Cloud-Computing-Sicherheit – Taxonomie der Sicherheitsaspekte und Herausforderungen für die IT-Sicherheit

Dr. Werner Streitberger

Projektleiter Cloud-Computing-Sicherheit

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Frankfurt, 20.11.2009

Übersicht

1. Motivation
2. Cloud-Computing-Charakteristika
3. Sicherheitsimplikationen
4. Taxonomie der Sicherheitsaspekte
5. Zusammenfassung

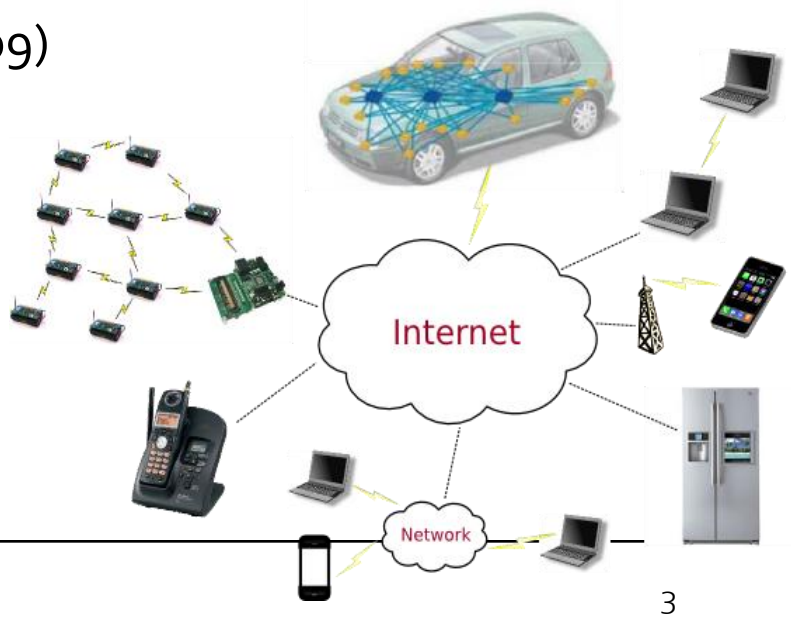
1. Motivation

„The broad and rich foundation of the internet will unleash a "service wave" of applications and experiences available instantly. Services designed to scale to tens or hundreds of millions [of users] will dramatically change the nature and cost of solutions deliverable to enterprises or small business. This new wave will be very disruptive." (Bill Gates, 2005)

„Sie werden zu jedem Zeitpunkt, von jedem Ort, mit jedem Gerät ins Netz gehen können. […] Aber ihre Privatsphäre verschwindet, finden Sie sich damit ab." (Leonard Kleinrock, SZ, 29.10.2009)

Internet der nächsten Generation:

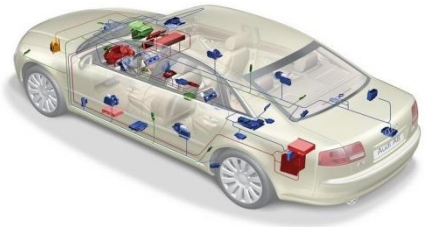
- Hochgradig verteilt und vernetzt
- Heterogen, hoch dynamisch und interaktiv
- Vielzahl von kooperierenden Systemen

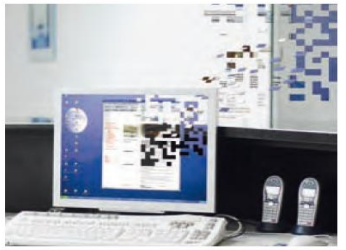


1. Motivation

Internet der nächsten Generation: Herausforderung für die IT-Sicherheit

- Ubiquitäre Vernetzung und IT-Durchdringung
  Schutz von Daten in offenen Umgebungen?
- Vielzahl interagierender Komponenten
  Identifikation, Schutz eingebetteter Komponenten?
- Offene Dienste-Marktplätze
  Vertrauenswürdige Dienste in offenen Umgebungen?





These: Internet der nächsten Generation ist

- Das Internet der Dinge und Dienste
- Cloud-Computing ist ein integraler Bestandteil

