



Sicherheit – die Herausforderungen beim Outsourcing

Rolf Oppliger / 29. August 2012



Übersicht

- Einleitung
- #1: Kontrolle und Verfügbarkeit
- #2: Vertraulichkeit
- Vertrauen: Trust vs. Confidence
- Schlussfolgerungen und Ausblick



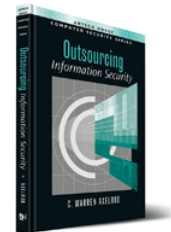
Einleitung

- **Outsourcing** ≈ Auslagerung einer Tätigkeit oder eines Arbeitsprozesses an einen Dritten (Diensteanbieter)
- In unserer arbeitsteiligen Welt ist Outsourcing allgegenwärtig (zunehmend auch in der IKT)
- **Cloud Computing** ≈ dienst-zentrierte Form des IKT-Outsourcings (vgl. Referat von Prof. Lubich)
- Weil a priori nicht klar ist, in welchen Rechenzentren und auf welchen Computersystemen Daten beim Cloud Computing gespeichert und bearbeitet werden, kommen neue Sicherheitsfragen hinzu



Einleitung

- Es gibt viele Studien zur Sicherheit im IKT-Outsourcing bzw. Cloud Computing
 - European Network and Information Security Agency (ENISA)
 - Cloud Computing Benefits, Risks and Recommendations for Information Security (November 2009)
 - Security & Resilience in Governmental Clouds (Januar 2011)
 - Cloud Security Alliance (CSA)
 - Security Guidance for Critical Areas of Focus in Cloud Computing (Version 3.0, 2011)





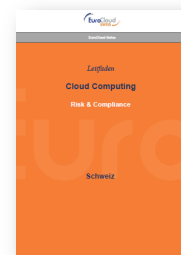
Einleitung

- Fraunhofer-Gesellschaft
 - Einrichtung für Angewandte und Integrierte Sicherheit (AISEC)
 - Cloud Computing Sicherheit Schutzziele, Taxonomie, Marktübersicht (September 2009)
 - Institut für Sichere Informationstechnologie (SIT)
 - On the Security of Cloud Storage Services (März 2012)
 - Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS)
 - Cloud-Computing für die öffentliche Verwaltung (ISPRAT-Studie, November 2010)



Einleitung

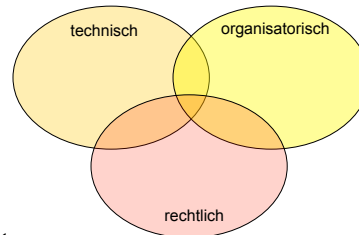
- EuroCloud Swiss
 - Leitfaden «Cloud Computing - Risk & Compliance» (März 2012)
- National Institute of Standards and Technology (NIST)
 - Special Publication 800-144 «Guidelines on Security and Privacy in Public Cloud Computing» (Dezember 2011)





Einleitung

- Das ISB erarbeitet zur Zeit auch eine konsolidierte Risikoanalyse
- Die Risiken sind technischer, organisatorischer und/oder rechtlicher Art
- Zentrale Problemfelder bzw. Herausforderungen
 - Kontrolle und Verfügbarkeit
 - Vertraulichkeit



#1: Kontrolle und Verfügbarkeit

- Wer seine Datenbearbeitung auslagert, verliert die (alleinige) Kontrolle und wird vom Dienstleister abhängig
- Diese Abhängigkeit betrifft insbesondere auch die Verfügbarkeit, d.h. die Daten sind nur solange verfügbar, wie der Dienstleister das will
- Weil der Dienstleister möglicherweise einem anderen Rechtssystem untersteht und sich dieses ändern kann, können unerwartete Probleme entstehen (vgl. «Das Mädchen und die Cloud» in: digma 2012, Seite 28)

→ Vertrauen!



#2: Vertraulichkeit

- Die Bearbeitung von Daten bedingt normalerweise, dass die Daten im Klartext vorliegen (Ansätze, wie Fully Homomorphic Encryption oder Secure Multiparty Computation, sind nicht praktikabel)
- Entsprechend hat der Dienstanbieter Einsicht in die Daten
- Daraus können Vertraulichkeitsprobleme entstehen

→ Vertrauen !



