Sicherheit und Cloud Computing -- Ein Widerspruch?

Dr. Werner Streitberger

Projektleiter Cloud-Computing-Sicherheit

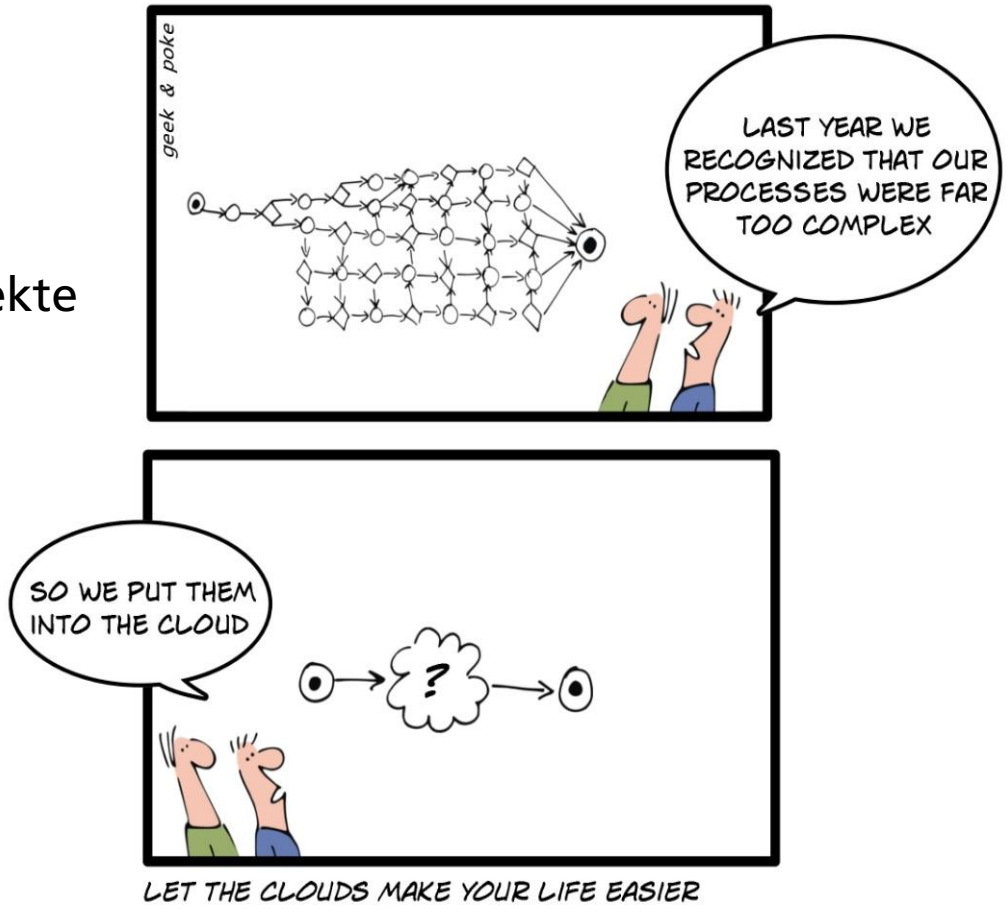
Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

München, 28.04.2010

Fraunhofer SIT

Übersicht

- Motivation
- Definition: Cloud-Computing
- Sicherheitsimplikationen
- Taxonomie der Sicherheitsaspekte
- Datensicherheit
- Zusammenfassung



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)

