

# Messgeräte und die „Cloud“

Daniel Peters, Florian Thiel  
Fachbereich 8.5 Metrologische Informationstechnik



- Don't believe the hype! Bewertung neuer Technologien.
- Grundlagen
- Bedrohungen, Bewertungsverfahren, Sicherheitsstandards
- Beispiele im gesetzlichen Messwesen
- Nationale und europäische Aktivitäten

# Gartner Hype Cycle for Emerging Technologies

Figure 1. Hype Cycle for Emerging Technologies, 2013

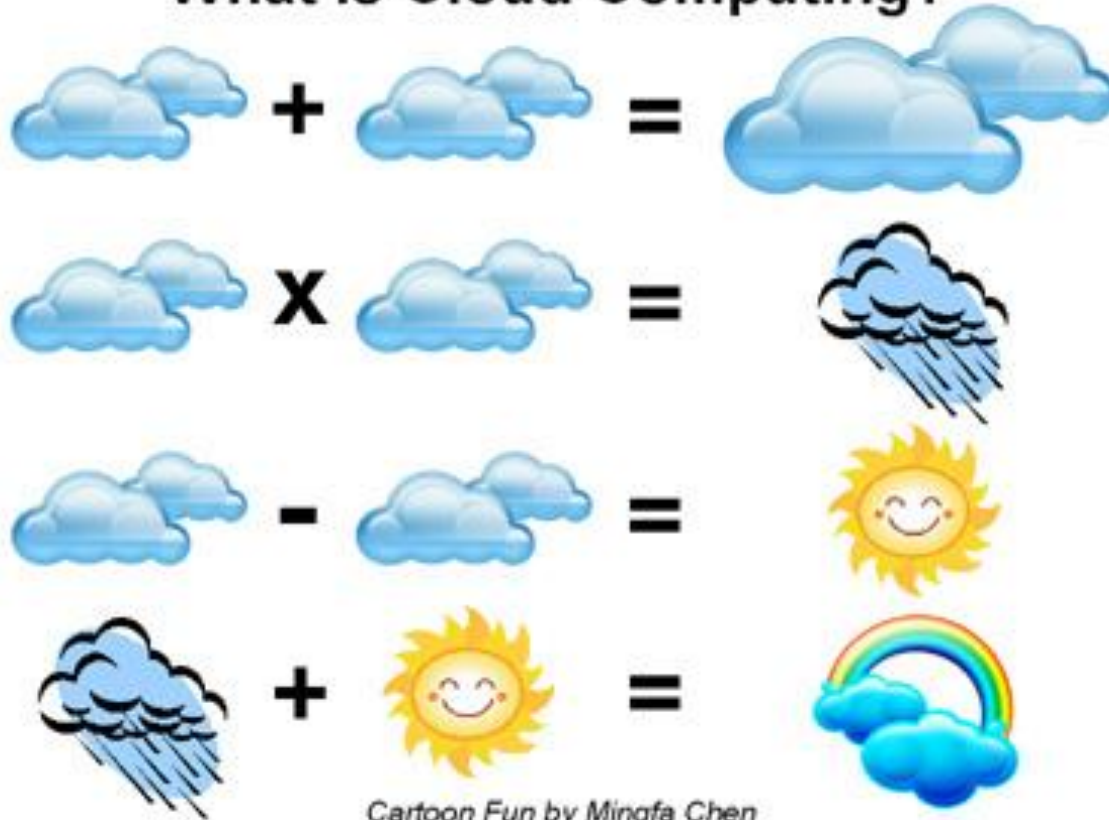


Cloud Computing steckt momentan fast am Tiefpunkt der Enttäuschungen.

In den kommenden zwei bis fünf Jahren werden Unternehmen realistischere Strategien für den Umgang mit der Cloud erarbeiten und diese auch umsetzen.

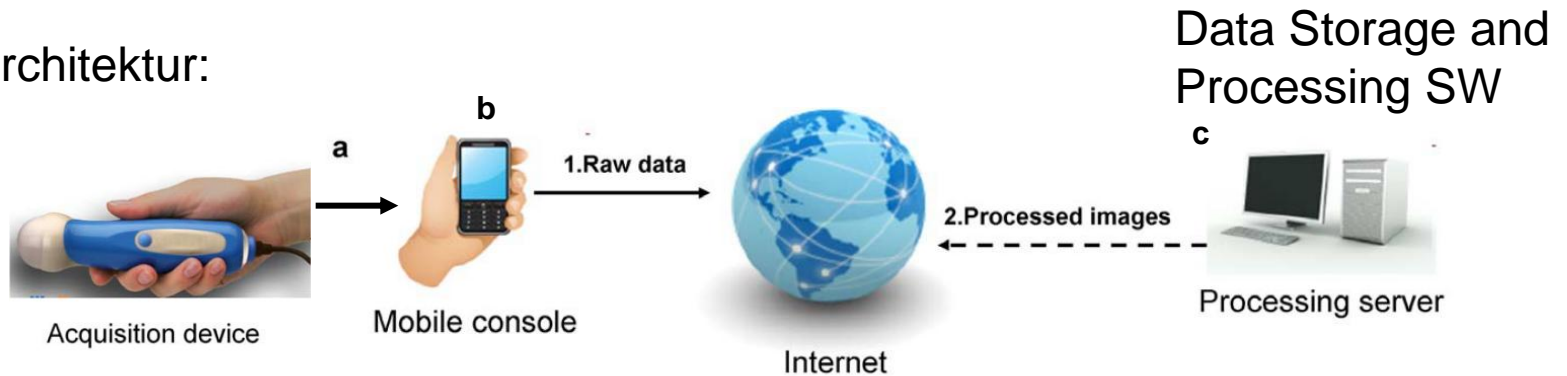
Source: Gartner (July 2013)

## What is Cloud Computing?

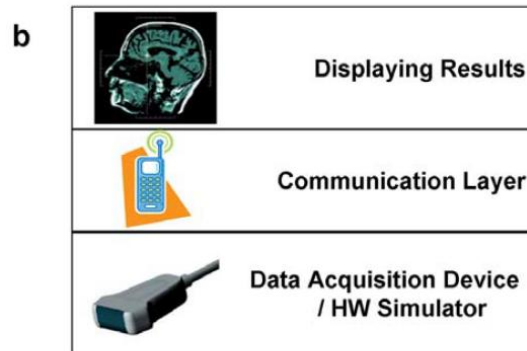


# Ein Beispiel aus der “Medizinischen Metrologie”:

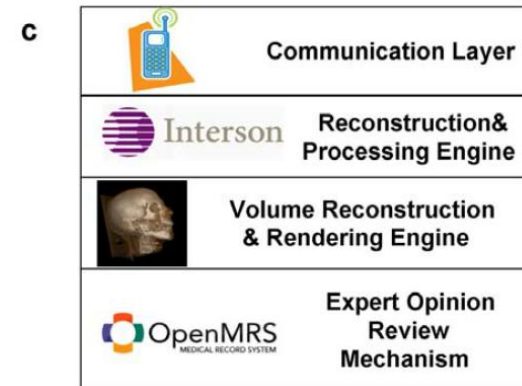
## Systemarchitektur:



## Mobile Console Architecture



## Server Architecture



**Figure 1. System Architecture.** (a) Overall system architecture includes the mobile console component and the remote processing server (Expert System) which performs the computation-extensive work. (b) Mobile Console Architecture. The console has one or more data acquisition devices, a communication module and a display capability. (c) Server Architecture. Contains a communication module, a processing engine, a visualization engine and an expert assessment mechanism.

# Grundlagen

Cloud Computing is the result of **evolution and adoption of existing technologies and paradigms**.

The goal of cloud computing is to allow users to take benefit from all of these technologies, **without the need for deep knowledge** about or expertise with each one of them.

The cloud aims to cut costs, and help the users **focus on their core business** instead of being impeded by IT obstacles.