Vertrauen: Trust vs. Confidence

- Vertrauen ist ein Begriff, der die Menschheit seit jeher begleitet hat, und dem im Rahmen von Outsourcing bzw. Cloud Computing eine zentrale Bedeutung zukommt
- Dabei ist der Begriff nur schwer fassbar und «schwammig» definiert
- Im angelsächsischen Sprachraum unterscheidet man zwei Formen bzw. Ausprägungen
 - Vertrauen im Sinne von «Trust»
 - Vertrauen im Sinne von «Confidence»



Vertrauen: Trust vs. Confidence

- **Trust** ≈ Bereitschaft, sich in Erwartung eines positiven Ausgangs und im Glauben in etwas (z.B. Person oder System) verletzlich zu machen
- Charakteristische Eigenschaften
 - subjektiv
 - nicht auf messbaren Beurteilungsgrundlagen und -kriterien basierend (→ nicht wissenschaftlich)
 - zukunftsorientiert
- Wer im Sinne von «Trust» vertraut, macht sich vom zukünftigen Verhalten einer Person oder eines Systems abhängig → Risiken

In
God
We
Trust



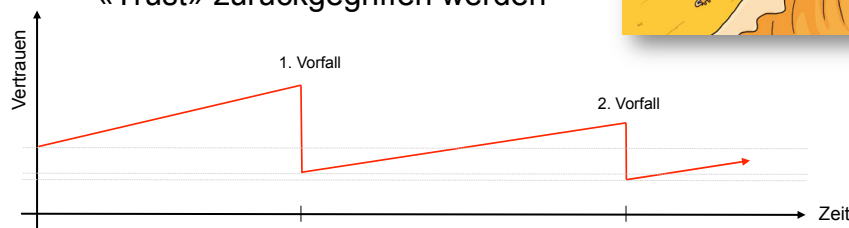
Vertrauen: Trust vs. Confidence

- **Confidence** ≈ auf Erfahrung und Evidenz basierender Glaube, dass gewisse zukünftige Ereignisse wie erwartet eintreten (≈ Zuversicht)
- Charakteristische Eigenschaften
 - objektiv
 - auf messbaren Beurteilungsgrundlagen und -kriterien basierend (→ wissenschaftlich)
 - vergangenheitsorientiert
- Grundlage für den Aufbau von «Confidence» sind statistische Aufzeichnungen und Auswertungen



Vertrauen: Trust vs. Confidence

- Idealerweise stellt Vertrauen im Sinne von «Confidence» die Basis für eine Zusammenarbeit dar
- Wenn Vertrauen im Sinne von «Confidence» (noch) nicht existiert oder verloren gegangen ist, muss auf Vertrauen im Sinne von «Trust» zurückgegriffen werden



Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

Sicherheit im Outsourcing / Rolf Oppliger / 29. August 2012

13



Vertrauen: Trust vs. Confidence

- Der Aufbau von Vertrauen (im Sinne von «Confidence») erfordert Zeit und ein Ausbleiben von grösseren Vorfällen
- Dabei kann nur der zweite Punkt direkt beeinflusst werden
- In der Zwischenzeit ist man auf vertrauensbildende Massnahmen angewiesen
 - Expertengutachten
 - Öffentlichkeitsarbeit
 - ISO/IEC 27001:2005-Zertifikate
 - Andere Zertifikate



Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

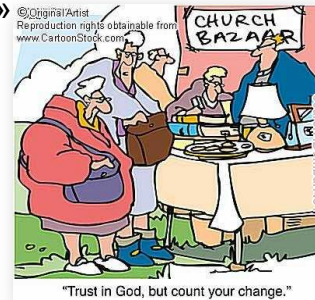
Sicherheit im Outsourcing / Rolf Oppliger / 29. August 2012

14



Schlussfolgerungen und Ausblick

- Viele Sicherheitsfragen im Outsourcing bzw. Cloud Computing lassen sich nicht schlüssig beantworten und führen unweigerlich zu einer Vertrauensfrage
- Vertrauen im Sinne von «Confidence» wäre zwar wünschenswert, in der Praxis ist aber leider oft nur Vertrauen im Sinne von «Trust» möglich
- Vertrauen ist gut, Kontrolle wäre besser!
- Die Verantwortung bleibt in jedem Fall beim Datenherrn



Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

Sicherheit im Outsourcing / Rolf Oppliger / 29. August 2012

15