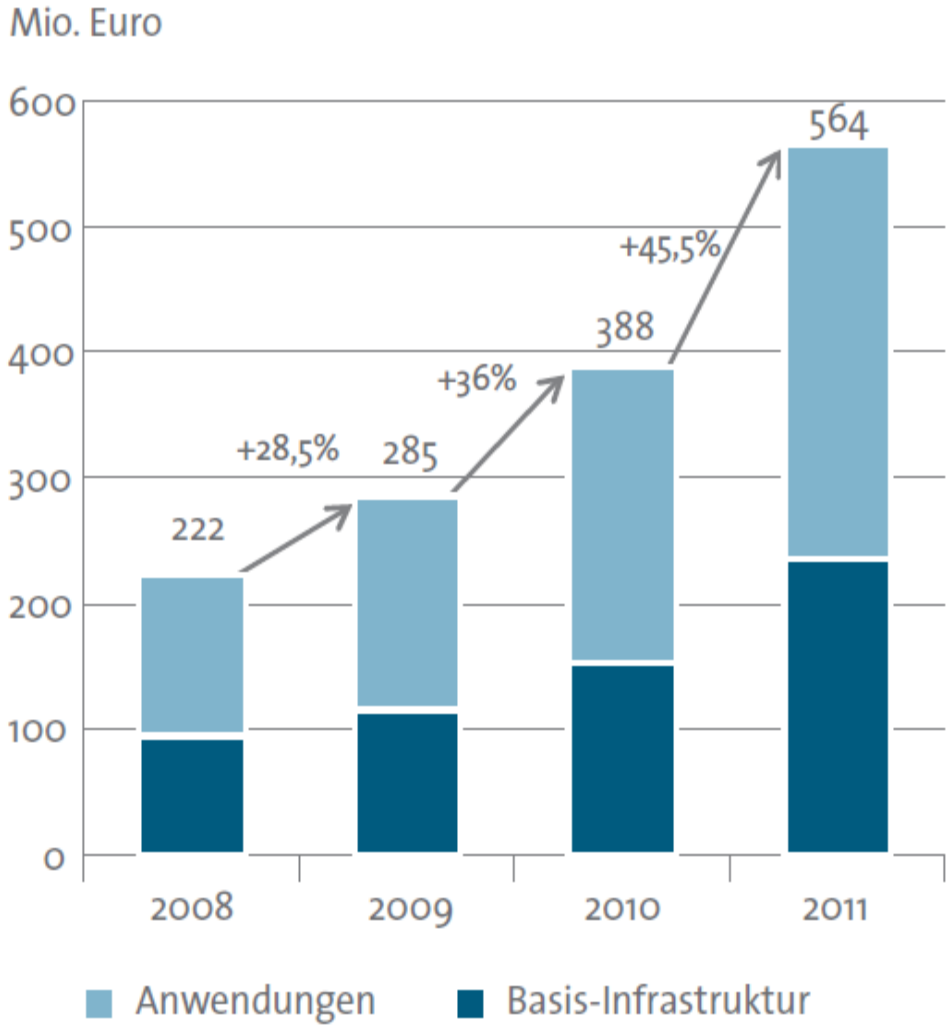
Motivation

"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, Technology Review, 16.11.2009)

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

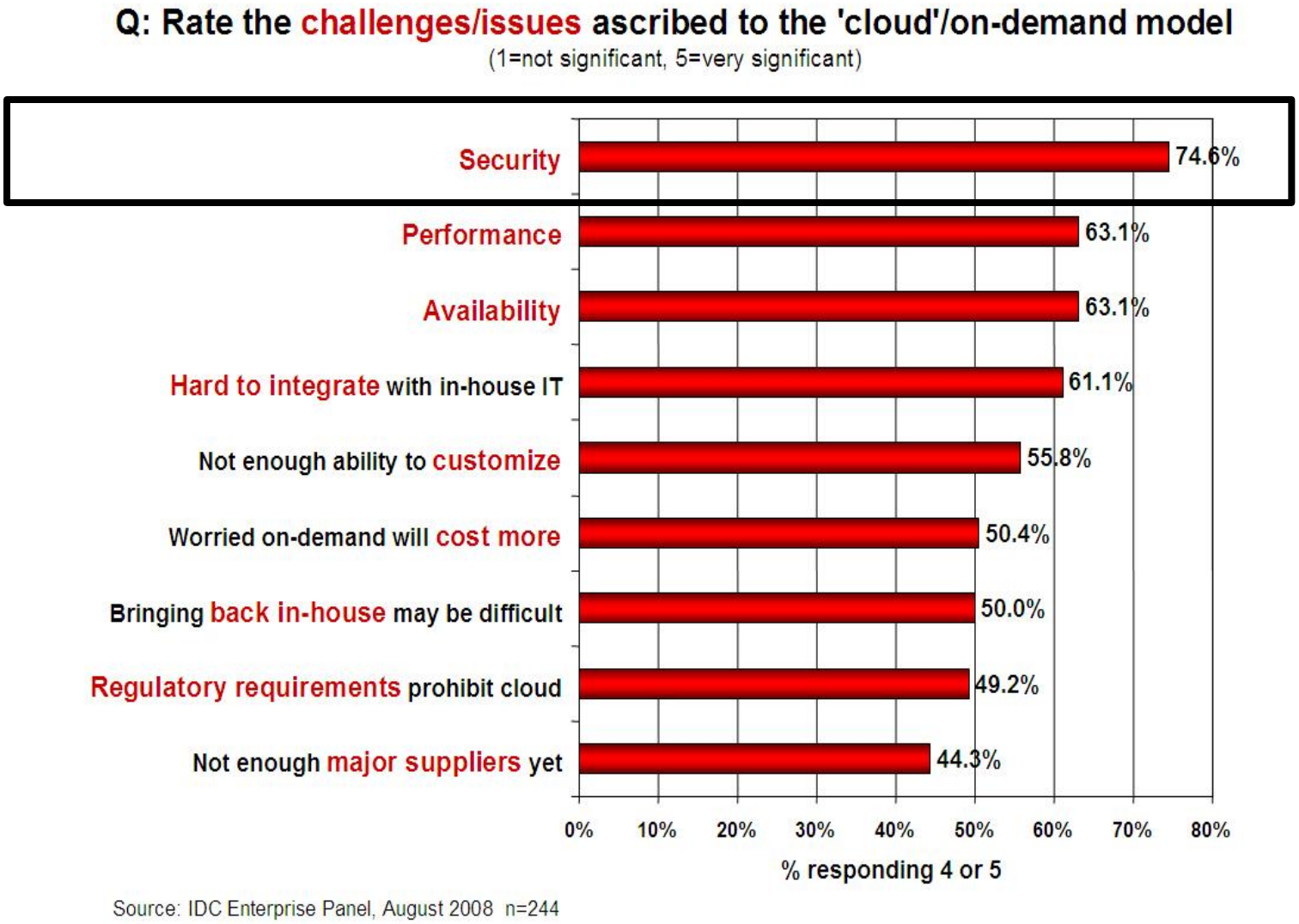
Marktentwicklung für Cloud-Computing in Deutschland



