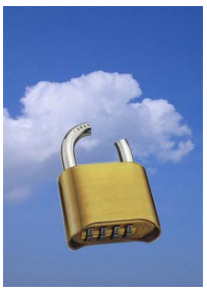
Cloud-Computing – eine Herausforderung für die Sicherheit



Claudia Eckert

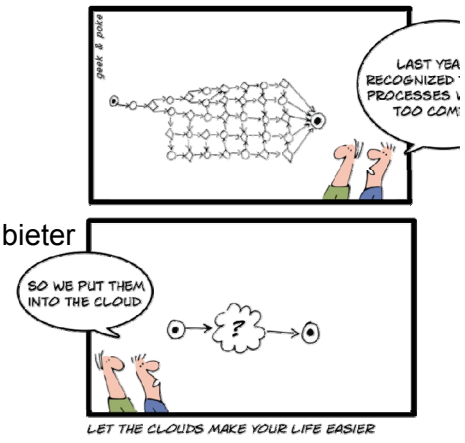
Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Technische Universität München

Zürich, 9.9. 2009

Übersicht

1. Motivation
2. Cloud-Computing
3. Cloud-Computing: Service Anbieter
4. Sicherheitsimplikationen
5. Risikobewertung
6. Zusammenfassung



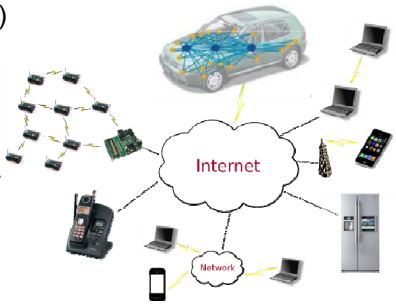
1. Motivation

Durchdringung unseres Alltags mit IT:

- „Informationstechnische Systeme sind allgegenwärtig und ihre Nutzung [ist] für die Lebensführung vieler Bürger von zentraler Bedeutung“.
- Grundrecht auf Vertraulichkeit und Integrität informations-technischer Systeme (BVerfG, BvR 370/07,27.2. 2008)

Internet der nächsten Generation:

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



9.9. 2009 Fraunhofer SIT 3

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

9.9. 2009 Fraunhofer SIT 4

2. Cloud-Computing

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

Cloud-Charakteristika

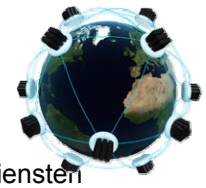
- Hardware-Komponenten, wie CPU, Speicher, Netz werden on-demand zur Verfügung gestellt,
  Nutzer muss keine eigene Infrastruktur betreiben
- ‚unendlich' viele Ressourcen durch dynamische Hinzunahme von Kapazitäten:
  Nutzer muss nicht im Voraus planen, kaufen, konfigurieren, …
- Einfache Erstellung 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: Chancen

Nutzer-Sicht:

- Kostenreduzierung u.a.
  - Bezahlung nur der verbrauchten Ressourcen
  - Bezug von IT-Kapazitäten bei Bedarf (skalierend)
- Verkürzung der Zeit zur Marktreife
  - Wiederverwendung bestehender Dienste, höhere Agilität/Flexibilität
- Neue Möglichkeiten in der Gestaltung von IT-Prozessen

Anbietersicht:

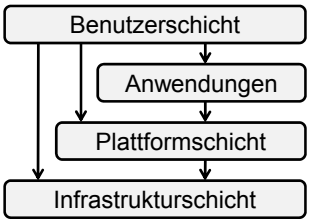


- Optimierung des Rechenzentrumsbetriebs
  - Automatisierung der administrativen Prozesse
  - Reduktion des Testaufwands bei einheitlicher Plattform
- Verkürzte Innovationszyklen bei der Bereitstellung von Diensten

