Bundesministerium
des Innern

Cloud Computing aus Sicht von Datensicherheit und Datenschutz

Peter Batt

Bundesministerium des Innern
Ständiger Vertreter des IT-Direktors

Berlin, den 19. April 2012

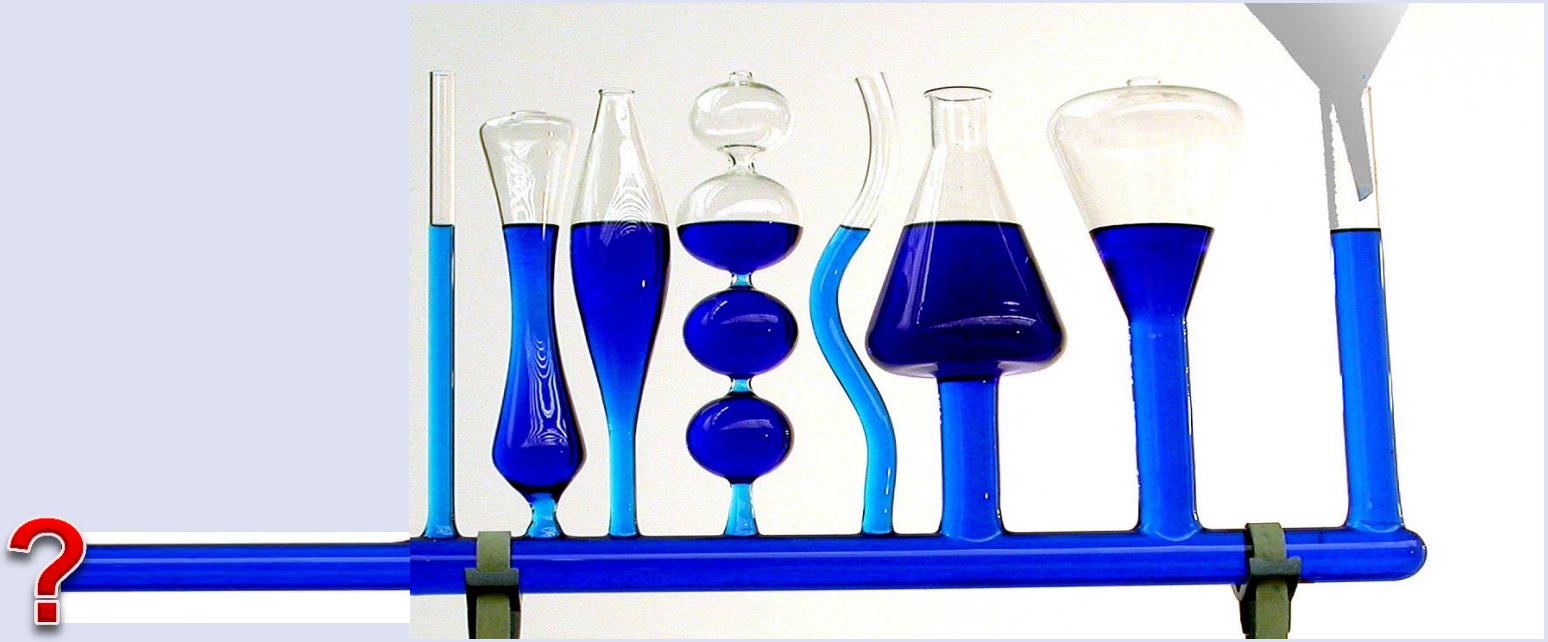
Grundlagen: Sicherheitsempfehlungen des BSI

- Für Anbieter und Nutzer
- Im Dialog mit der Wirtschaft entstanden
- Grundlagen
- Angemessene Sicherheitsempfehlungen
  - Gegliedert in 10 Kapitel
  - Praxisnah
  - mit vertretbarem Aufwand umsetzbar
  - Organisatorische + personelle + technische Maßnahmen
- Ein Kapitel Datenschutz (vom BfDI verfasst)

Strukturierung der Sicherheitsmaßnahmen im Eckpunktepapier

- Sicherheits-management beim Cloud-Anbieter
- Sicherheitsarchitektur
- ID- und Rechtemanagement
- Kontrollmöglichkeiten für Nutzer
- Monitoring und Security Incident Management
- Notfallmanagement
- Portabilität und Interoperabilität
- Sicherheitsprüfung und -nachweis
- Anforderungen an das Personal
- Vertragsgestaltung
- Datenschutz und Compliance

Je wolkiger, umso billiger
Je kontrollierter, umso sicherer
– aber auch teurer



experimente.phys.ethz.ch

Was hindert ?