Quelle: Cloud Computing - Evolution in der Technik, Revolution im Business, BITKOM-Leitfaden, 2009

Fraunhofer SIT

Herausforderungen des Cloud-Computing



Fraunhofer SIT

Definition: Cloud-Computing

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

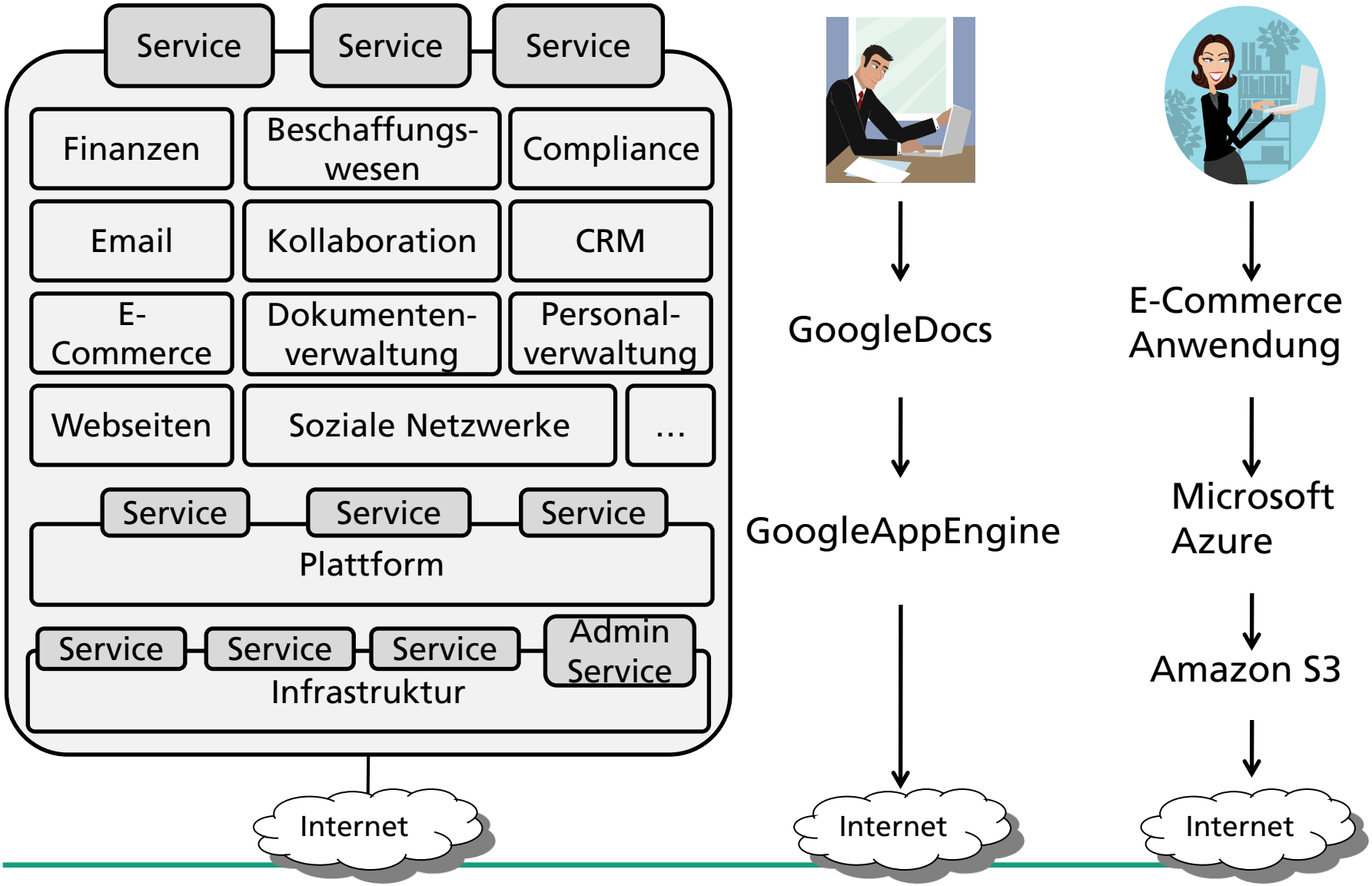
Cloud-Charakteristika

- Infrastrukturkomponenten wie CPU, Speicher, Netz werden bei Bedarf zur Verfügung gestellt
- „unendlich“ viele Ressourcen durch dynamische Hinzunahmen von Kapazitäten
- Zugriffe auf ausgelagerte Daten: jederzeit, von überall
- Einfache Erstellung von neuen Web-Anwendungen als Services, die über die Cloud global nutzbar gemacht werden können