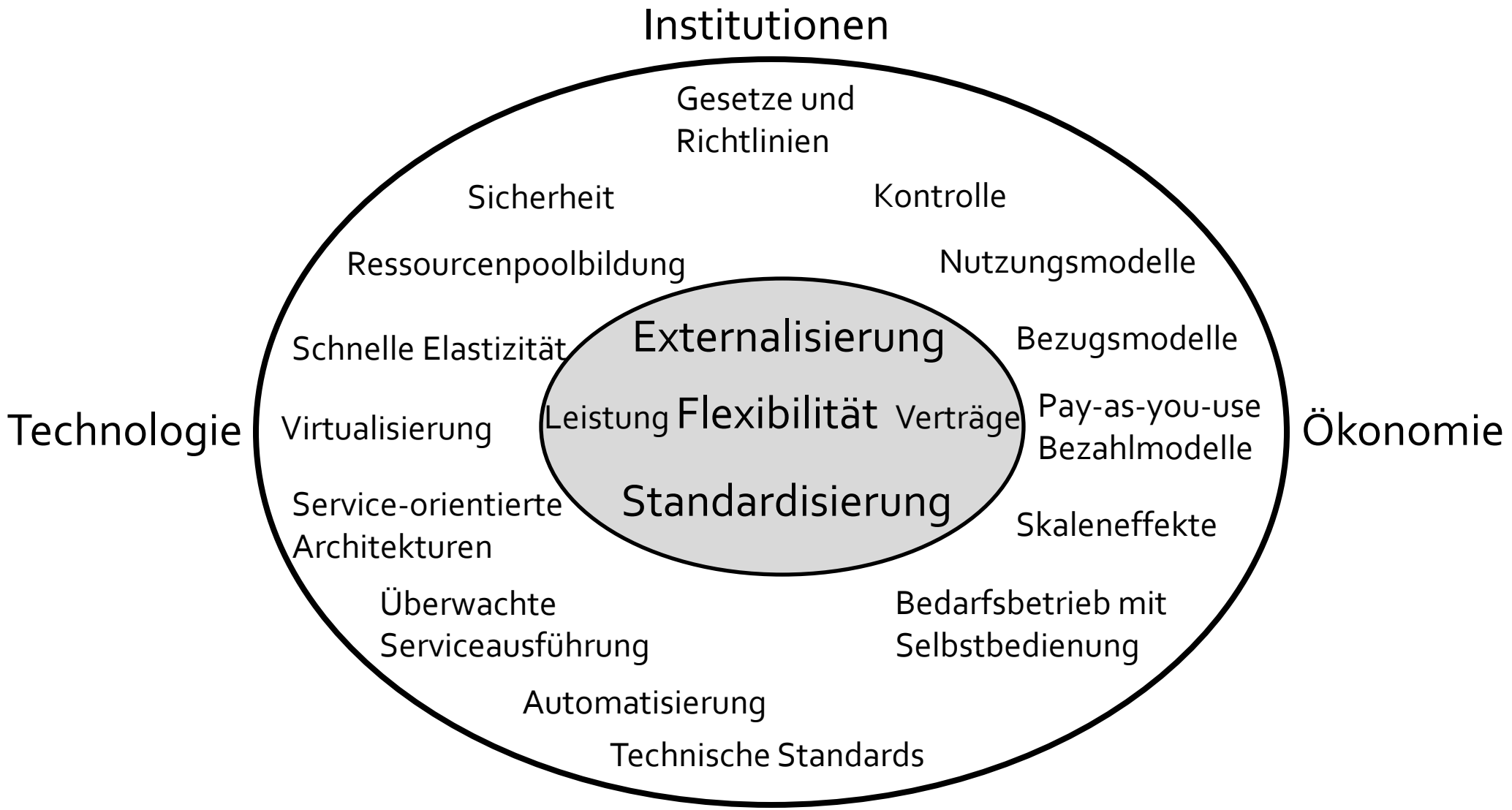
2. Cloud-Computing

Cloud: Pool aus vernetzten IT-Komponenten, die Kundenanwendungen verwalten und die Ressourcennutzungen nach Verbrauch abrechnen

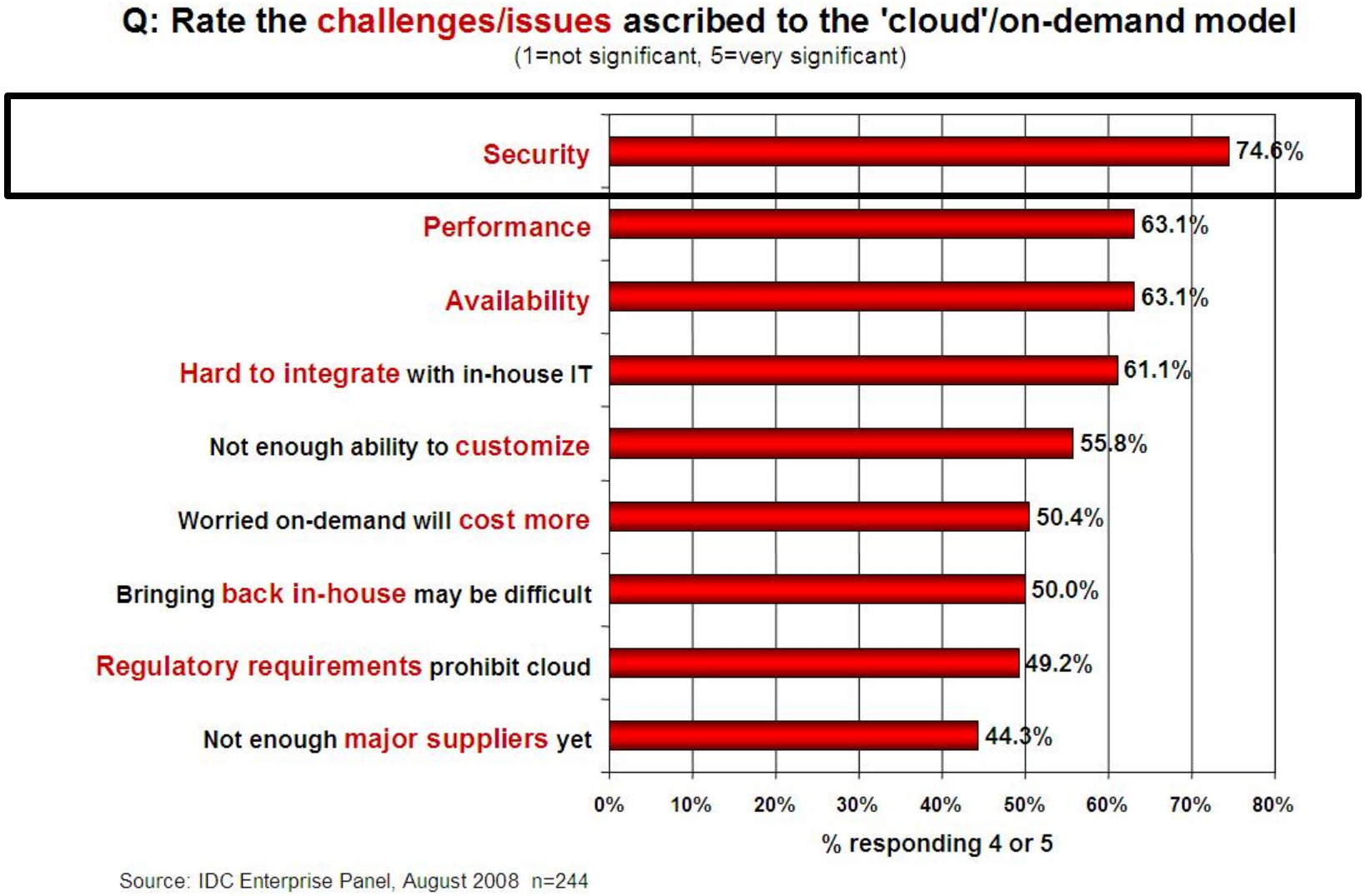
Cloud-Charakteristika

- Hardware-Komponenten, wie CPU, Speicher, Netz werden bei Bedarf zur Verfügung gestellt
  - Nutzer muss keine eigene Infrastruktur betreiben
- ‚unendlich' viele Ressourcen durch dynamische Hinzunahmen von Kapazitäten:
  - Nutzer kann in kürzeren Intervallen im Voraus planen, konfigurieren, …
- Einfache Erstellung von neuen Web-Anwendungen als Services, die über die Cloud global nutzbar gemacht werden können
- Zugriffe auf ausgelagerte Daten: jederzeit, von überall

2. Cloud-Computing: Charakteristika, Einflussfaktoren, Ziele



2. Cloud-Computing: Herausforderungen



3. Sicherheitsimplikationen

"The effect of the growing dependence on cloud computing is similar to that of our dependence on public transportation, particularly air transportation, which forces us to trust organizations over which we have no control, limits what we can transport, and subjects us to rules and schedules that wouldn't apply if we were flying our own planes. On the other hand, it is so much more economical that we don't realistically have any alternative."