HAMDAQA, Mohammad (2012). [Cloud Computing Uncovered: A Research Landscape](#). Elsevier Press. pp. 41–85. [ISBN 0-12-396535-7](#).



# Grundlagen: Die NIST-Definition

Definition des NIST (National Institute of Standards and Technology):

„Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und Überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider Interaktion zur Verfügung gestellt werden können.“



# Grundlagen: Die NIST-Definition, Charakteristiken

## 1. On-demand-Self-Service:

Die Provisionierung der Ressourcen (z. B. Rechenleistung, Speicher, etc.) läuft automatisch ohne Interaktion mit dem Service Provider ab. Der Kunde passt seinen Bedarf selbstständig an.

## 2. Broad Network Access:

Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an eine bestimmte Client-Architektur gebunden (z.B. Handy, Tablet, Laptop, oder Workstation) .

## 3. Resource Pooling:

Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können. Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z.B. Region, Land oder Rechenzentrum, festlegen.

## 4. Rapid Elasticity:

Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch.

## 5. Measured service:

Cloud Systeme kontrollieren die genutzten Ressourcen automatisch (z.B. storage, processing, bandwidth, and active user accounts). Die genutzten Ressourcen können angezeigt, kontrolliert und aufgelistet werden. Das unterstützt die Transparenz für Provider und Konsument.

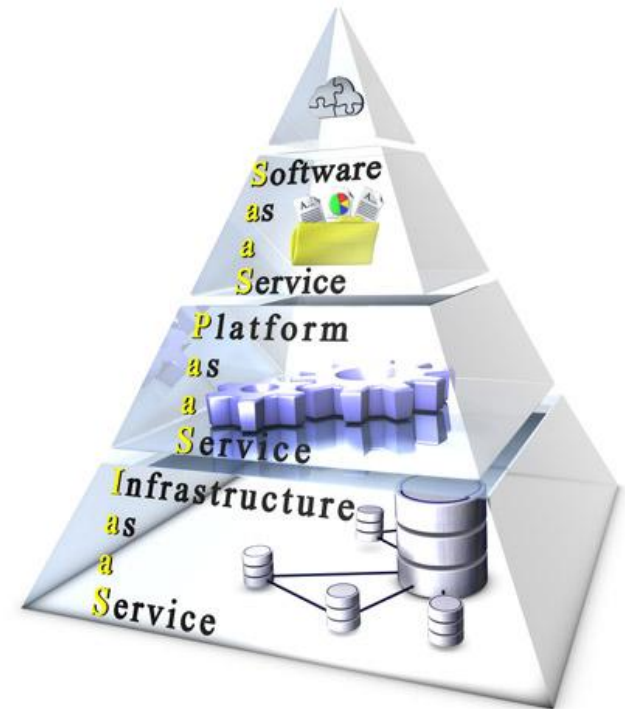
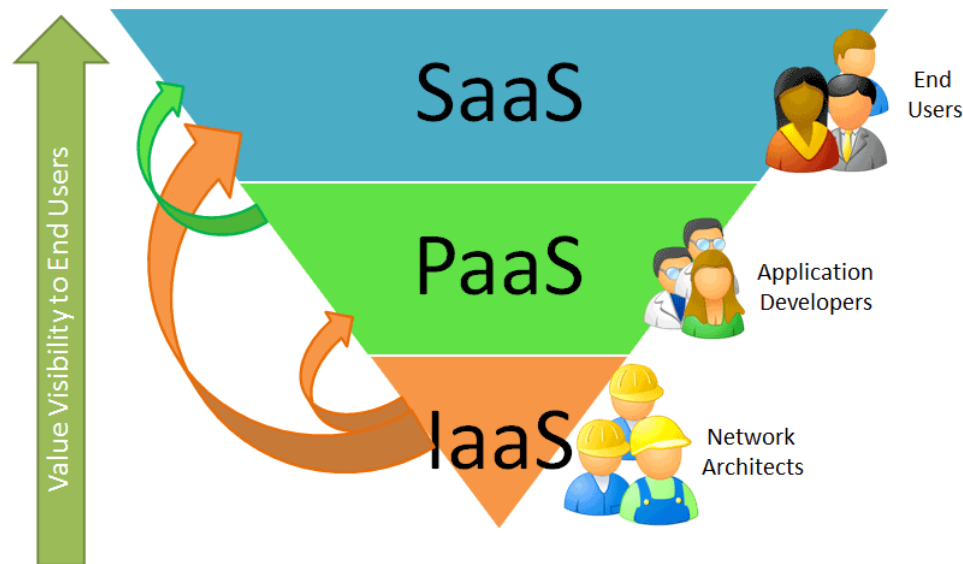
## 6. Auditability and certifiability:

Die Erfüllung von regulatorischen Anforderungen erfordert deren Durchsetzung. Die Services sollten die Nachverfolgung der "policies" erlauben ("logs" und "trails"), zur Sicherstellung, dass diese auch korrekt durchgesetzt/umgesetzt werden.

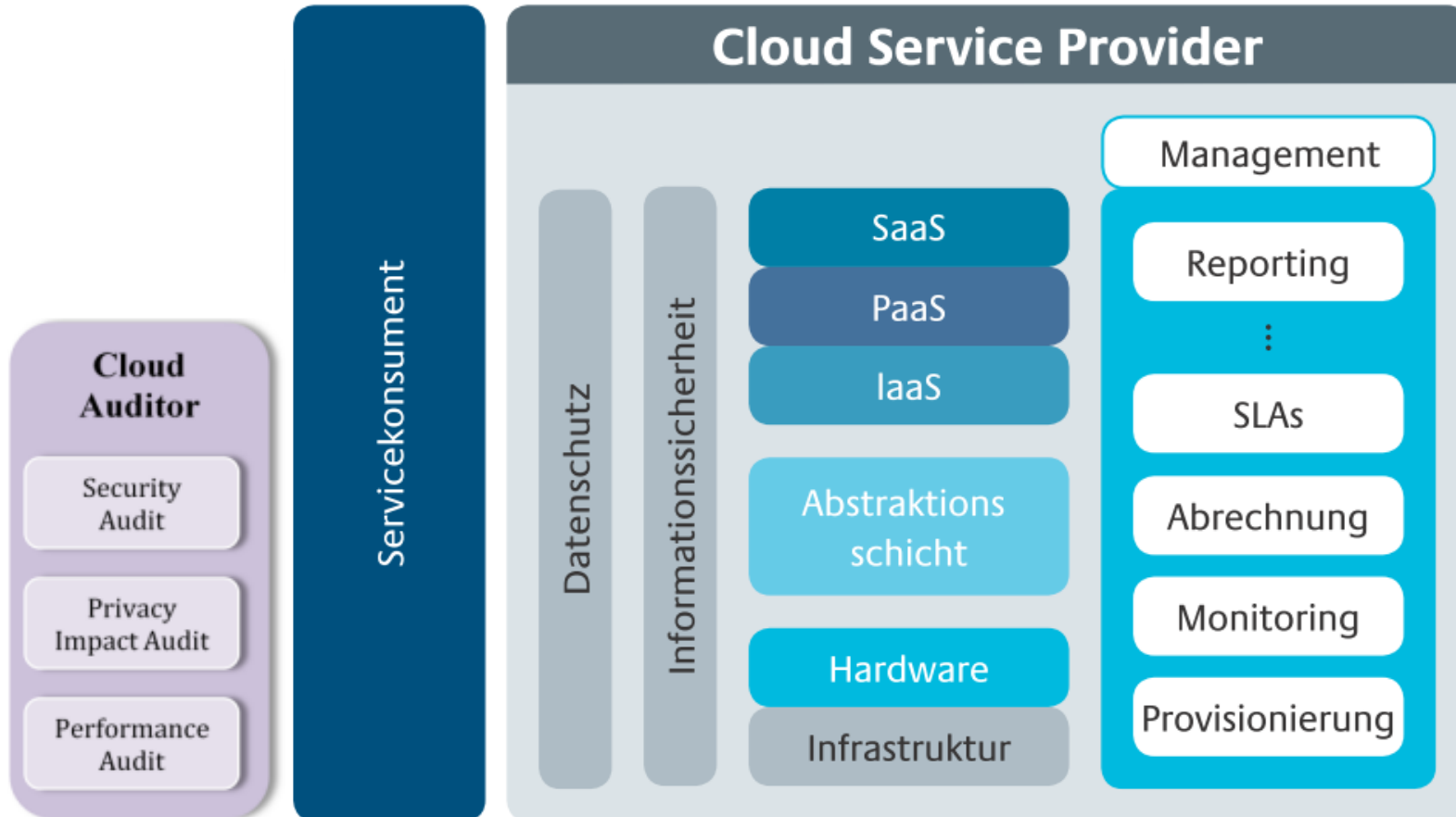


# Reference Architecture: Service Layers

- Infrastructure as a Service (IaaS): basic O/S, hardware,
- Platform as a Service (PaaS): IaaS + development environment
- Software as a Service (SaaS): complete application