Sicherheitsimplikationen der Cloud-Charaktersitika

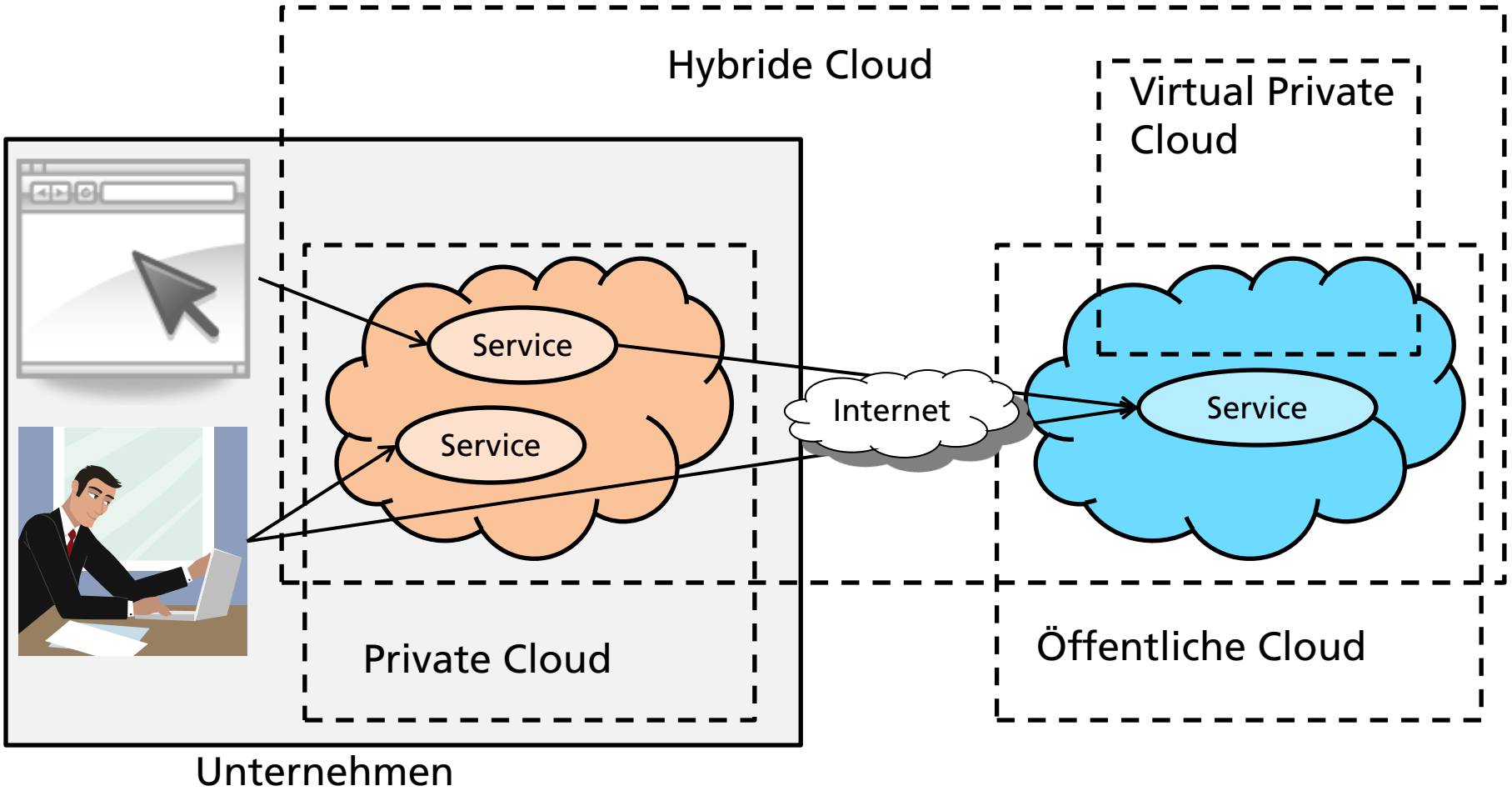
- Bereitstellung der Infrastrukturkomponenten
  - Wo werden die Daten gespeichert? Wie wird verschlüsselt?
  - Wie wird die Identitäts- und Zugriffsverwaltung durchgesetzt?
- „unendlich“ viele Ressourcen
  - Schutz der Privatsphäre vs. Abrechenbarkeit? Integrität der Daten?
- Einfache Erstellung von Services, globale Nutzung der Services
  - Vertrauenswürdigkeit der Cloud-Dienste?
  - Verwaltung von Zugriffsrechten, Schlüssel, Identitäten?
- Zugriffe auf ausgelagerte Daten: jederzeit, von überall
  - Verfügbarkeit? Denial-of-Service-Angriffe durch Botnetze?
  - Gefahr von Lock-in-Effekten?

Sicherheitsimplikationen Software-as-a-Service



Fraunhofer SIT

Sicherheitsimplikationen öffentliche/private Cloud



Sicherheitsimplikationen einer öffentlichen 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

Sicherheitsimplikationen einer privaten 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
- Kombination private und öffentliche Cloud: hybride Cloud
  - Problem: Klassifikation der Daten notwendig

Top 7 Bedrohungen der Cloud

(1) Missbrauch der Cloud-Ressourcen
(2) Unsichere Schnittstellen und APIs
(3) Bösartige Mitglieder und Eingeweihte
(4) Probleme gemeinsam benutzter Technologien
(5) Datenverlust und/oder Datenabfluss
(6) Übernahme des Benutzerkontos oder des Dienstes
(7) Unbekanntes Risikoprofil

