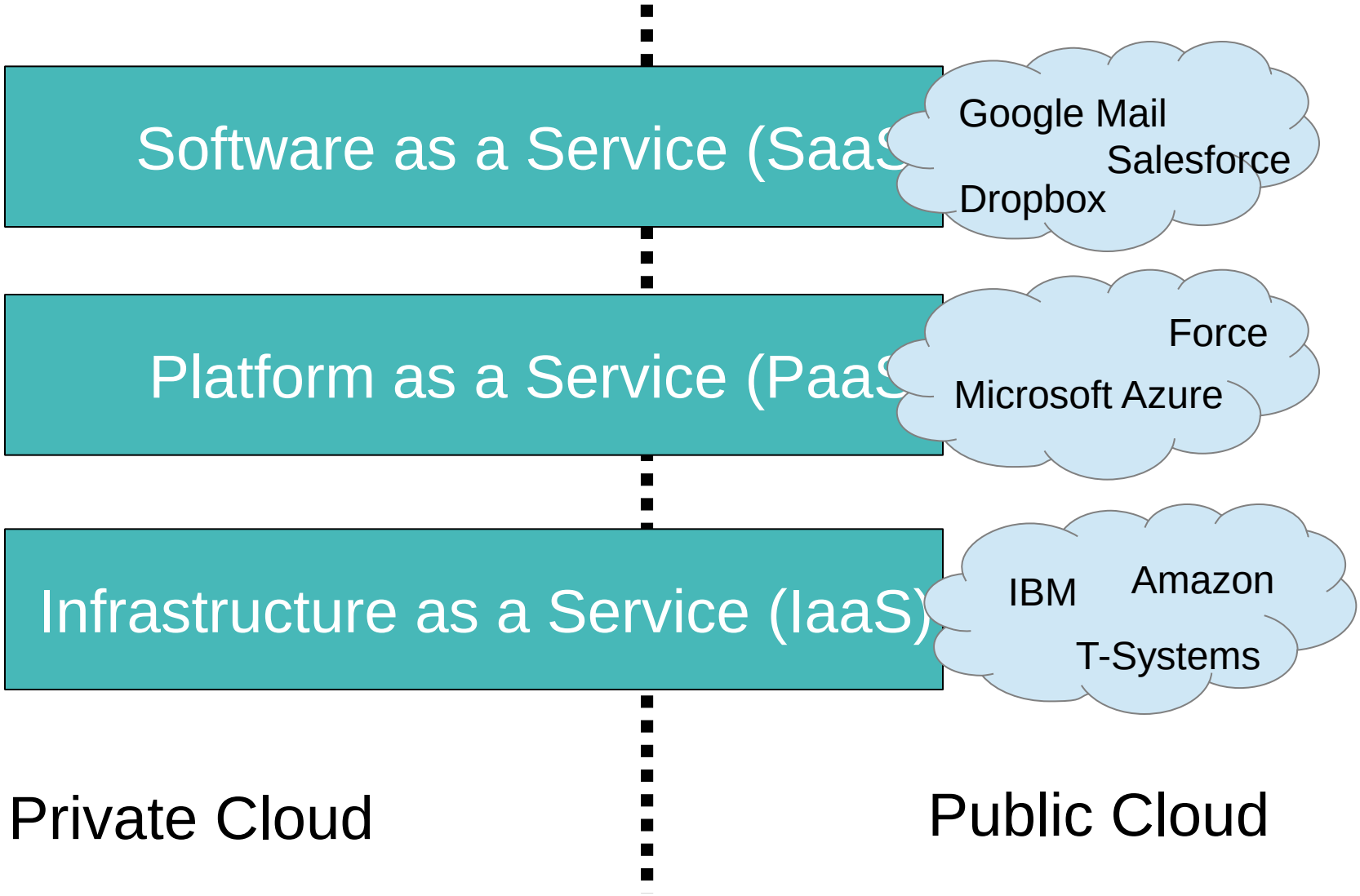
IT-Forensik in cloudbasierten Systemen

1. Cloud Computing
2. Probleme und Lösungen
3. Präventive Lösungen
4. Forensik mit der Cloud

Disclaimer

Betrachtet wird Cloudforensik aus der Sicht interner Ermittlungen in Unternehmen.

Cloud Computing



IT-Forensik in cloudbasierten Systemen

Probleme und Lösungen

IT Forensik
FH Aachen

Fehlender physikalischer Zugriff

- Technisches Problem:
  Kein direkter Zugriff auf Hardware möglich
- Forensisches Problem:
  Keine Imageerstellung möglich
- Lösung:
  Image des Cloud Service Providers (CSP)
  → Chain of custody erst ab Image des CSP

Mehrere Kunden pro Server

- Rechtliches Problem:
  Kein direkter Zugriff auf Hardware möglich
  aus Datenschutzgründen
- Forensisches Problem:
  Keine Imageerstellung möglich
- Lösung:
  Image der Virtuellen Maschine (VM)
  → Festplatten Image und RAM Image