2. Cloud-Computing: Schichten-Modell

Cloud-Angebote auf unterschiedlichen Schichten

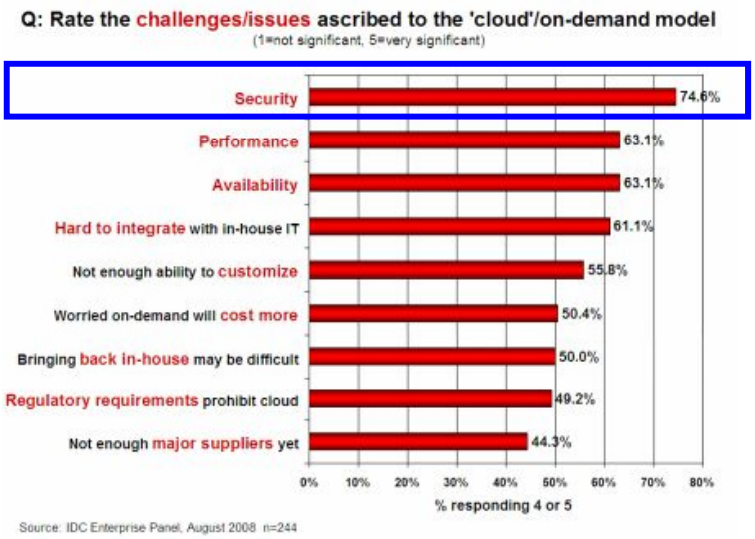
- Infrastructure as a Service (IaaS) (Rechner, Speicher)
  Beispiel: Elastic Compute Cloud von Amazon: stellt virtuelle Server zur Verfügung
- Platform-as-a-Service (PaaS)
  Beispiel: Google App Engine, force.com
  Entwickeln/Upload von Anwendungen
- Software as a Service (SaaS) (Mail, CRM, Textverarbeitung, …)
  Beispiel: Google Docs, GMail, gliffy



3. Cloud-Computing: Service-Anbieter

- **Amazon-Web-Services (IaaS-Ebene)**
  Elastic Compute Cloud, Simple Storage Services (AS3), Simple DB:
  – sehr flexibel nutzbar, low-level konfigurierbar durch Anwender
- **Google Apps Engine (PaaS-Ebene)**
  – Plattform zum Entwickeln und Hosten von Webanwendungen auf den Servern von Google
  – Nutzer können ihre eigenen Anwendungen hochladen und zur Nutzung zur Verfügung stellen
- **Salesforce (SaaS-Ebene)**
  – Anbieter von on-demand Geschäfts- und CRM-Anwendungen,
- **Google Docs (SaaS-Ebene)**
  – Kooperative, online Erstellung von Texten, Tabellen, Präsentationen in Echtzeit

2. Cloud-Computing: Herausforderungen



9.9. 2009 Fraunhofer SIT 9

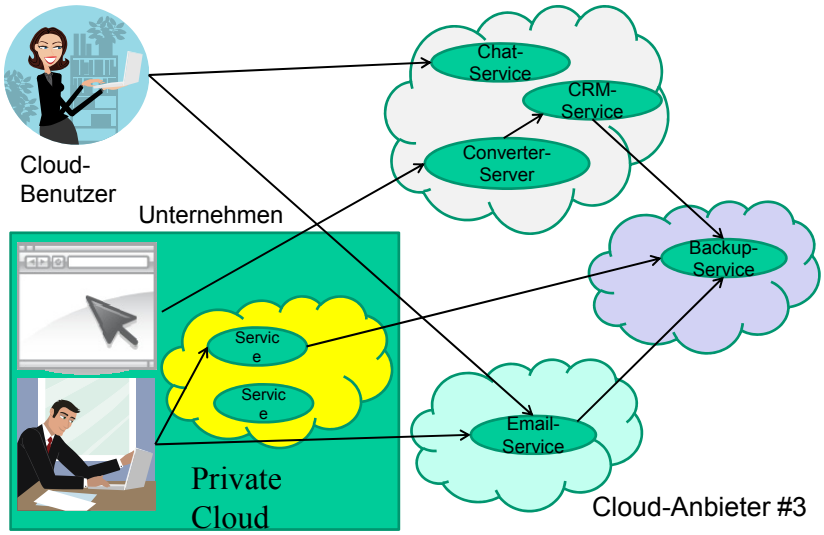
4. Sicherheitsimplikationen

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-Servce-Angriffe, Gefahr des Daten-Lock-in, ….