Quelle: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Taxonomie der Sicherheitsaspekte

Ziel: Rahmen zur Bewertung der Cloud-Sicherheit
Ansatz: Taxonomie der sicherheitsrelevanten Bereiche
Vollständige Taxonomie: Cloud-Sicherheits-Studie
des Fraunhofer SIT, Sept.2009

Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen

- Infrastruktur
  - Physikalische Sicherheit
  - Host
  - Virtualisierung
  - Netzwerk
- Anwendung und Plattform
  - Datensicherheit
  - Anwendungs-sicherheit
  - Plattformsicherheit
  - Sicherheit als Service
- Verwaltung
  - Phasen der Servicenutzung
  - Prüfung
  - Identitäts- und Rechteverwaltung
  - Schlüsselverwaltung
  - Interoperabilität und Portabilität
- Compliance
  - Datenschutz
  - Risiko-management
  - Rechtlicher Rahmen
  - Governance

Fraunhofer SIT

Risikobewertung: Datensicherheit

Aus Sicht des Nutzer zu klären:

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

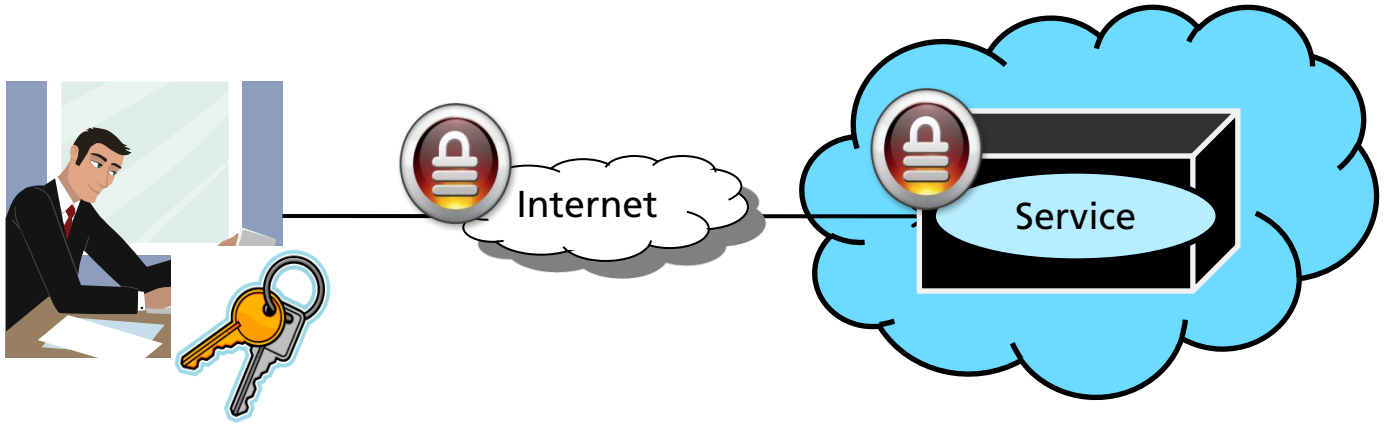
Maßnahmen für Datensicherheit durch SaaS oder IaaS Anbieter

- Sichere Übertragung und Speicherung der 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?

Risikobewertung: Datensicherheit

Modell 1: Datensicherheit ohne Garantien des Cloud-Serviceanbieters

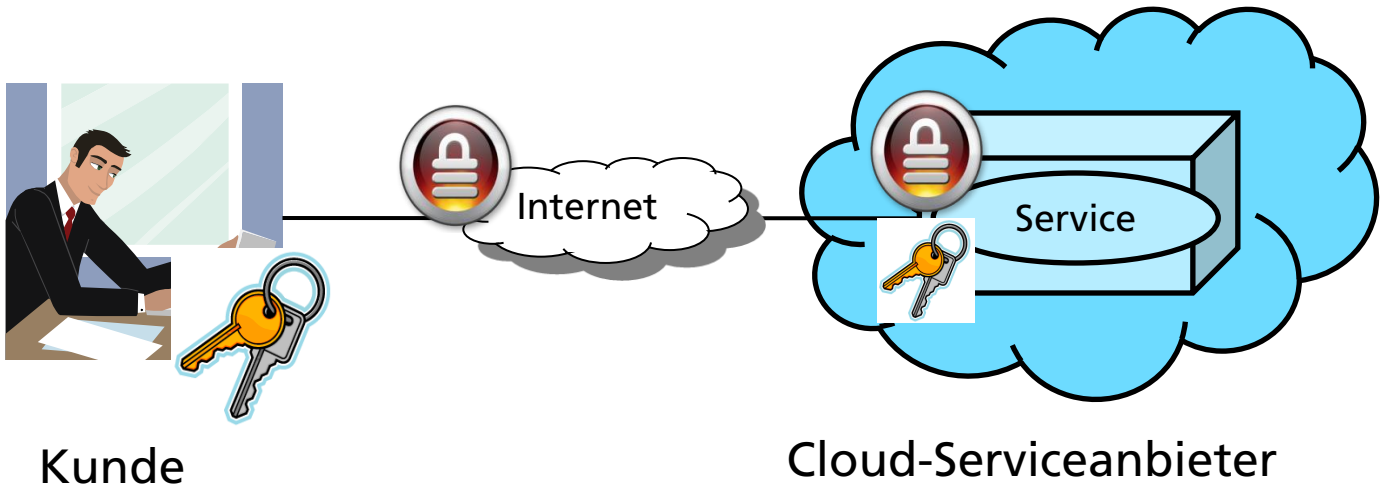
- Kunde muss alle Aktionen vor der unsicheren Cloud-Umgebung verstecken (z. B. durch Verschlüsslung oder durch Anwendung von „Security-by-Obscurity“)