Speicherort der Daten außerhalb der EU

- Rechtliches Problem:
  - Kein EU-Recht anwendbar
  - → Datenschutzprobleme, Gerichtsurteile schwer durchsetzbar
- Lösung:
  - Mit CSP geographischen Speicherort vereinbaren

Keine allgemeingültigen Standards

- Technisches Problem:
  Standard Software nicht einsetzbar
- Lösung:
  Bei jedem CSP individuelle Lösung erforderlich

Kein voller Systemzugriff (SaaS, PaaS)

- Technisches Problem:
  Kein Zugriff bis auf Kern der VM möglich
- Forensisches Problem:
  Keine Imageerstellung oder Datenabzug möglich
- Lösung:
  Tools des CSP verwenden
  Vereinbarungen im Vorfeld treffen

IT-Forensik in cloudbasierten Systemen

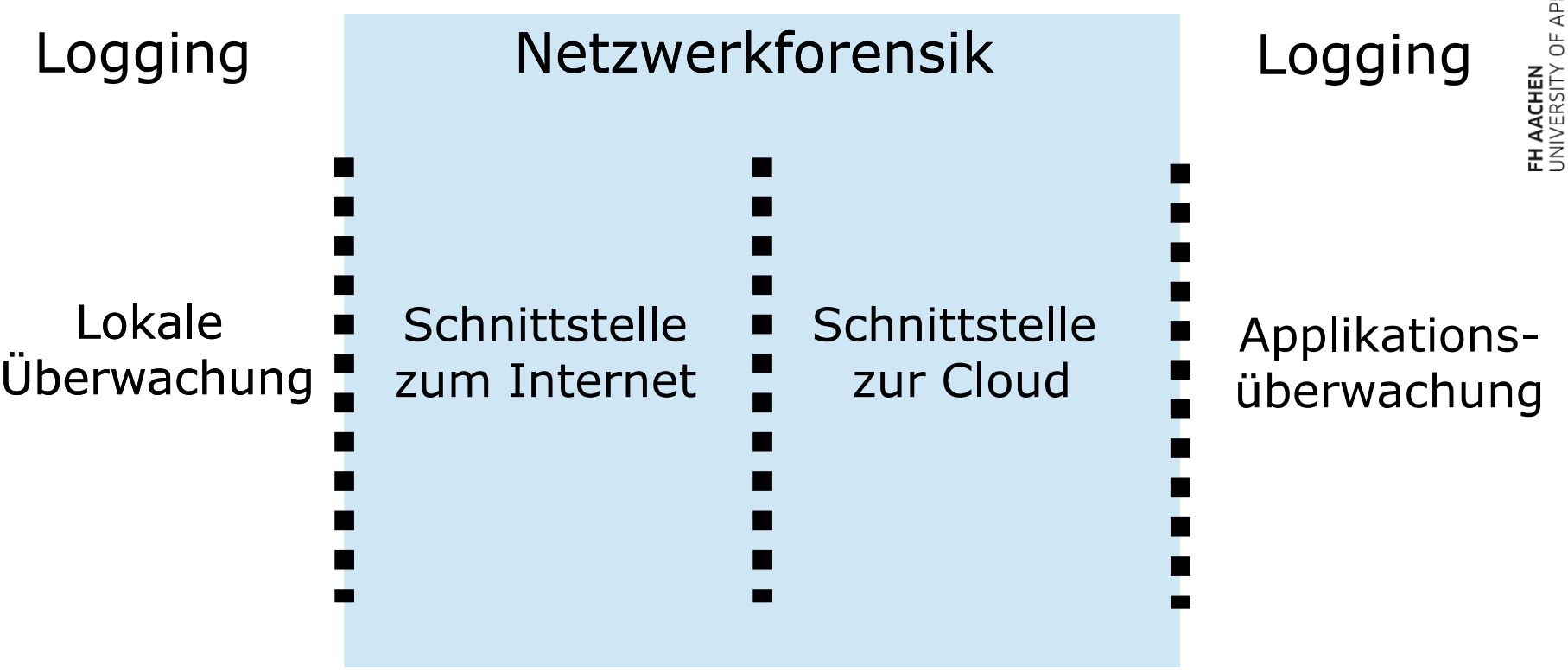
Präventive Lösungen

IT Forensik
FH Aachen

Service Level Agreements

- Datenzugriff gewährleisten
- Geographisch geeigneter Datenspeicherort
- Datenformat das zur Verfügung gestellt wird

Transaktionsüberwachung



Filelogger

- Schnittstelle zum Internet
- Daten die mit offenen Protokollen verschickt werden
- Logging
  - Zeit
  - User
  - Datei
  - Ziel
- C# Software

IT-Forensik in cloudbasierten Systemen

Forensik mit der Cloud

IT Forensik
FH Aachen

Forensik as a Service (FaaS)

- Forensische Dienste an Cloudanbieter auslagern
  - Passwörter knacken
  - Verschlüsselungen lösen
  - Datenanalysen
- Problem: Datenschutz

Forensik mit der Cloud

- Große Rechenkapazitäten
- Große Speicherkapazitäten
- Geringe Kosten
- Große Flexibilität

Vielen Dank für Ihre Aufmerksamkeit!

IT Forensik
FH Aachen