Worum geht es ?

„ **SCHNEIDER:** Wir stehen als Versicherer mit Compliance und Data Protection vor zwei riesigen Herausforderungen. ***Ich habe überhaupt keine Lust, von irgendeinem Provider abhängig zu sein***, wenn es um die Verbindung zu unseren Daten geht.

HAUPTER: Ich will Sie keineswegs davon überzeugen, dass Public Cloud die einzige Lösung ist. Cloud verändert die Art, wie IT ausgeliefert wird, nämlich als Services. ***So*** wie wir diese Cloud-Services anbieten, ***können Sie selbst entscheiden, ob sie und welche Dienste beziehungsweise Anwendungen Sie in Ihren eigenen Rechenzentren betreiben.*** "

http://www.computerwoche.de/management/it-strategie/2368976/

Auswahl notwendiger Sicherheitsmaßnahmen (1/2)

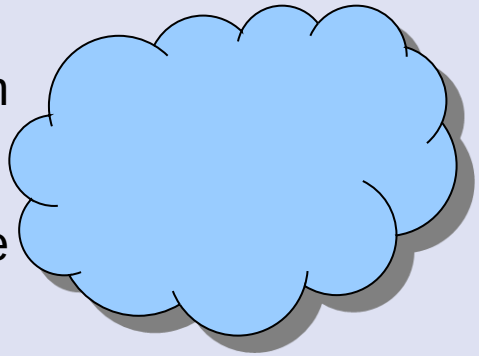
- Implementierung eines international anerkannten ISMS z. B. basierend auf IT-Grundschutz
- Aufbau einer Sicherheitsarchitektur zum Schutz der Ressourcen (Gebäude, Netze, Server, etc.)
- Robuste Trennung der Cloud-Anwender auf allen Ebenen des Cloud Computing Stacks
- Sichere und vollständige Löschung aller Daten (gemäß Vertrag)
- Zwei-Faktor-Authentisierung für Administratoren der Cloud ggf. auch für Nutzer
- Bereitstellung geeigneter Schnittstellen zur Überwachung der SLAs

Auswahl notwendiger Sicherheitsmaßnahmen (2/2)

- 24/7 Umfassende Überwachung der Cloud-Dienste und zeitnahe Reaktion
- Portabilität der Daten (kein Vendor Lock-in)
- Unterstützung von Standards (Interoperabilität)
- Regelung aller Sicherheitsleistungen in einem SLA
- Kontinuität der Geschäftsprozesse auch bei Insolvenz
- Offenlegung der Standorte, Subunternehmen
- Transparenz über staatliche Einsicht- und Eingriffsrechte
- Vertrauenswürdiges und geschultes Personal
- Schutz personenbezogener Daten gemäß BDSG

IT-Grundschutz und Cloud Computing

- Ziel: Volle Integration Cloud-spezifischer Anforderungen in IT-Grundschutz und Zertifizierbarkeit von Cloud-Angeboten nach ISO 27001 auf Basis von IT-Grundschutz
- Ergänzung des BSI-Standards 100-2 um Cloud-spezifische Aspekte wie z. B. Virtualisierung mit hoher Dynamik und Vernetzung
- Erstellung diverser IT-Grundschutz-Bausteine wie z. B.
  - Cloud-Nutzung
  - Cloud-Management
  - Web Services
- Probeevaluierung bis Ende 2012