Risikobewertung: Datensicherheit

Modell 2: Datensicherheit mit Garantien des Cloud-Serviceanbieters

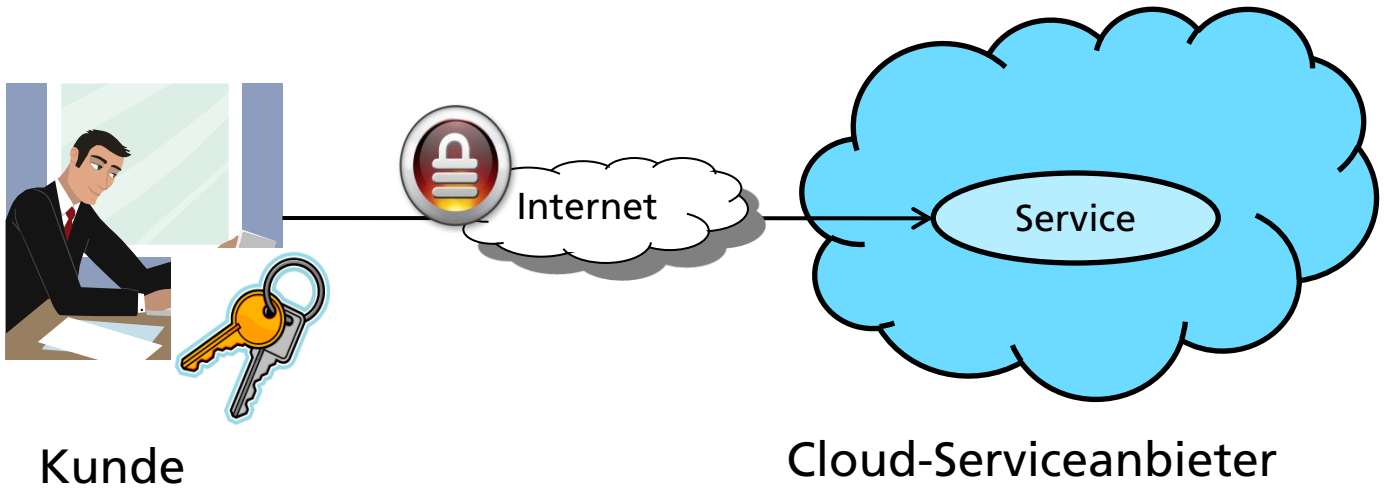
- Benutzung einer abgegrenzten Umgebung



Risikobewertung: Datensicherheit

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

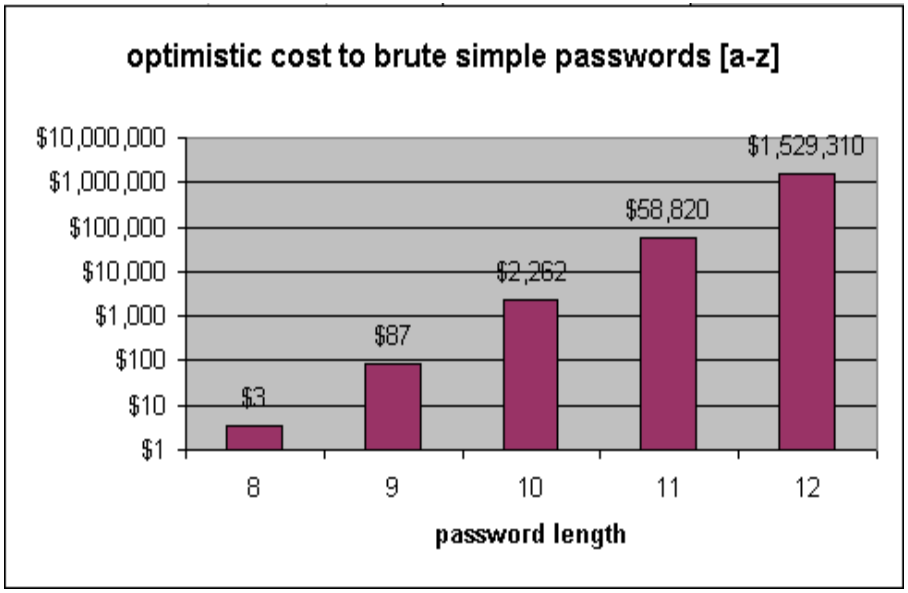
- Vertrauen in Zertifikate und Reputation des Anbieters