# NIST Referenzarchitektur für Cloud Computing Plattformen



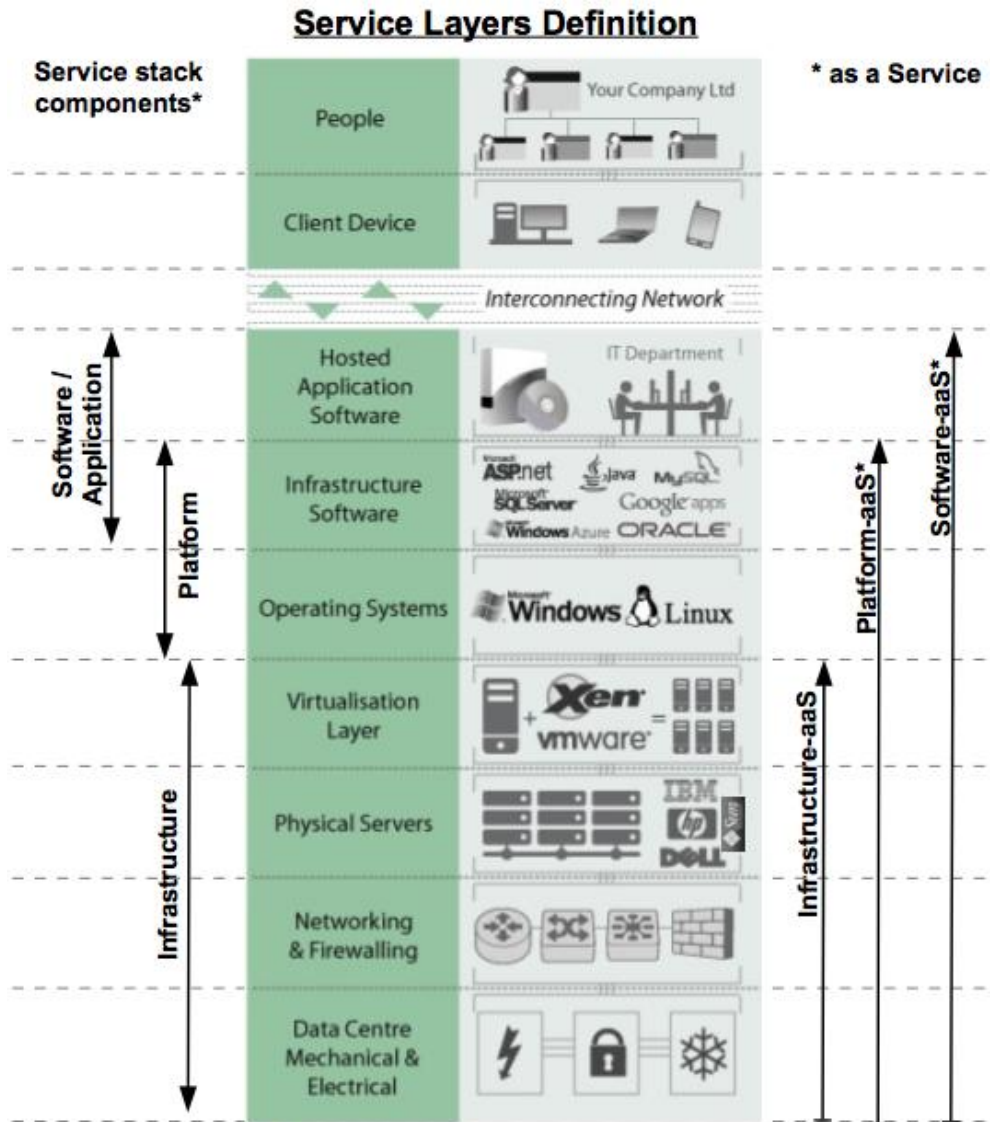
Genutzt von: IBM, u.a.

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Special Publication 509-292

**NIST Cloud Computing  
Reference Architecture**

# Reference Architecture: Service Layers



# Reference Architecture: Deployment Models

	Type	Properties
1.	Private cloud	<ul style="list-style-type: none"><li>• Outsource or own</li><li>• Lease or buy</li><li>• Separate or virtual data center</li></ul>
2.	Community cloud	<ul style="list-style-type: none"><li>• Private cloud for a set of users with specific demands</li><li>• Several stakeholders</li></ul>
3.	Public cloud	<ul style="list-style-type: none"><li>• Mega scaleable infrastructure</li><li>• Available for all</li></ul>
4.	Hybrid cloud	<ul style="list-style-type: none"><li>• Combination of two clouds</li><li>• Usually private for sensitive data and strategic applications</li></ul>

Tendenz bei industrieller Nutzung der „Cloud“: Private Cloud „Do-it-yourself!“

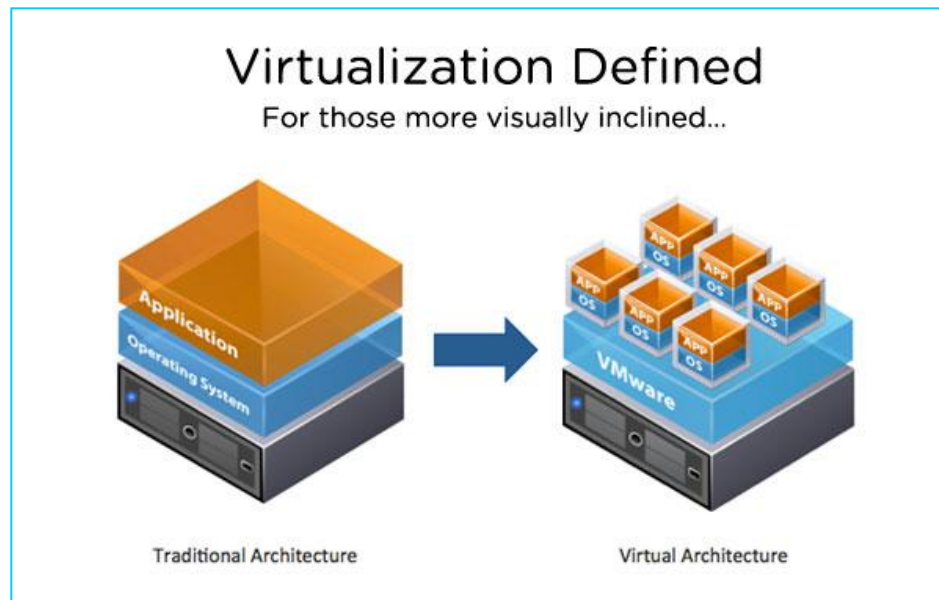
# Grundlagen: Virtualisierung

The main enabling technology for cloud computing is **virtualization**

Virtualization abstracts the physical infrastructure and makes it available as a soft component that is easy to use and manage.