(Whitfield Diffie, TR, 16.11.2009)

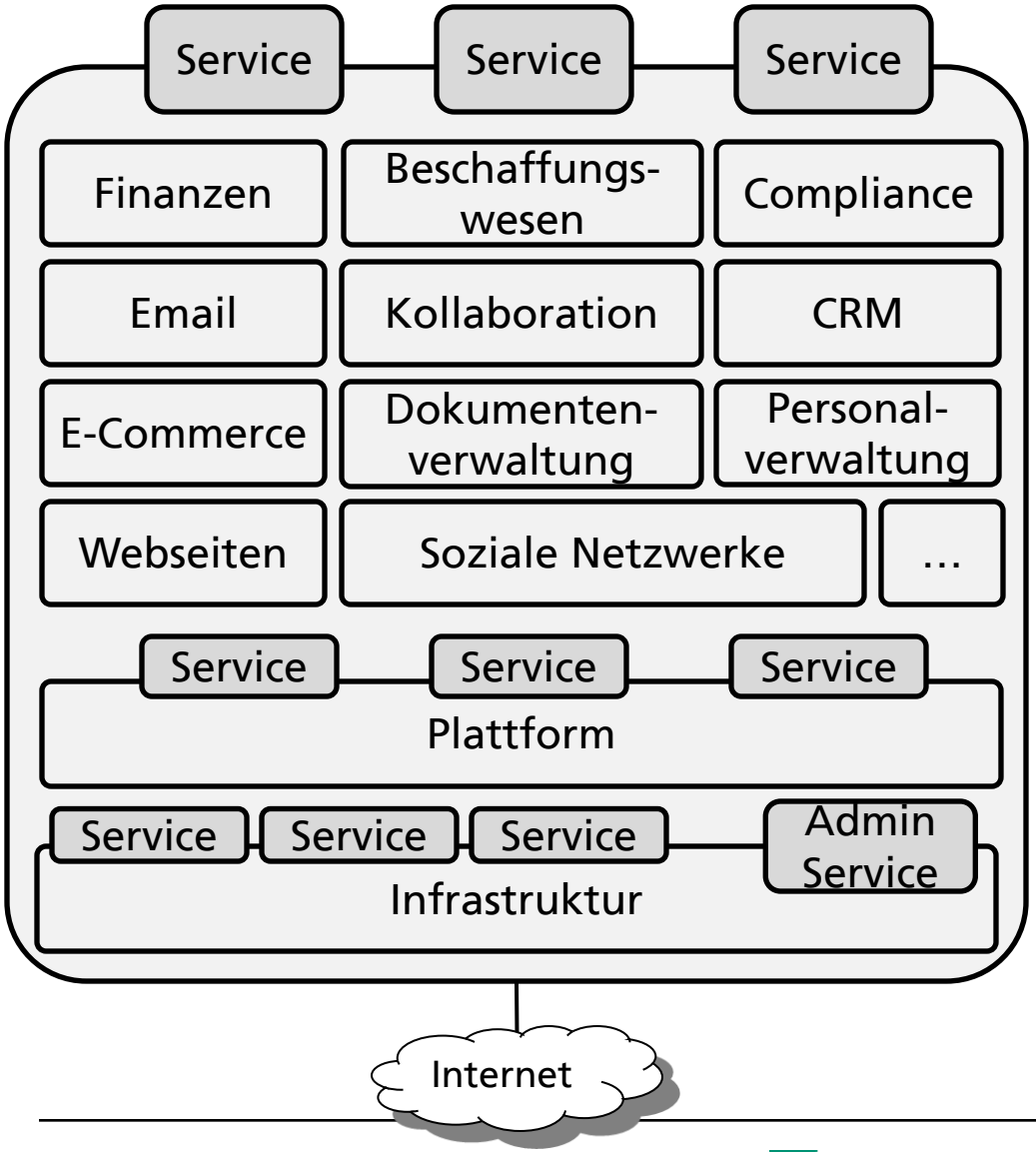
Quelle: http://www.technologyreview.com/computing/23951/

3. Sicherheitsimplikationen

Cloud-Charakteristika und deren Auswirkungen auf die Sicherheit

- Hardware-Komponenten, wie CPU, Speicher, Netz werden on-demand zur Verfügung gestellt:
  - Vertraulichkeit? Wo werden die Daten gespeichert (Land?), wie wird verschlüsselt,…
  - Authentizität? Wie wird ein Identitäts- und Access-Management durchgesetzt
- „unendlich" viele Ressourcen durch dynamische Hinzunahme von Kapazitäten:
  - Privatsphäre: Wohin werden Daten ausgelagert, Privacy versus Abrechenbarkeit
  - Integrität? Aufteilung von Daten, Transaktionsintegrität?
- Einfache Erstellung von neuen Web-Anwendungen als Services, die über die Cloud global nutzbar gemacht werden können
  - Vertrauenswürdigkeit der Cloud-Server? Verwaltung von Zugriffsrechten, Schlüssel, Identitäten? Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit der Dienste?
- Zugriffe auf ausgelagerte Daten: jederzeit, von überall
  - Verfügbarkeit? Denial-of-Service-Angriffe, Gefahr des Daten-Lock-in, ….