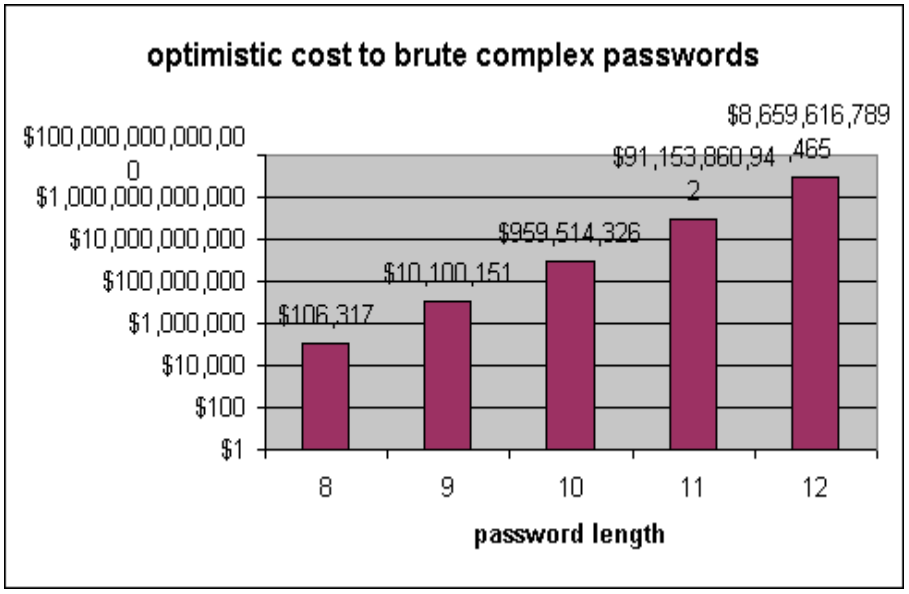


Risikobewertung: Bedrohungen der Datensicherheit

Beispiel: Schlüsselbrechen in der Cloud (10/2009)

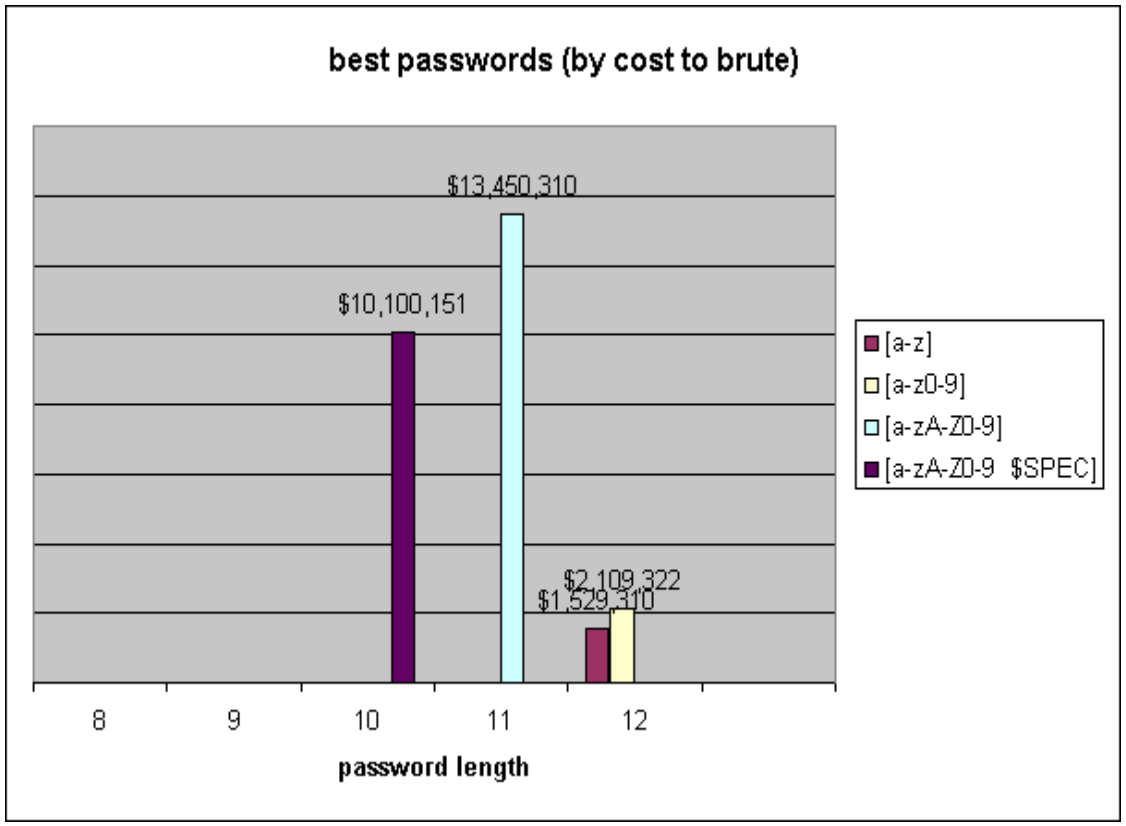
- Kosten für das Brechen eines PGP-Schlüssels mit der Software EDPR auf Amazon EC2 Ressourcen