Virtualization provides the agility required to

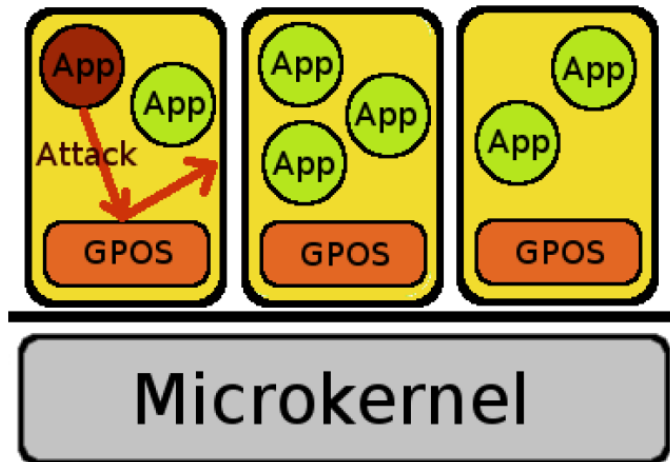
- speed up IT operations,
- and reduces cost by increasing infrastructure utilization.
- automates the process through which the user can provision resources on-demand.
- By minimizing user involvement, automation speeds up the process and reduces the possibility of human errors.



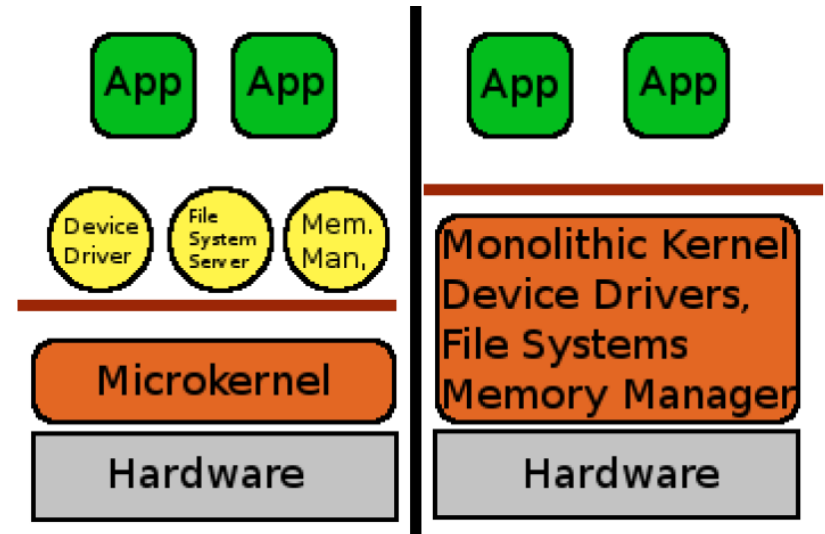
[www.vmware.com](http://www.vmware.com)

# Grundlagen: Virtualisierung

Left VM's general-purpose operating system (GPOS) is compromised by a pernicious application.  
Due to isolation the other VMs are not vulnerable



Comparison between a microkernel (left) and a monolithic kernel design (right)



Quelle: D. Peters, U. Grottker, F. Thiel, M. Peters, J.-P. Seifert,  
*Achieving Software Security for Measuring Instruments under Legal Control*,  
Federated Conference on Computer Science and Information Systems (FedCSIS),  
Emerging Aspects in Information Security (EAIS'14), accepted, (2014)

Separations - Kerne: EAL4 and higher (> Windows)

**Kooperation** mit TU Berlin, **Security in Telecommunications (SecT)**,  
**An-Institut Telekom Innovation Laboratories (T-Labs)**,



Telekom Innovation Laboratories



**Threat #1: Abuse and Nefarious Use of Cloud Computing**

Example: Botnets have used IaaS Servers

**Threat #2: Insecure Interfaces and APIs**

Example: authentication, access control, encryption, activity monitoring

**Threat #3: Malicious Insiders**

Example: Administrator

**Threat #4: Shared Technology Issues**

Example: unauthorized access to data of other cloud customers

**Threat #5: Data Loss or Leakage**

**Threat #6: Account or Service Hijacking**

**Threat #7: Unknown Risk Profile**

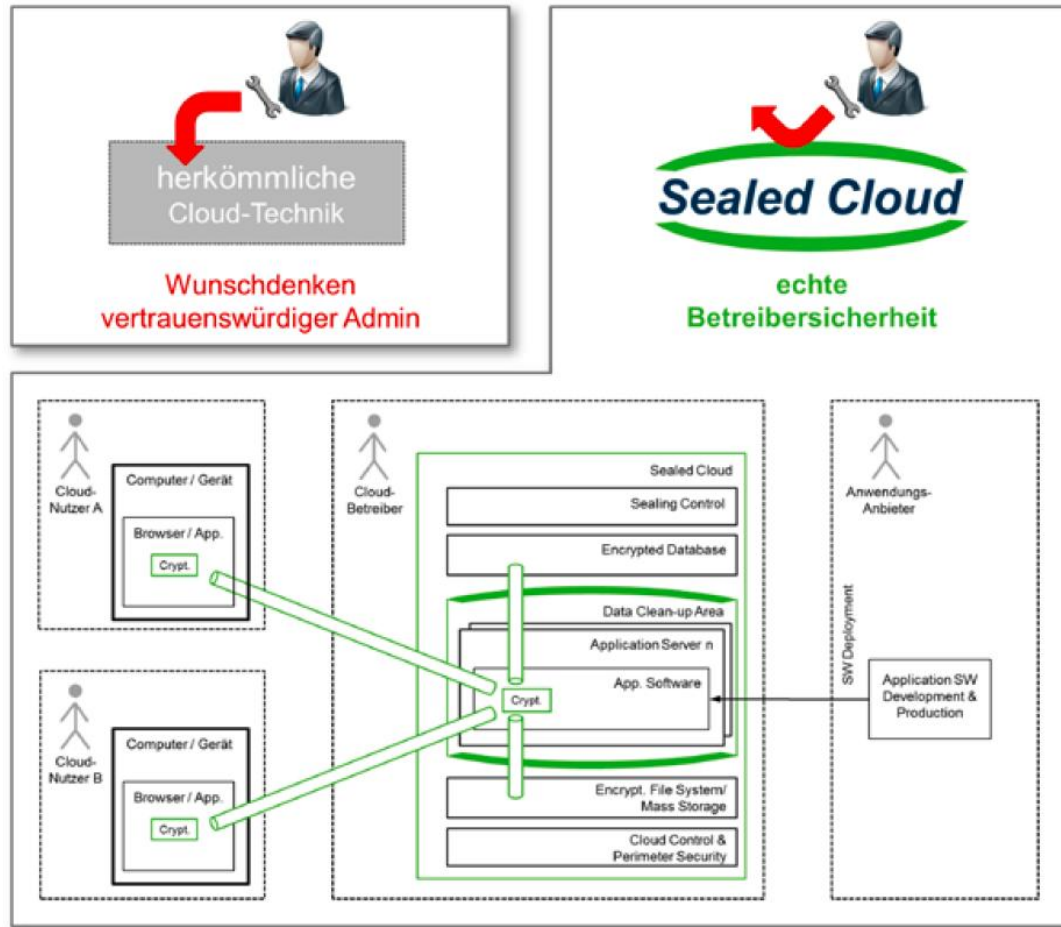
Example: Customer does not have all information of, e.g. internal security procedure.