9.9. 2009 Fraunhofer SIT 10

4. Sicherheitsimplikationen: ein Szenario



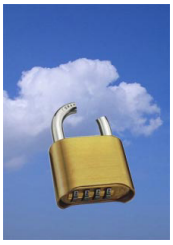
9.9. 2009 Fraunhofer SIT 11

4. Sicherheitsimplikationen: Vorfälle

CCI	Date	Product	Provider	Severity	Incident Type	Incident Sub-Type	Exploit	Affected
CCI-0006	2008-01-07	Salesforce.com	Salesforce.com	High	Outage	Network Outage	No	All
CCI-0005	2008-10-18	AWS Services	AWS	High	Security	Man-in-the-Middle	No	All
CCI-0004	2008-10-15	Gmail	Google	High	Outage	502 error	No	Unknown number of users
CCI-0002	2008-09-18	Google Docs	Google	High	Security	Session Hijacking	No	Some Thai Users
TBA	2008-09-15	App Engine	Google	Low	Outage	Performance Degradation	No	All
TBA	2008-09-02	Google Apps	Google	High	Security	User Impersonation	Yes [11]	All SSO users
TBA	2008-08-26	FlexiScale	FlexiScale	Critical	Outage	Disaster Recovery	No	All
TBA	2008-08-12	Gmail	Google	High	Outage	Change Management	No	Many
TBA	2008-08-08	The Linkup	Nirvanix MediaMax	Critical	Data Loss	Closure	No	20,000
TBA	2008-07-20	Amazon S3	AWS	Critical	Outage	Design Fault	No	All
CCI-0003	2008-07-10	MobileMe	Apple	Moderate	Outage	Migration	No	All
CCI-0003	2008-07-09	.Mac	Apple	Info	Outage	Scheduled Outage	No	All
TBA	2008-04-28	EC2	Amazon	Low	Outage	Degraded Performance	No	Small subset of instances
TBA	2008-02-15	Amazon S3	AWS	Low	Outage	Authentication Failures	No	All

9.9. 2009 Fraunhofer SIT Quelle: http://wiki.cloudcomputing.org/wiki/CloudComputing:Incidents_Database 12

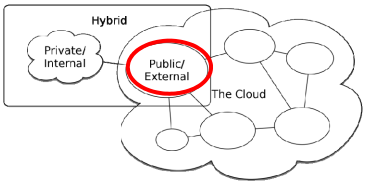
4. Sicherheitsimplikationen: Vorfälle



Bereits aufgetretene Probleme:

- Viele Verletzungen des Schutzziels Verfügbarkeit
  - Häufig sind alle Benutzer betroffen
- Durchgeführte Angriffe auf existierende Cloud-Dienste
  - Bekannte Angriffe auf Cloud-Dienste angewandt
    d.h. bekannte Schwachstellen Internetbasierter Dienste ausgenutzt
    Aber: durch interne Angreifer (Nutzer) höhere Risiken,
    größere Schäden
- **Beispiel** (07/2009): Diebstahl von Finanzdaten eines Twitter-Gründers
  - Auslöser: Ausspionieren des Passworts für Google Docs

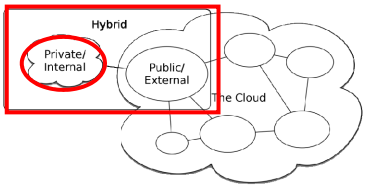
4. Sicherheitsimplikationen



Verschiedene Cloud-Modelle
Public Cloud

- Auswahl des Dienstes durch den Cloud-Nutzer
  - Wie erfüllt 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

4. Sicherheitsimplikationen



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 Ressourcenbenutzung leichter durchsetzbar