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

Risikobewertung: Bedrohungen der Datensicherheit



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

Fraunhofer SIT

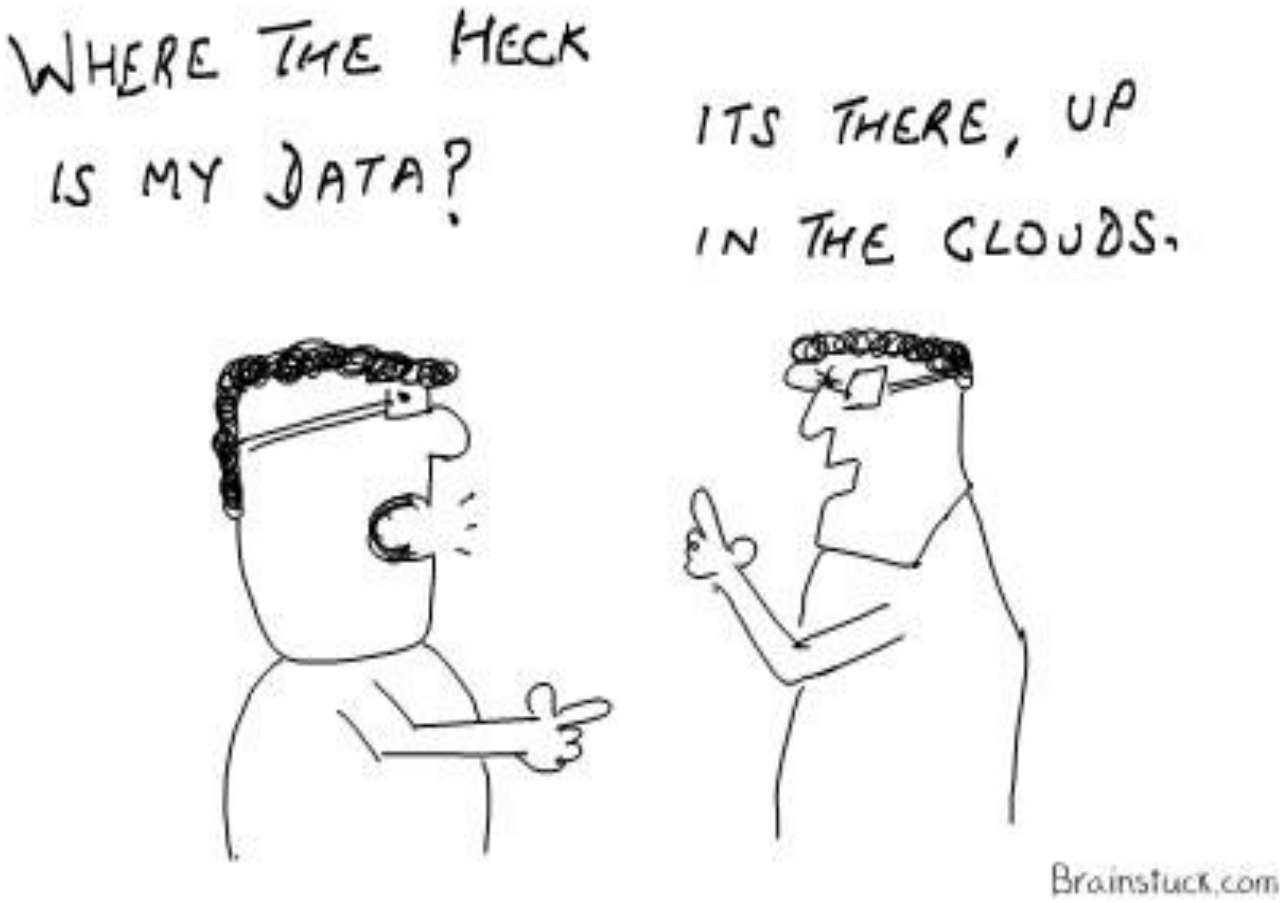
Die 10 Do‘s and Dont‘s der Cloud-Computing-Sicherheit

1. Anwendung eines gesamtheitlichen Sicherheitskonzepts
2. Integration in ein bestehendes Sicherheitskonzept
3. Herstellen einer Vertrauensbeziehung zwischen Cloud-Konsument und Cloud-Anbieter
4. Schutz der Netzinfrastruktur
5. Nutzung innovativer Sicherheitslösungen für Cloud-Computing-Systeme
6. (Wieder-)Verwendung von Basisdiensten
7. Beachtung von Lock-in-Effekten
8. Einfordern von Sicherheitszertifikaten und Sicherheitstestaten
9. Kein Verzicht auf Sicherheitskonzepte aus ökonomischen Überlegungen heraus
10. Einsatz von Service-Level-Agreements

Zusammenfassung

- Cloud-Computing: **Chancen** für Nutzer und Anbieter:
  - Kostenreduktion, innovative Geschäftsprozesse, …
- Cloud-Computing: Vielzahl von **Sicherheitsbedrohungen**
  - Bedrohung der Privatheit, Vertraulichkeit, Integrität, Verfügbarkeit
  - Bedrohungen durch Lücken bei der Aufteilung der Verantwortlichkeiten zwischen Nutzer und Anbieter
- SIT-Taxonomie als Rahmen für eine systematische **Bewertung der Sicherheitsrisiken**
  - **Grundlage** für die Ableitung von Maßnahmen
- Offene Fragen
  - Was wird sich an Technologienstandards durchsetzen?
  - Wie können Lock-In Effekte vermieden werden?

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