# Zugriff des Administrators? (Malicious Insiders)

Ausschluss des Zugriffs des Betreibers der „Cloud“:

Sealed cloud, <http://www.uniscon.de/sealedcloud/>

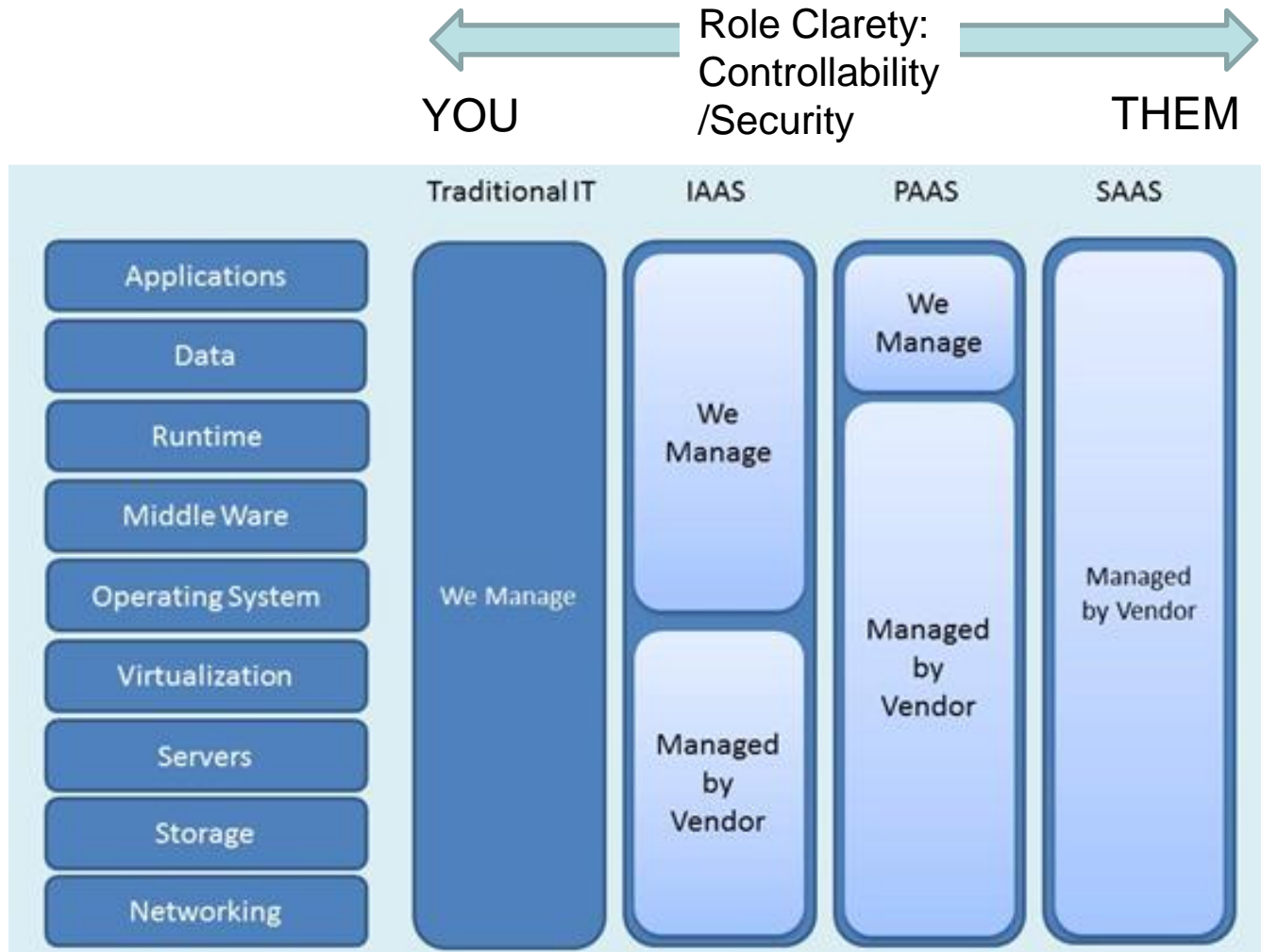


## Zielsetzung

- Die versiegelte Cloud-Infrastruktur unterbindet unbefugten Zugriff auf alle Daten des Cloud-Anwenders
- Auch der Cloud-Anbieter bzw. dessen Mitarbeiter können nicht auf die Daten zugreifen
- Neben den Inhalten der Kommunikation sind auch die Metadaten geschützt

Herausforderung bekannt!

# Verantwortung für Sicherheit, Privacy, Service



Welche Sicherheitsempfehlungen gibt es?

## BSI-Empfehlung für externe Cloud Nutzung:



White Paper

**Security Recommendations  
for Cloud Computing Providers**

### Vertragsgestaltung

Notfallmanagement  
(BS 25999, BSI-Standard 100-4)

IT-Sicherheit (Privacy, Security)  
ISO/IEC 27001/2 auf Basis  
BSI-IT Grundschutz

### Anforderungen:

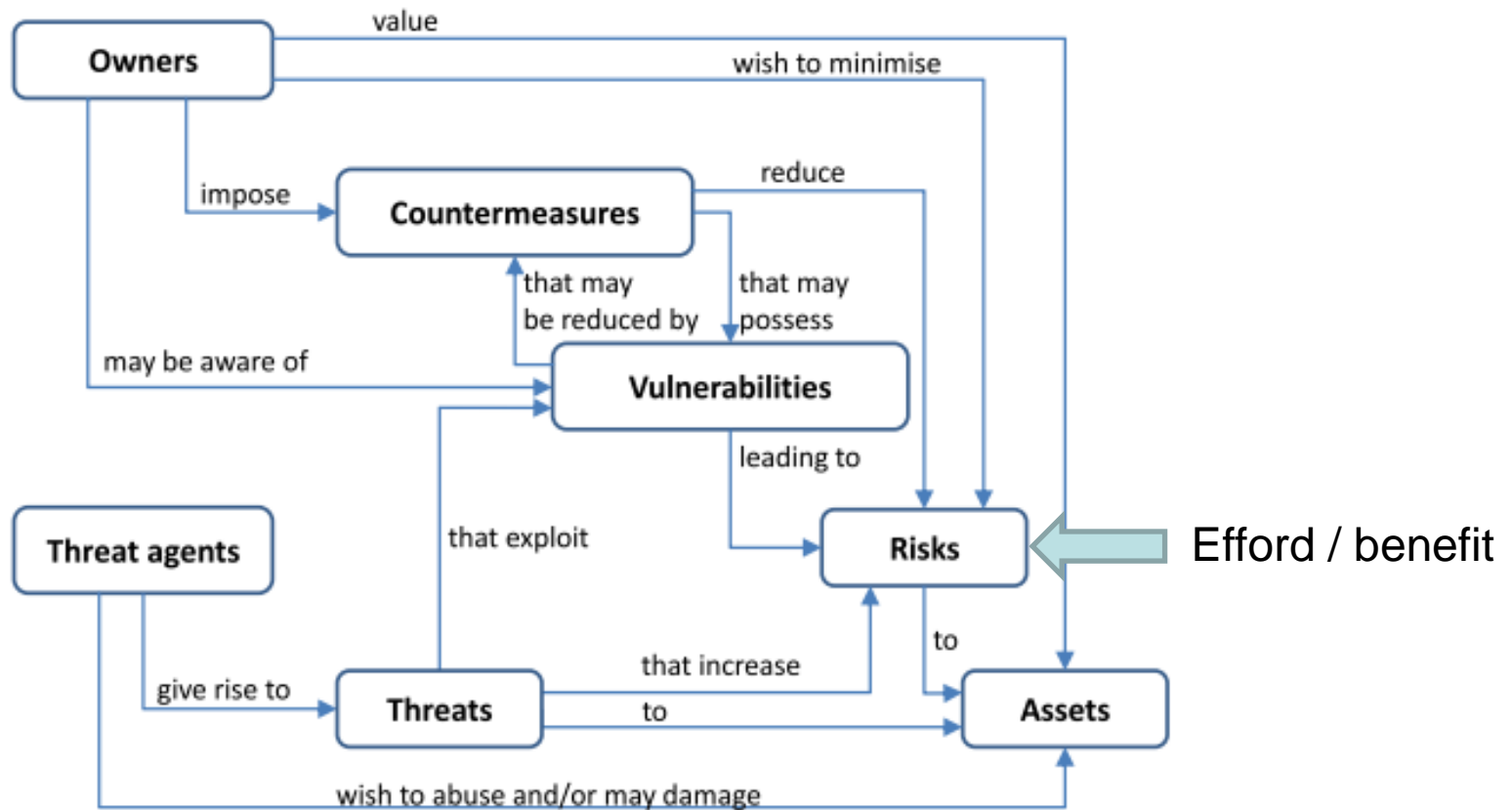
- Wer hat die Kontrolle über die Daten?
  - Auf welchem Server gespeichert?
  - Datentransfer läuft über welche Wege?
  - Wer kann lesen/schreiben?
  - Hohe Verfügbarkeit: 99,95% = ~4h/a Ausfall
- Maßnahmen gegen Datenverlust.
- Sicherheitsanforderungen (Security / Privacy)