Aber: geringere Flexibilität, Skalierbarkeit, eingeschränkter Nutzerkreis

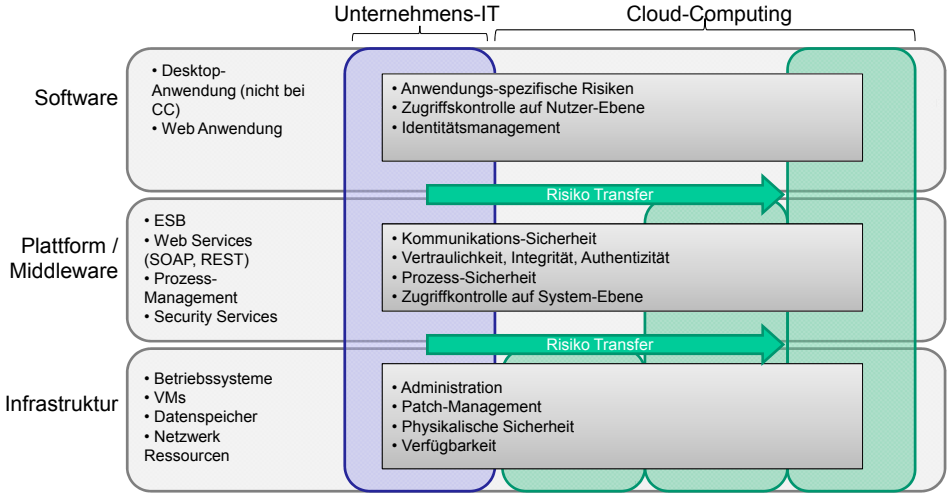
Hybride Cloud

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

9.9. 2009 Fraunhofer SIT 15

4. Sicherheitsimplikationen: Risikoverlagerung

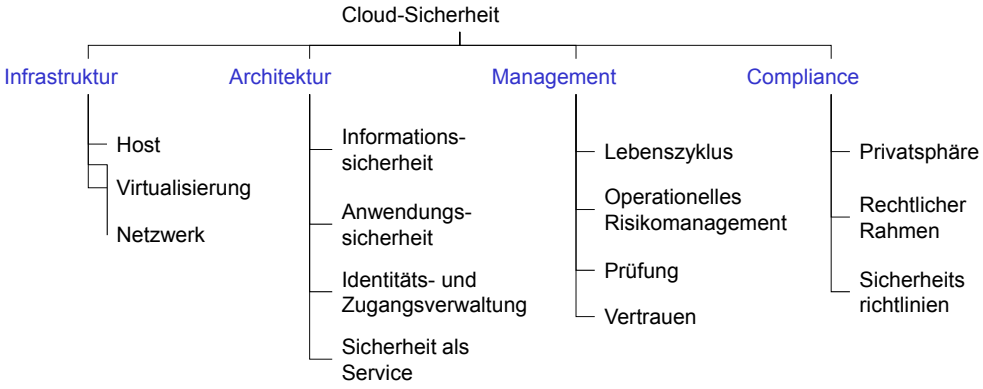
Auslagern von Diensten in die Cloud: Verlagerung der Risiken?



9.9. 2009 Fraunhofer SIT 16

5. Risikobewertung

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



5. Risikobewertung : Infrastruktur

Probleme:

- Nutzer hat idR keinen Einfluß, Risiken sind kaum bewertbar
- Nutzer muss Vertrauen in den Anbieter haben (Zertifiziert, Verträge, …)

- **Bedrohungen des Hosts**:
  - Bedrohung durch andere Rechenjobs auf gleichem Rechner,
  - Zugriff auf den Host durch Anbieter oder externen Angreifer,
  - fehlerhafte Ressourcenzuweisung, DoS (‚verhundern')

  Mögliche Sicherheitsmaßnahmen durch IaaS-Anbieter:
  - Überwachung und Dokumentation der Aktionen während der Ausführung
  - Isolation der Benutzerumgebungen durch Virtualisierung

5. Risikobewertung: Infrastruktur

- **Bedrohungen der Virtualisierungsschicht**
  - Verschieben von virtuellen Maschinen bzw. Verschieben oder Erstellen von Datenreplicas, so dass Privacy bedroht sein kann
  - Fehlerhafte Konfiguration bzw. Sicherheitslücken der Virtualisierungslösung: unberechtigte Zugriffe auf VM-Verwaltung

  Mögliche Sicherheitsmaßnahmen durch IaaS-Anbieter:
  - Überwachung der administrativen Prozesse des Anbieters
  - Zugriffsschutz durch privilegierte Nutzer z. B. auf den VMM
- **Bedrohungen des Netzwerks**
  - Alle klassischen Netzbasierten Angriffe

  Mögliche Sicherheitsmaßnahmen durch IaaS-Anbieter:
  - Verschlüsslung zwischen Benutzer und Anbieter, zwischen den Rechnern des Anbieters und allen weiteren beteiligten Akteuren
  - Maßnahmen gegen verteilte Denial-of-Service Angriffe

5. Risikobewertung: Architektur

Aus Sicht des Nutzer zu klären:

- welche Sicherheitsmaßnahmen werden eingesetzt, um die Service-Entwicklung und Nutzung abzusichern
- **Maßnahmen für Informationssicherheit 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), Replica-Verwaltung, Langzeitspeicherung, Speicherort, Löschung und Wiederherstellung ?
- **Maßnahmen zur Anwendungssicherheit**
  - Verwendung eines Entwicklungszyklus zur sicheren Programmierung?
  - Nur privilegierter Zugang zu Konfigurationsdateien?
  - Gegenseite Authentifizierung, föderierten Identitätsverwaltung?
  - Schutz der Privatsphäre durch z. B. die Verwendung von Pseudonymen?