3. Sicherheitsimplikationen: Software-as-a-Service



GoogleDocs

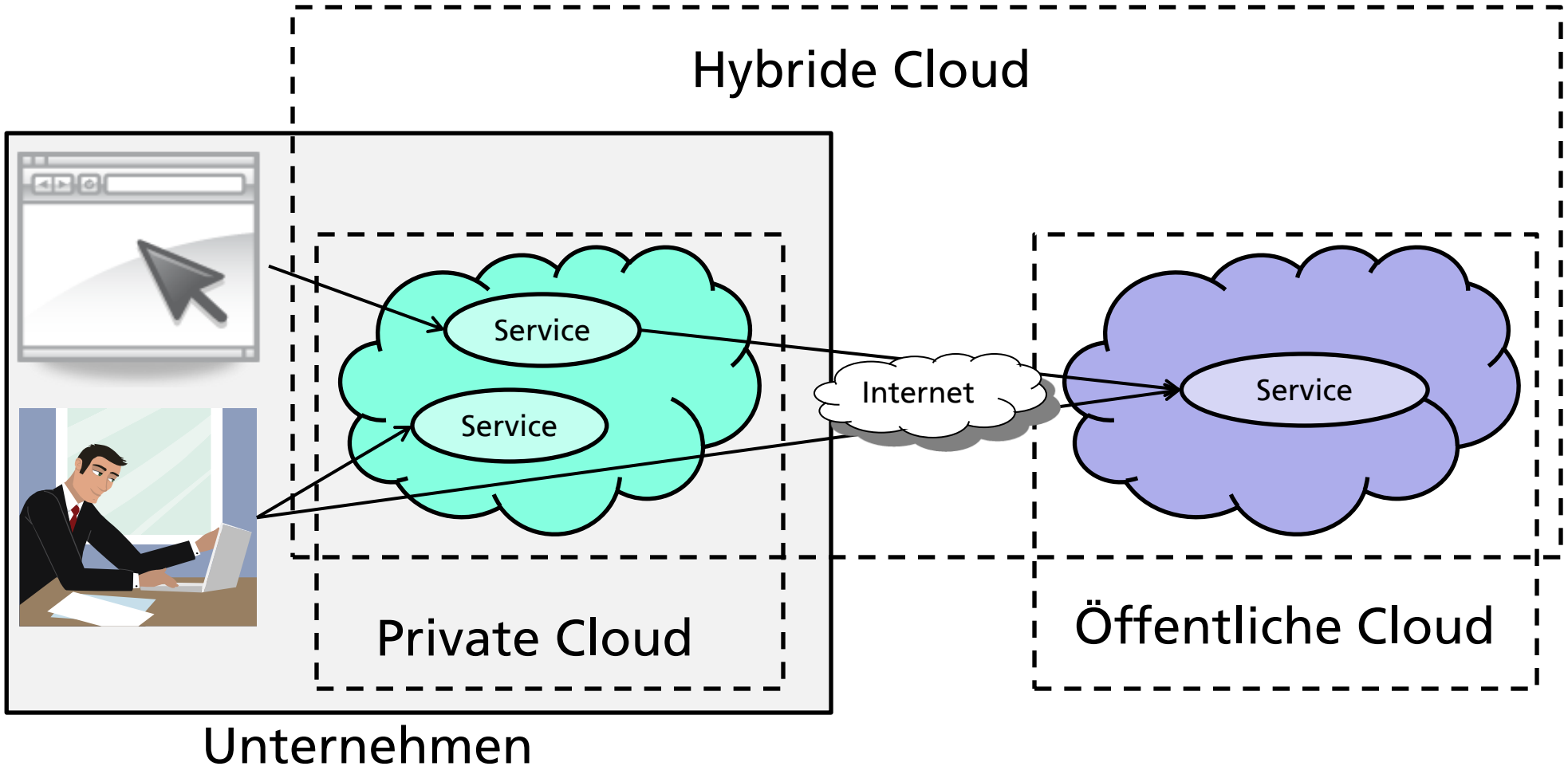
GoogleAppEngine

E-Commerce Anwendung

Microsoft Azure

Amazon S3

3. Sicherheitsimplikationen der Nutzungsmodelle



3. Sicherheitsimplikationen: Öffentliche Cloud

Öffentliche Cloud

- Auswahl des Dienstes durch den Cloud-Nutzer
  - Wie erfüllen Anbieter die Schutzziele der Nutzer? Nachweislich?
- Bereitstellung/Nutzung der Dienste über ein öffentliches Netzwerk
  - Alle Bedrohungen durch das Internet können auftreten
- Administration idR über ein Verwaltungsportal:
  - Administrative Schnittstelle ist lohnendes Angriffsziel, hohe Risiken
- Bezahlung durch ein Pay-per-Use Modell
  - Ökonomischer Schaden durch nicht-autorisierte Nutzung möglich
- Häufig kein permanenter Vertrag oder langfristige Vertragsbindung
  - Nur standardisierter Vertrag mit minimalen Garantien auswählbar
  - Häufig keine Risikoübernahme durch den Anbieter

3. Sicherheitsimplikationen: Private und hybride Cloud

Private Cloud

Emulation einer öffentlichen Cloud auf unternehmensinternen Ressourcen

- dynamische Ressoucenzuweisung ist begrenzt auf Domäne
- Bessere Kontrolle hinsichtlich der Sicherheit: ‚alles aus einer Hand‘, zentrale Kontrollen, homogenes Sicherheitsmanagement, SLAs
- Überwachung und Durchsetzung der Unternehmensrichtlinien hinsichtlich der Ressourcennutzung leichter durchsetzbar

Aber: geringere Flexibilität, Skalierbarkeit, eingeschränkter Nutzerkreis

Hybride Cloud

- Nutzung öffentlicher Cloud-Ressourcen bei kurzfristigen Kapazitätsspitzen
- Problem: Klassifikation der Daten ist notwendig, automatisch?
  Umgang mit datenschutzrelevanten Daten, Anonymisierung?