Einzufordernde Standards:

- Informationssicherheit-Management-System (ISMS ISO/IEC 27001/2)
- Sicherheitsevaluierung (ISO/IEC 15408, Common Criteria):  
Server mind. EAL4 (SMGW EAL4+)

# ISO 15408:2005 (Common Criteria)

The elements of a risk and their relationships according to ISO 15408:2005 (Common Criteria)

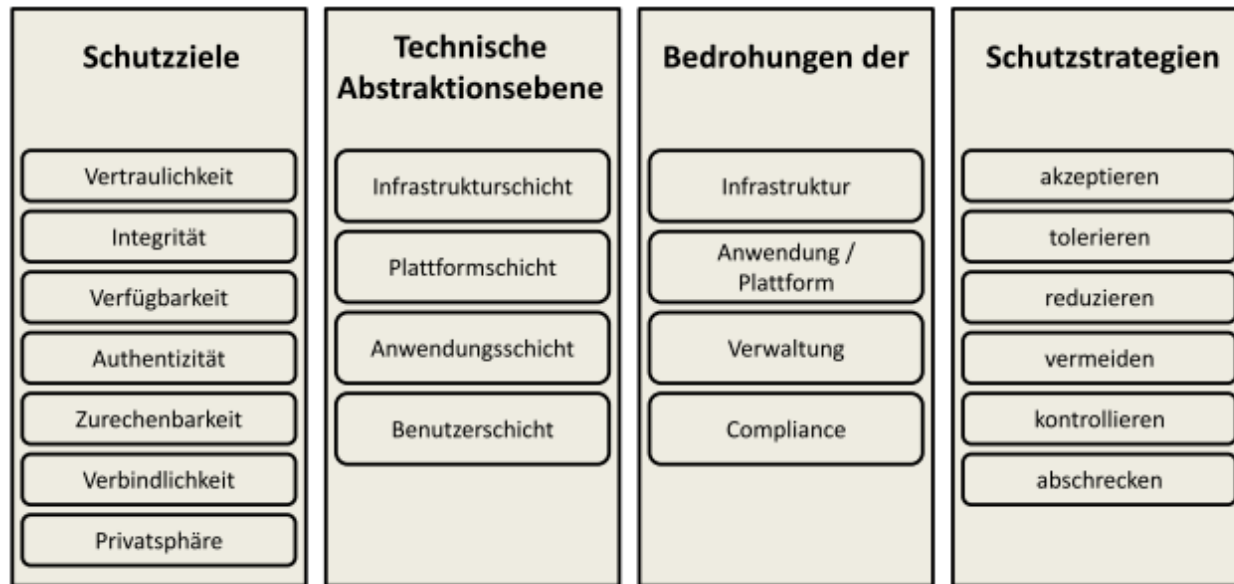


# Cloud Computing Sicherheit:

## CLOUD COMPUTING SICHERHEIT SCHUTZZIELE.TAXONOMIE.MARKTÜBERSICHT.

DR. WERNER STREITBERGER, ANGELIKA RUPPEL

09/2009



## 2014/32/EU Annex I / MessEV-E Anlage 2

Wesentliche Anforderungen

### 8. Schutz gegen Verfälschungen

8.4 Messdaten oder Software, die für die messtechnischen Merkmale entscheidend sind, sowie messtechnisch wichtige Parameter, die gespeichert oder übertragen werden, **sind angemessen** gegen versehentliche oder vorsätzliche Verfälschung zu schützen.

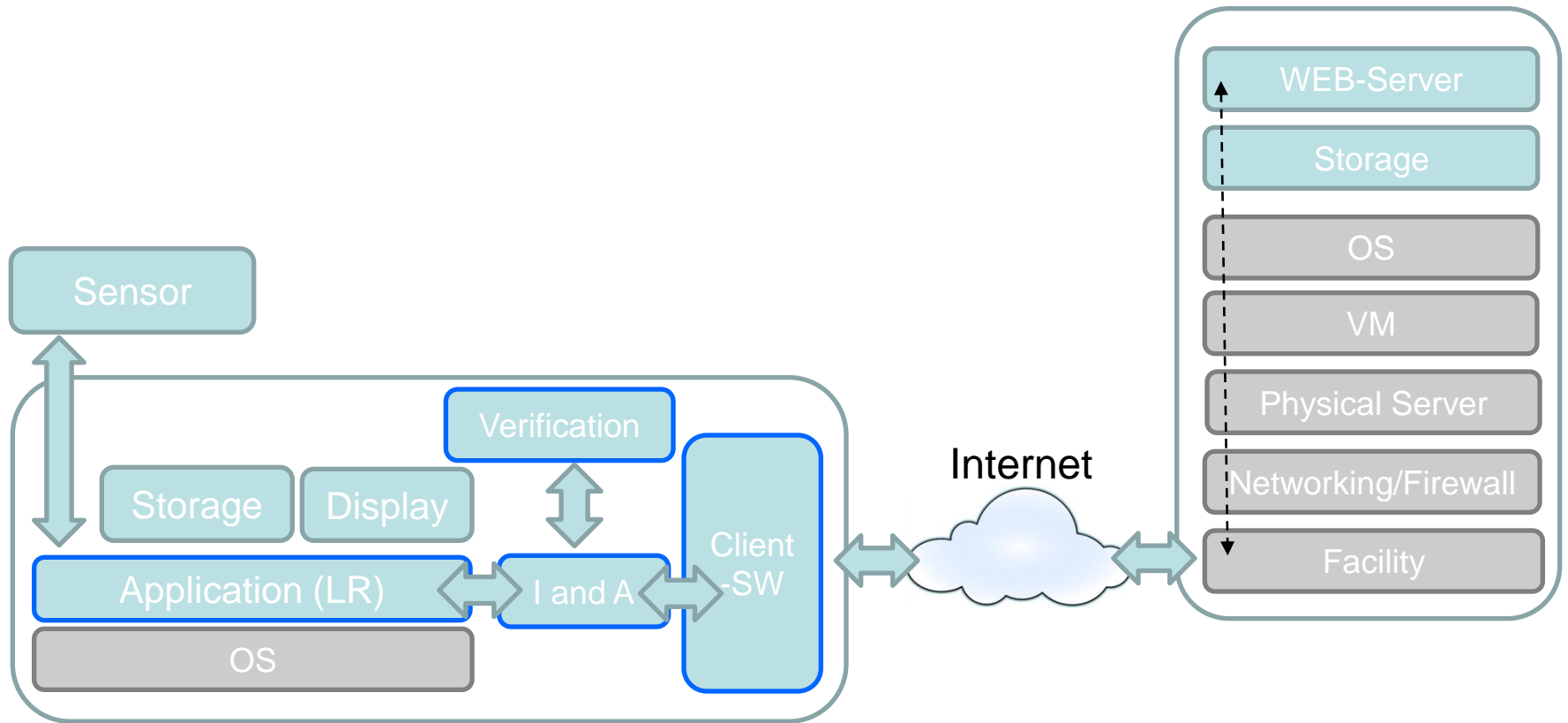
⇒ Bei komplexen Technologien ist ein objektives Bewertungsverfahren hilfreich.