5. Risikobewertung: Management

Aus Nutzersicht zu bewerten:

- welche Sicherheitsdienste bietet der Cloud-Anbieter für Service-Mgmt

u.a. Dienste zur

- **Absicherung der 4 Phasen des Lebenszyklus eines Cloud-Services**
  Anbahnung, Verhandlung, Ausführung, Kontrolle und Anpassung
  - Werden automatisiert prüfbare SLAs spezifiziert?
  - Gibt es Vertrauensnachweise des Anbieter z.B. über Zertifizierung?
  - Welche vertrauensbildenden Maßnahmen: TPM, Virtualisierung, Testate Zertifikate, werden verwendet?
- **Prüfung der sicherheitsrelevanten Ereignisse**
  - Können Prüfungsverfahren bei Vertragsabschluss festgelegt werden?
  - Sind Prüfpfade zum Nachweise der erbrachten Leistungen und möglicher Sicherheitsvorfälle implementiert?
  - Werden Prüfungen kontinuierlich durchgeführt?

5. Risikobewertung : Compliance

Zentrale Fragestellung: wie werden Datenschutzrechtliche Anforderungen vom Cloud-Anbieter erfüllt?

Basis: Nutzung eines Cloud-Services nach Bundesdatenschutzgesetz (BDSG) als "Datenverarbeitung in Auftrag" , d.h. Verantwortung für die Daten liegen beim Cloud-Nutzer als Auftraggeber!

- **Datenschutzkonforme Cloud-Dienste?**
  - Daten müssen in einem nach BDSG vertrauenswürdigem Land gespeichert werden, Weitergabe in nicht-vertrauenswürdiges Drittland ist verboten: vertragliche Regelungen, Garantien des Anbieters?
  - BDSG u.. EU-Datenschutzrecht: Ort der Daten kann jederzeit festgestellt werden: Verteilung in der Cloud transparent? Anbieter-Garantie?

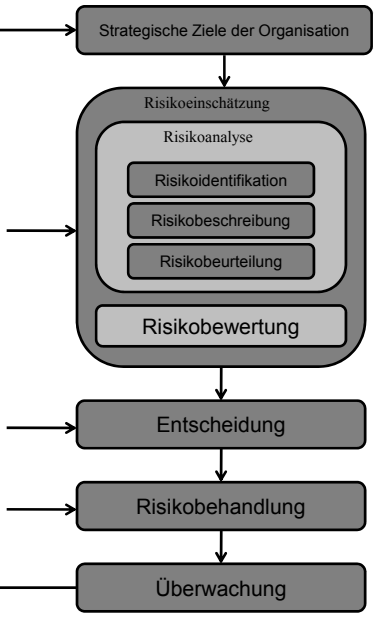
5. Risikobewertung: Compliance

Weitere Problembereiche: Risiken für den Nutzer:

- Einschränkungen des Einsatzes von Cloud-Computing-Systemen durch weitere gesetzliche Regelungen:
  - Alle Daten, die durch eigene Gesetze geregelt werden wie
    - Gesundheitsdaten, Daten bestimmter Berufsgruppen (Anwälte, Priester, etc.) oder Steuerdaten
  - Exportbeschränkungen für kryptografische Verfahren
- Gesetzliche Rahmenbedingungen bei Einstellung des Service oder bei Übernahme durch eine andere Firma
  - Schutz der Daten weiterhin gewährleistet? Welche Maßnahmen sind vorgesehen?

5. Risikobewertung: Fazit

- Vielfältige Risiken bei der Nutzung von Cloud-Services
- Einer Cloud-Nutzung sollte eine **Risiko-Analyse** vorangehen
- Die **Risiko-Behandlung** muss sich an den unternehmerischen Zielen orientieren:
  - Akzeptanz durch Nutzer
  - Risikovermeidung: nur unsensible Daten in die Cloud transferieren
  - Reduktion: zusätzliche Sicherheitsverfahren, z.B. Verschlüsselung, Security aaS
  - Risikotransfer: z.B. bezahlen einer Versicherungsprämie, spezielle Verträge



6. 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 Sicherheit heutiger Cloud-Angebote:

- In **IaaS** sind bereits einige Sicherheitsdienste im Einsatz
- **PaaS, SaaS:** Standards, Sicherheitsanalysen und Zertifikate fehlen
- **SLAs** meist nur mit minimalen Garantien, unzureichend für Risikotransfer

Offene Fragen: u.a.

- Standardisierte Technologien und Prozesse: was wird sich durchsetzen?
- Interoperabilität/Portabilität von Services: Lock-in-Effekte vermeiden?

Vielen Dank für Ihre Aufmerksamkeit

Claudia Eckert
Fraunhofer-Institut SIT
Parkring 4
D-85748 Garching bei München
E-Mail: claudia.eckert@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de