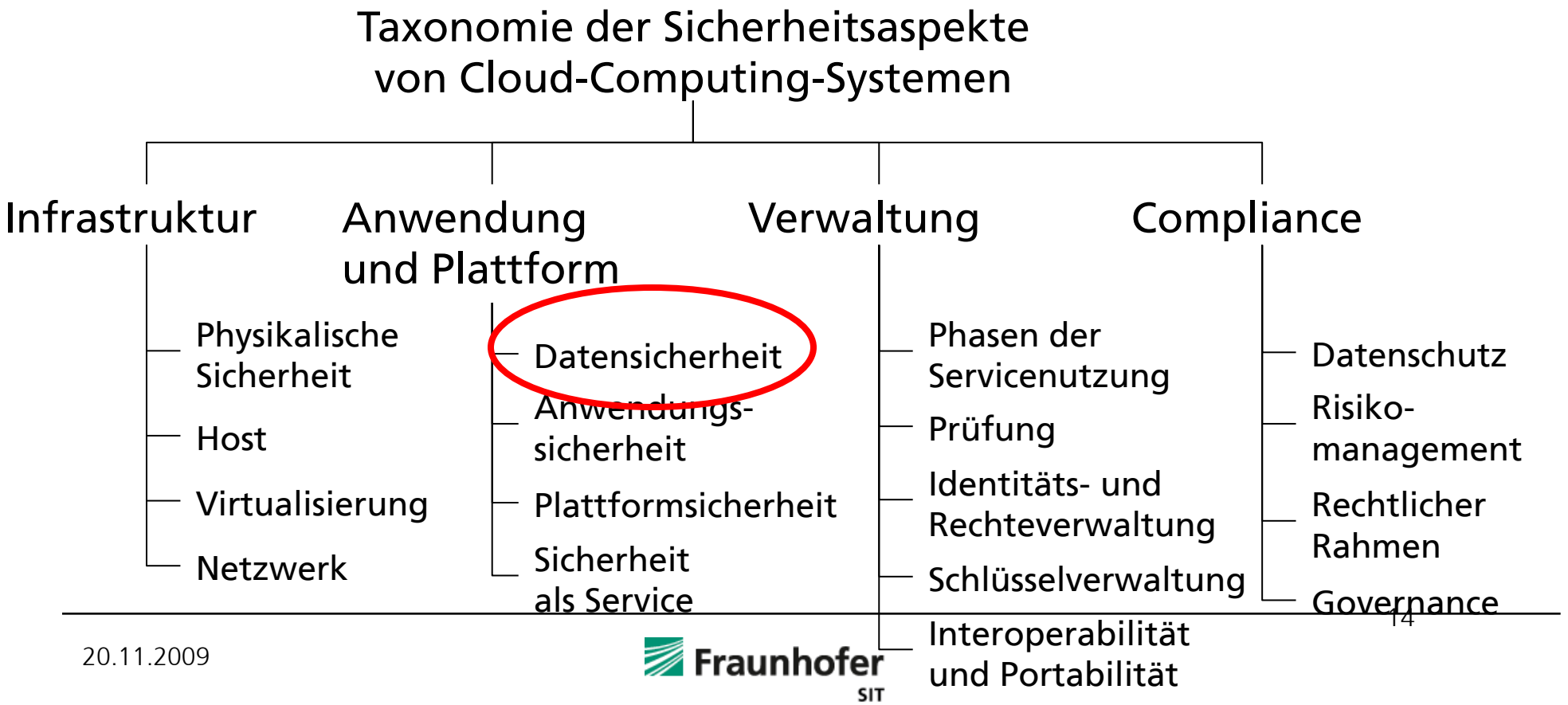
4. Taxonomie der Sicherheitsaspekte

Ziel: Rahmen zur Bewertung der Cloud-Sicherheit

Ansatz: Taxonomie der sicherheitsrelevanten Bereiche

Einsatz: Risikobewertung von Cloud-Services anhand der Taxonomie

Vollständige Taxonomie: Cloud-Sicherheits-Studie des Fraunhofer SIT, Sept.2009



4. Taxonomie: Datensicherheit

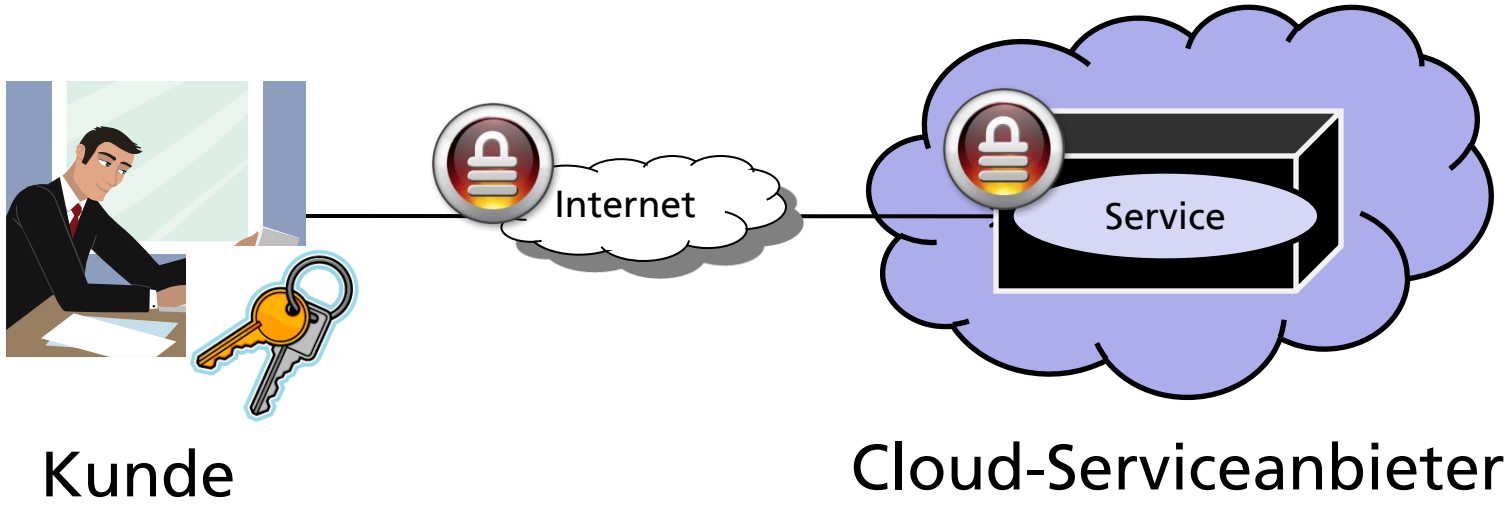
Aus Sicht des Nutzer zu klären:

- Welche Sicherheitsmaßnahmen werden eingesetzt, um die Datenspeicherung und Datenverarbeitung abzusichern?
- Welche Sicherheitsmaßnahmen besitzen die verwendeten Datenstrukturen?

- **Maßnahmen für Datensicherheit durch SaaS oder IaaS Anbieter**
  - Sichere Übertragung und Speicherung von Daten durch den Anbieter?
  - Verwendete Verfahren?
  - Sicherheitsrichtlinien und Regelungen zur Schlüsselverwaltung (z. B. verteilte Speicherung), Replikaverwaltung, Langzeitspeicherung, Speicherort, Löschung und Wiederherstellung?
  - Kontinuierliche Überprüfung der Datensicherheit durch externen Dienstleister? Zertifizierungen?

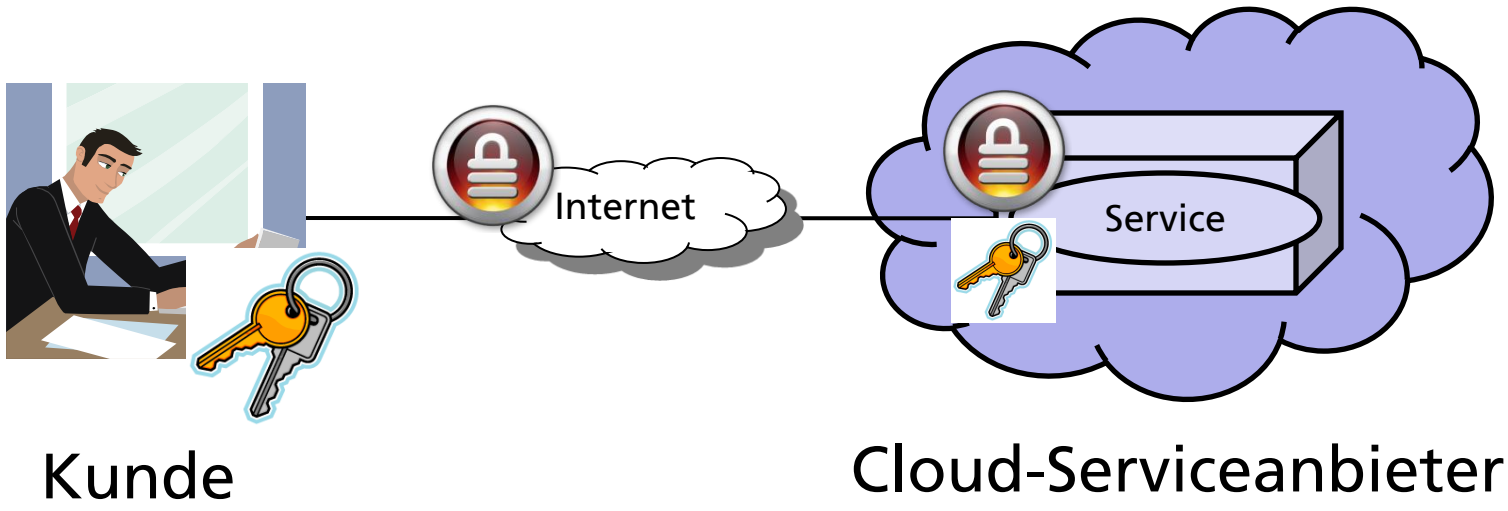
4. Taxonomie: Datensicherheit

- Modell 1: Datensicherheit ohne Garantien des Cloud-Serviceanbieters
  - Kunde muss alle Aktionen vor der unsicheren Cloud-Umgebung verstecken (z. B. durch Verschlüsslung oder durch Anwendung von „Security-by-Obscurity“)