Bewertung ausgerichtet an internationalen Standards wie den "Common Criteria for Information Technology Security Evaluation" ISO 15408:2005 (Common Criteria).

1. Externe Speicherung von Messdaten
2. Verarbeitungssoftware in der Cloud



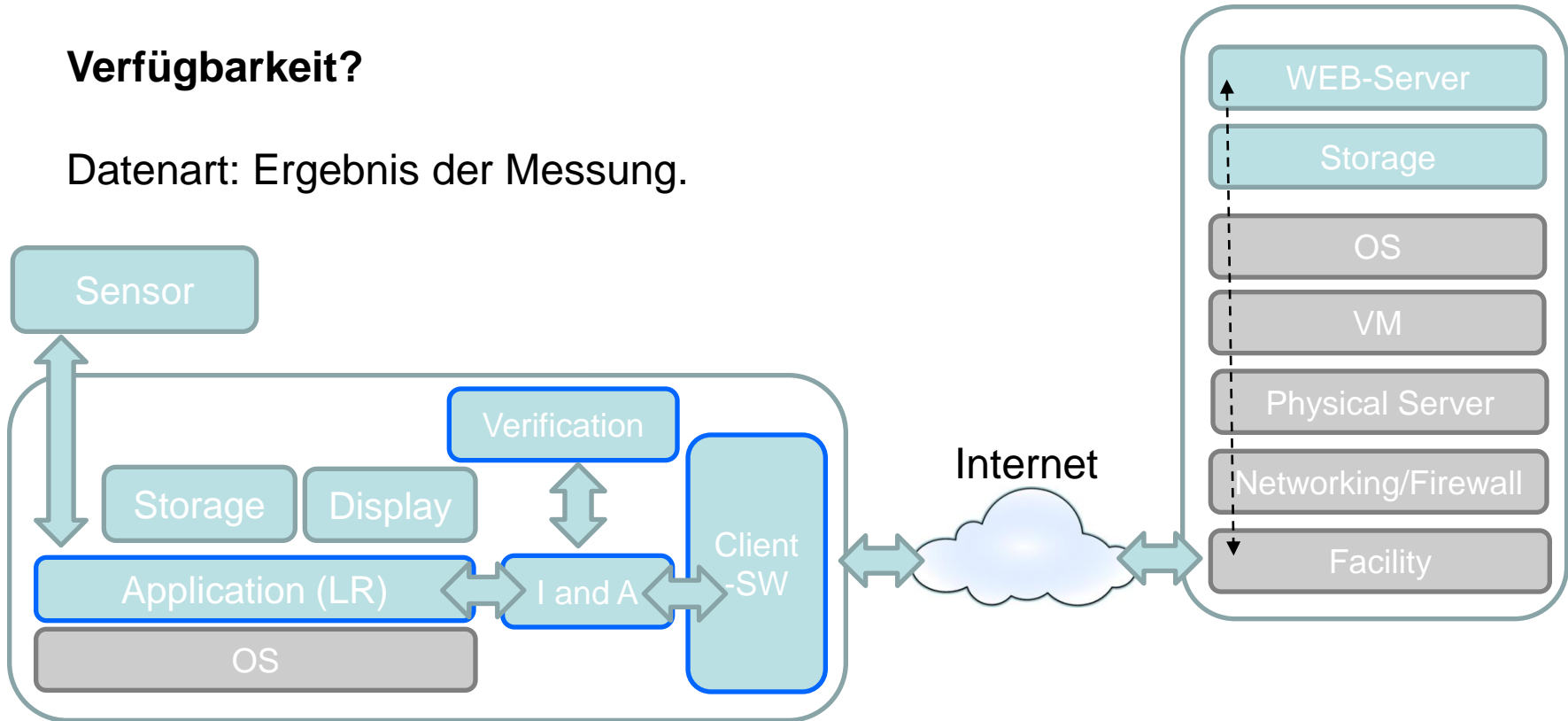
# Diskussions-Beispiele: Externe Speicherung von Messdaten



# Diskussions-Beispiele: Externe Speicherung von Messdaten

## Verfügbarkeit?

Datenart: Ergebnis der Messung.



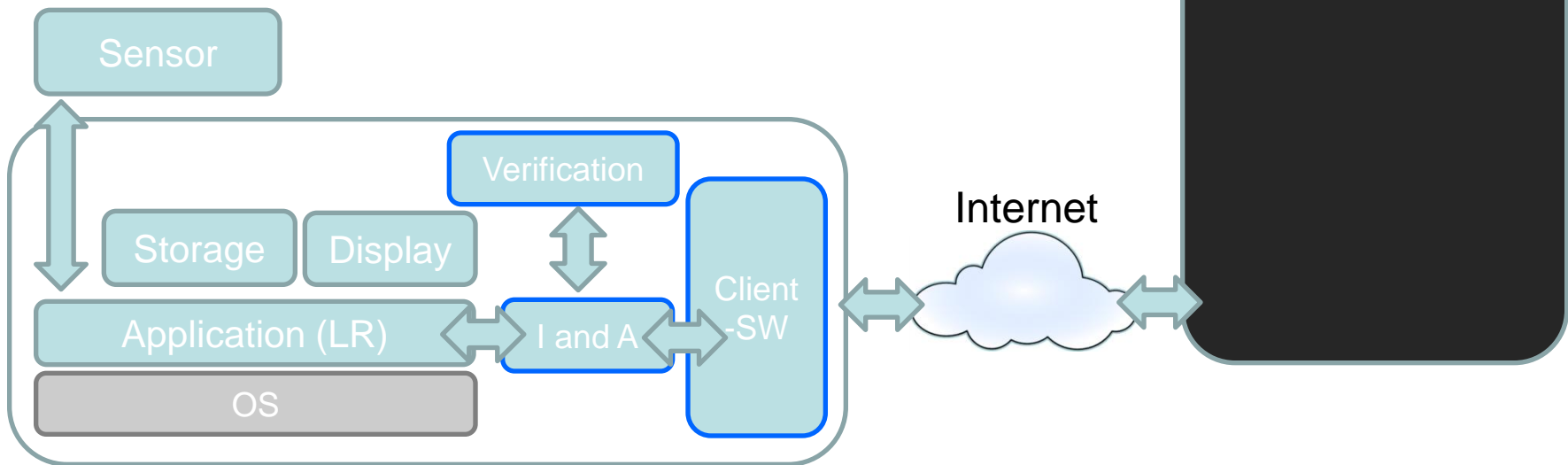
Gespeicherte Messdaten werden für die Abrechnung verwendet oder für die Befundprüfung.

„Ohne Beweis ist im Rahmen einer Befundprüfung die Schuld geklärt!“

# Diskussions-Beispiele: Externe Speicherung von Daten

**Sicherheit:** „Direct Trust“- (Ende-zu-Ende Sicherheit)

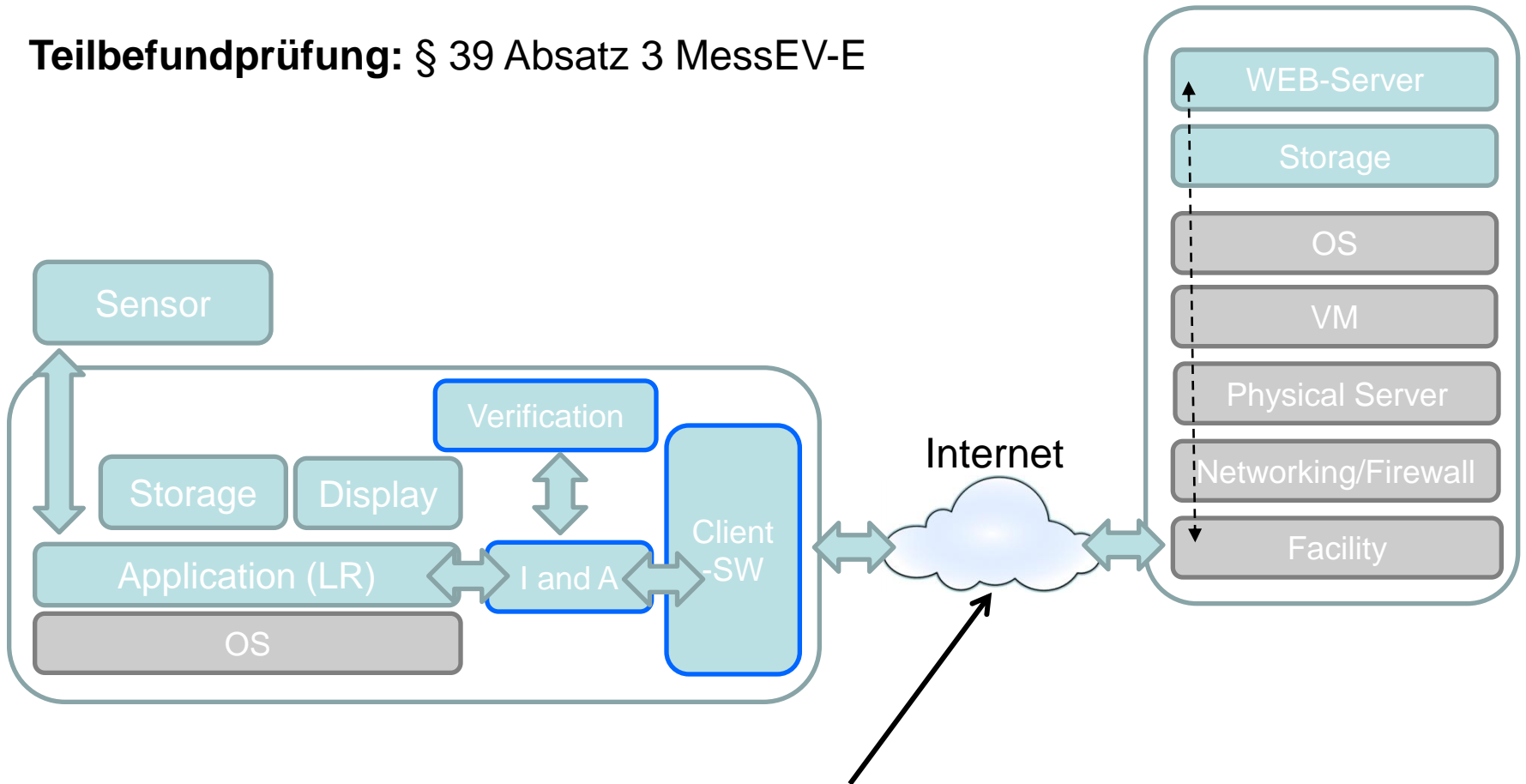
=> Cloud ist Black-Box



- Beispiel: Betonwaage: Tagesprotokoll in die Cloud.
- Integrität und Authentizität über Signatur, d.h. asymmetrische Kryptographie. Prüfung am Gerät möglich.

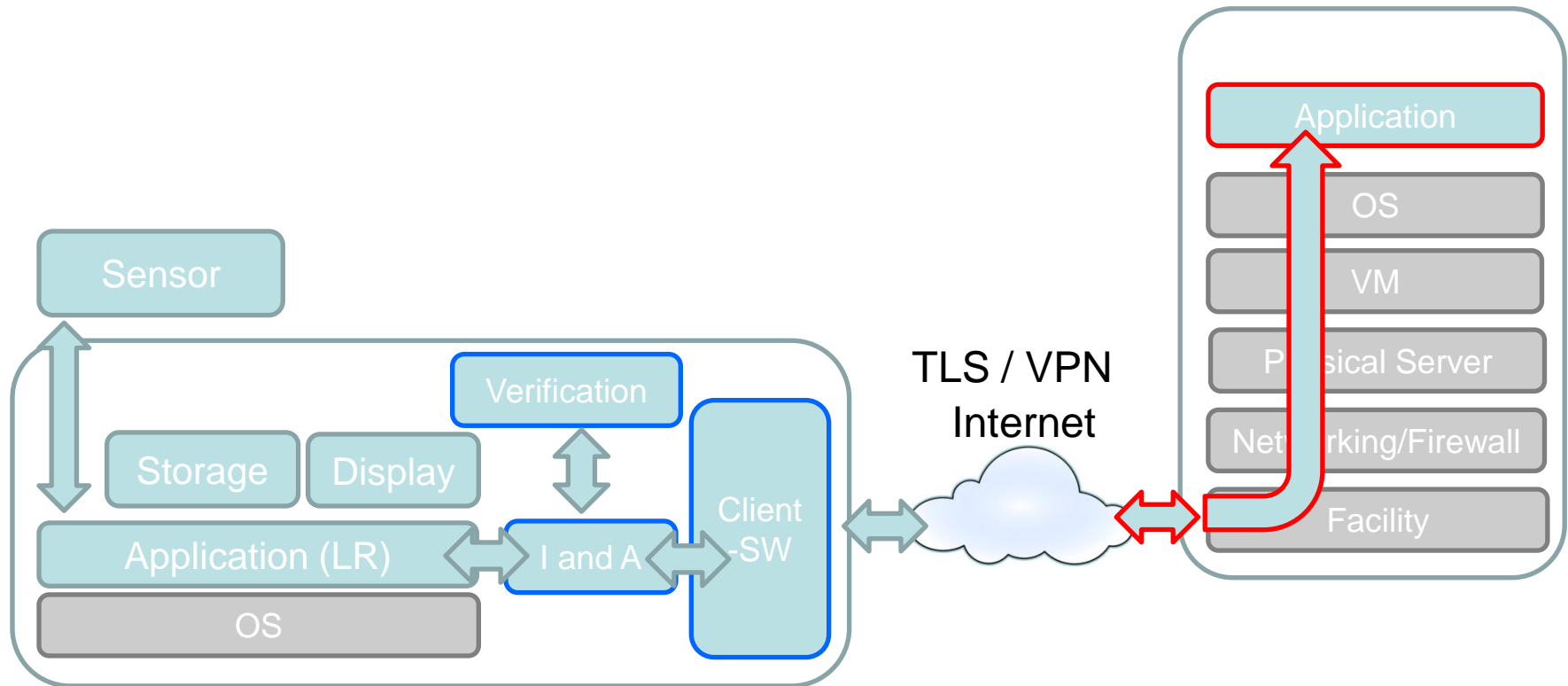
# Diskussions-Beispiele: Externe Speicherung von Daten

## Teilbefundprüfung: § 39 Absatz 3 MessEV-E



Externe Prüfung:  
PKI sichert Korrektheit des öffentlichen Schlüssels.

# Diskussions-Beispiele: Externe Software



- Gleichwertigkeit zur Desktop-Lösung
- Handshake-Betrieb und Internet-Tunnel
- Übliche Anforderungen an OS nach NSA/PTB Anforderungen?
- Sicherheitsupdates für OS über Hersteller.  
(Admin-Herausforderung => Eine Lösung über ROOT-PW Generation bei Eichbehörden)

## Danke für Ihre Aufmerksamkeit!

Fragen...



### Kontakt

Daniel Peters  
Tel.: 030 3481-7479  
E-Mail: [dieter.richter@ptb.de](mailto:dieter.richter@ptb.de)

Dr. Florian Thiel  
Tel.: 030 3481-7529  
E-Mail: [florian.thiel@ptb.de](mailto:florian.thiel@ptb.de)

### Sekretariat

Heike Kautz  
Tel.: 030 3481-7494  
Fax: 030-3481-7506  
E-Mail: [heike.kautz@ptb.de](mailto:heike.kautz@ptb.de)

### Anschrift

Physikalisch-Technische Bundesanstalt  
Fachbereich 8.5  
Abbe Str. 2-12  
10587 Berlin