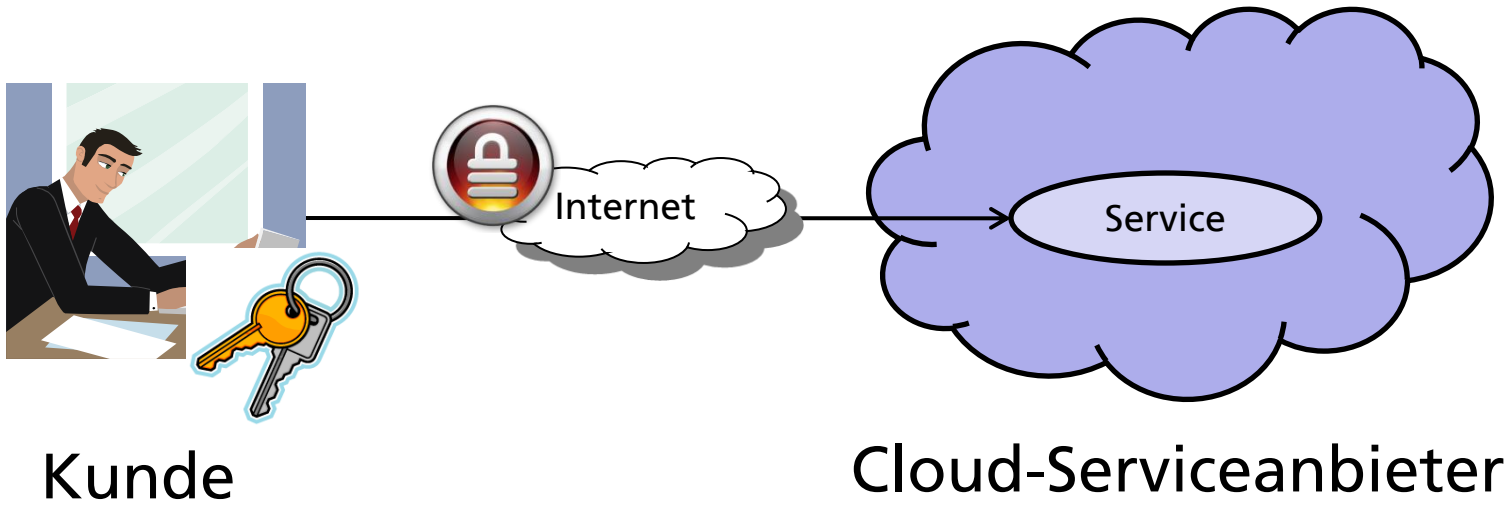
4. Taxonomie: Datensicherheit

- Modell 2: Datensicherheit mit Garantien des Cloud-Serviceanbieters
  - Benutzung einer abgegrenzten Umgebung (z. B. Amazon Virtual Private Cloud)



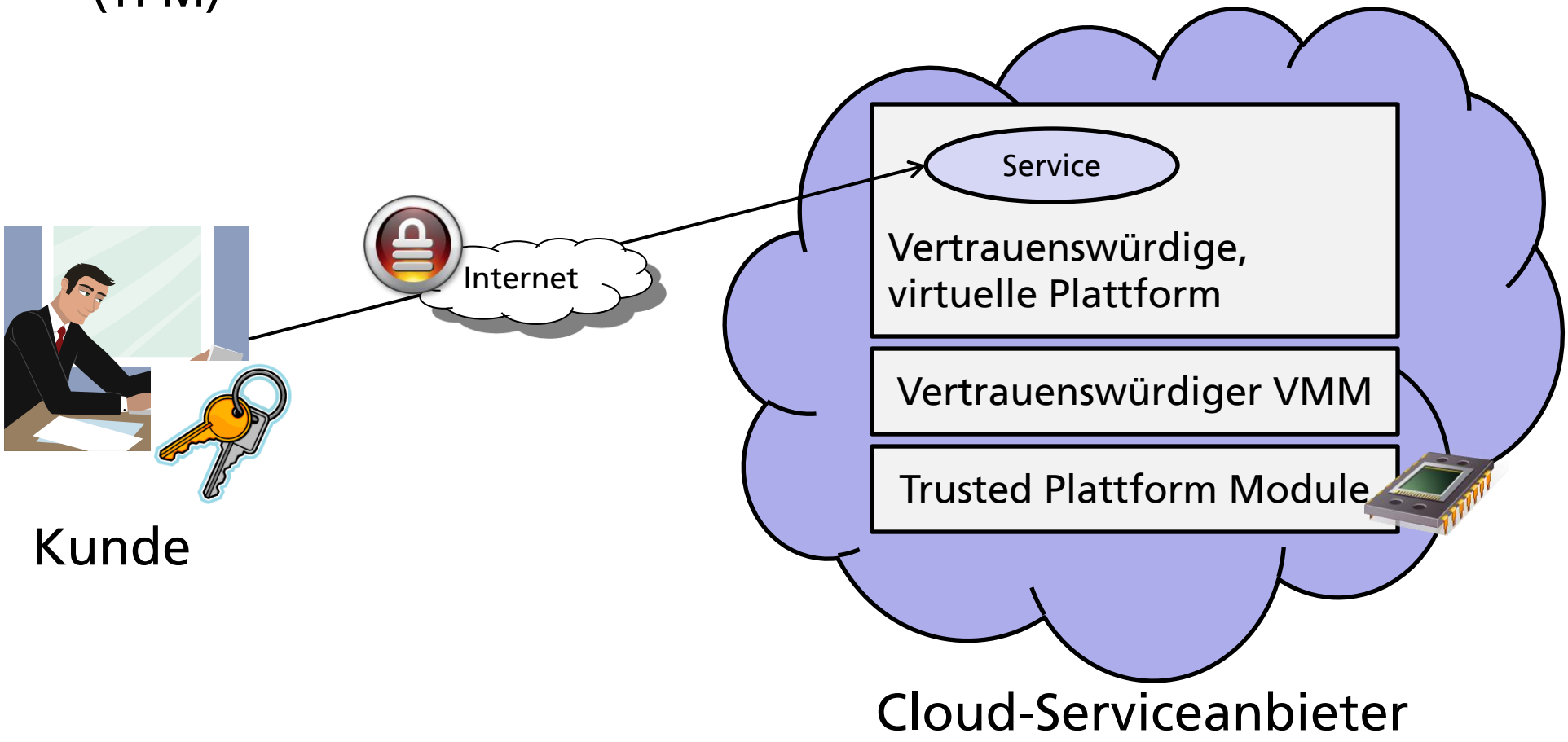
4. Taxonomie: Datensicherheit

- Modell 3: Datensicherheit mit Garantien des Cloud-Serviceanbieters und Vertrauen in den Serviceanbieter
  - Vertrauen in Zertifikate und Reputation des Anbieters



4. Taxonomie: Datensicherheit

- Modell 4: Verwendung von Trusted Plattform Modulen (TPM)



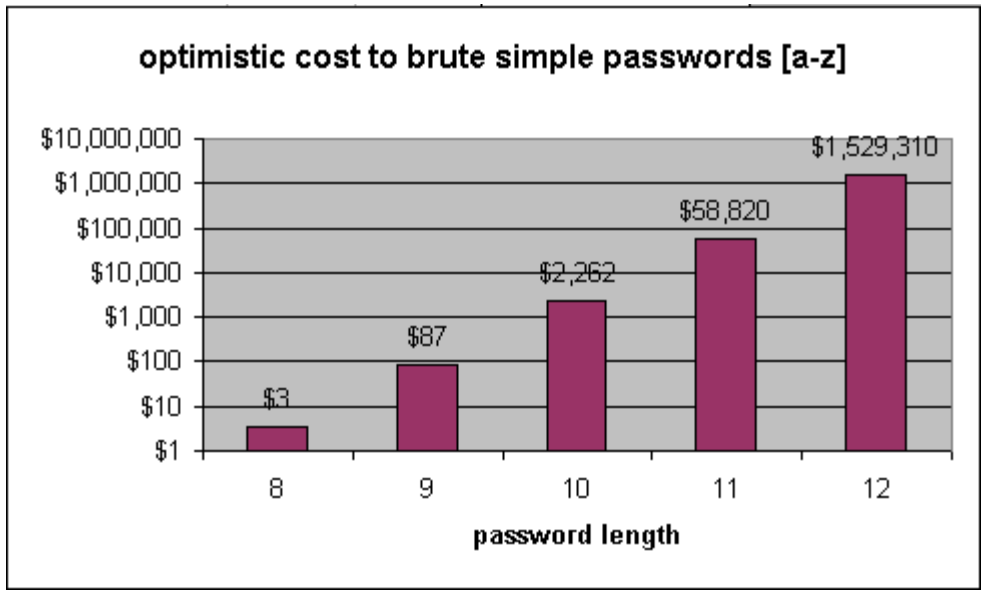
4. Taxonomie: Bedrohungen der Datensicherheit

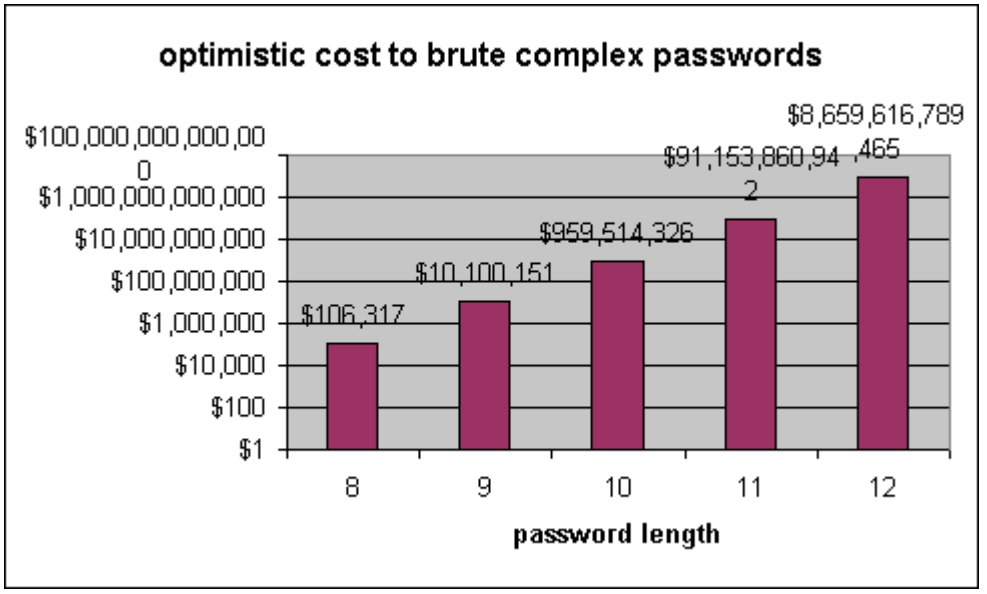
- Beispiel: **Datenverlust bei Sidekick von Danger/Microsoft** (10/2009)
- Datenverlust beim Upgrade des SAN
- Kein serverseitiges Backup der Daten
- Temporäre, lokale Kopie der Daten im Speicher des Endgeräts

Quelle: http://www.heise.de/newsticker/meldung/Sidekick-Datenverlust-wirft-Schatten-auf-die-Cloud-821328.html

4. Taxonomie: Bedrohungen der Datensicherheit

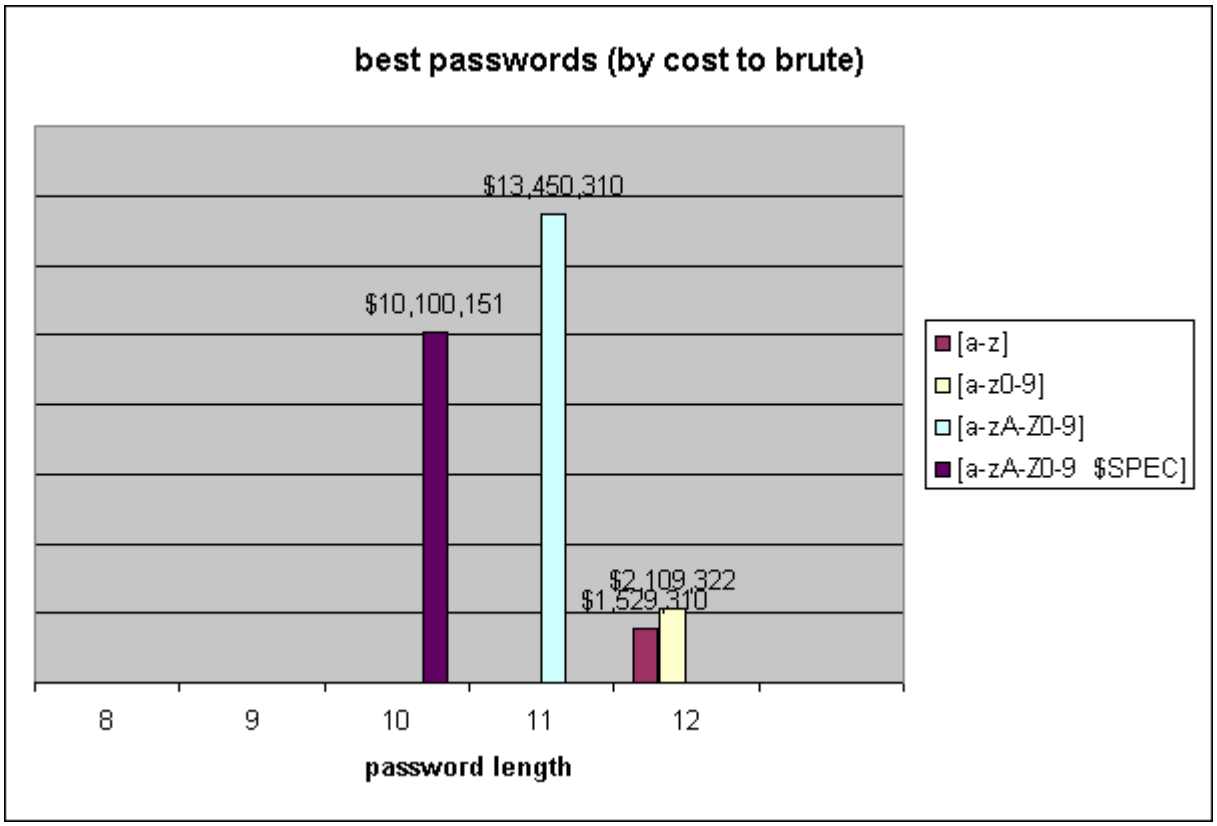
- Beispiel: Schlüsselbrechen in der Cloud (10/2009)
  - Kosten für das Brechen eines PGP-Schlüssels mit der Software EDPR auf Amazon EC2 Ressourcen





Quelle: http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html

4. Taxonomie: Bedrohungen der Datensicherheit



Quelle: http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html

5. Zusammenfassung

- Cloud-Computing: **Chancen** für Nutzer und Anbieter:
  - Kostenreduktion, innovative Geschäftsprozesse, ...
- Cloud-Computing: Vielzahl von **Sicherheitsrisiken**
  - Bedrohung der Privatheit, Vertraulichkeit, Integrität, Verfügbarkeit
- SIT-Taxonomie als Rahmen für eine systematische **Risikobewertung**

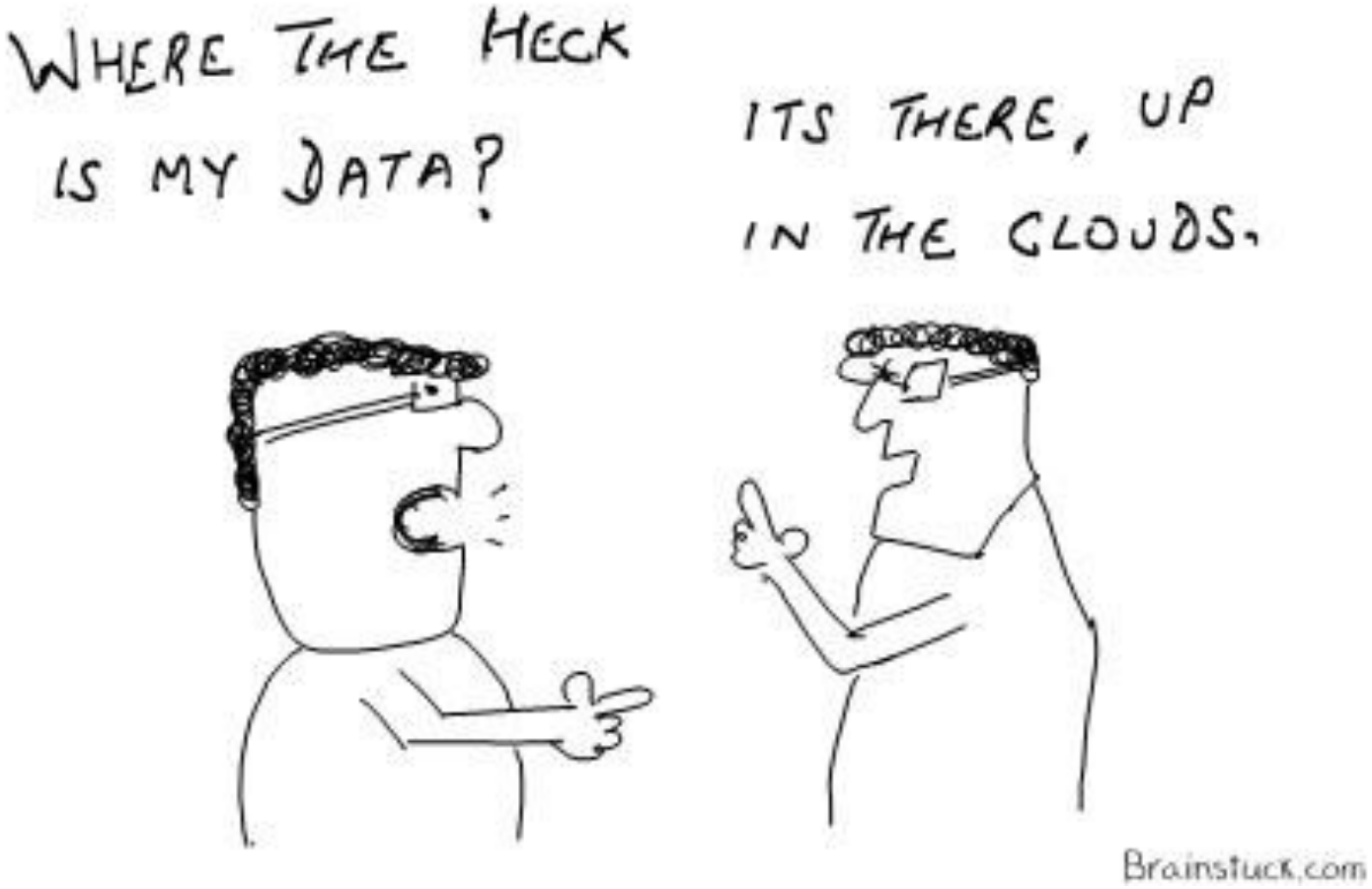
Stand der Datensicherheit heutiger Cloud-Angebote:

- Verschlüsselte Datenübertragung Standard
- Vertrauen in den Anbieter notwendig
- **SLAs** meist nur mit minimalen Garantien, unzureichend für Risikotransfer

Offene Fragen: u.a.

- Standardisierte Technologien und Prozesse: Was wird sich durchsetzen?
- Interoperabilität/Portabilität von Datenformaten: Lock-in-Effekte?

5. Zusammenfassung



Vielen Dank für Ihre Aufmerksamkeit

Dr. Werner Streitberger

Sichere Services und Qualitätstests

Fraunhofer-Institut SIT

Parkring 4

D-85748 Garching bei München

E-Mail: werner.streitberger@sit.fraunhofer.de

Internet: http://www.sit.fraunhofer.de