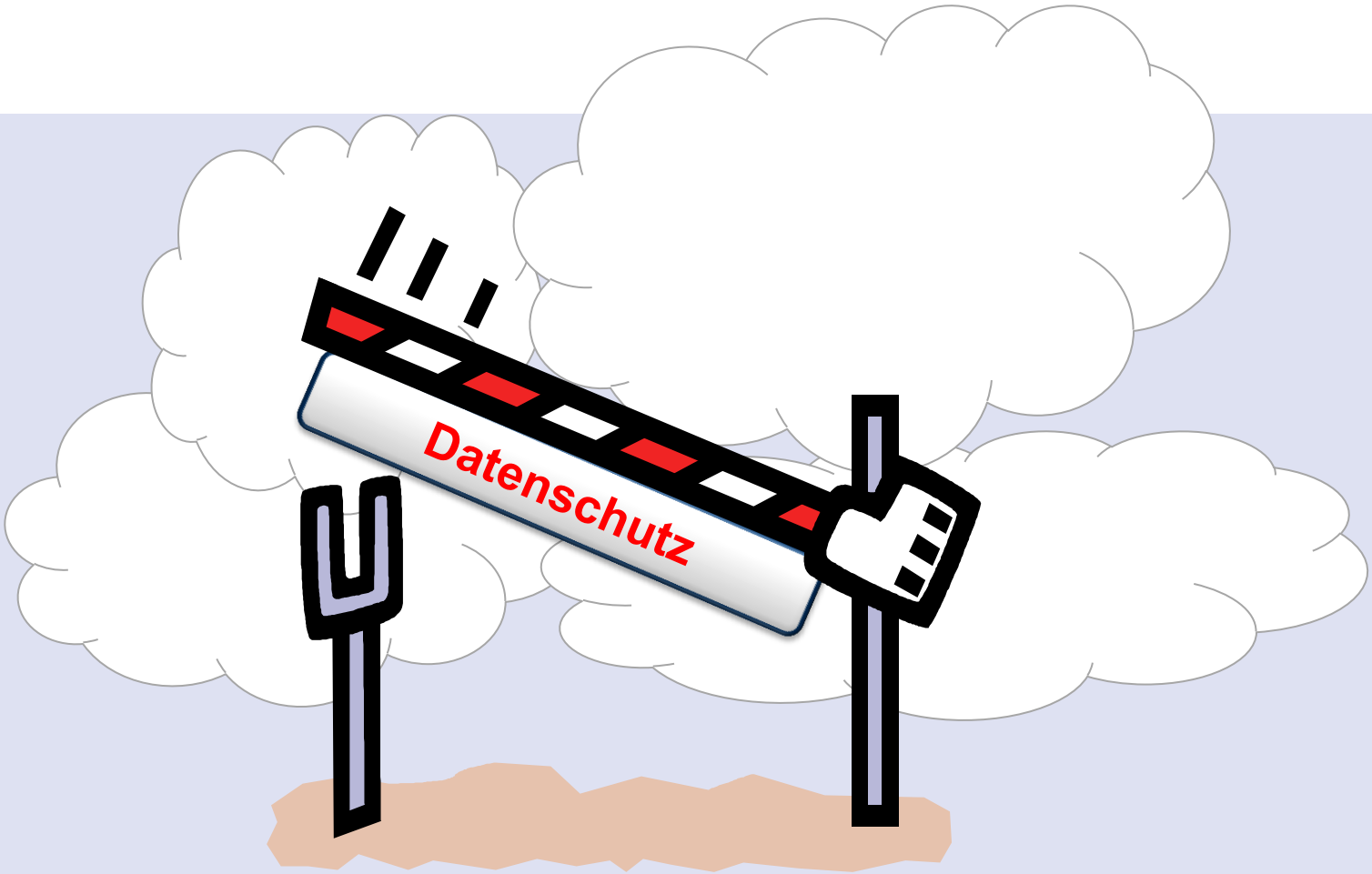
Zertifizierung von Cloud Diensten - Ziel

- Ziele der Zertifizierung:
  - Vergleichbarkeit der (Sicherheits-) Angebote von Cloud Diensteanbietern
  - Einhaltung der Anforderungen an Integrität, Vertraulichkeit und Verfügbarkeit der Daten gemäß Nutzeranforderungen und/oder gesetzlicher Vorgaben (z.B. Datenschutz)
- Aufgrund unterschiedlicher Nutzeranforderungen branchenspezifischer Ausprägung, z.B. für
  - die Versicherungswirtschaft


DIE DEUTSCHEN VERSICHERER
GDV
<Branche 2>
<Branche 3>
<Branche n>
Bundesamt
für Sicherheit in der
Informationstechnik
Grundschutz

Bundesministerium
des Innern

Cloud Computing und Datenschutz



Datenschutz in Deutschland

- Wettbewerbshindernis ?
- Qualitätsmerkmal ?
- Geltung für internationale Unternehmen ?
- Überholte Konzepte ?
- Selbstregulierung !?

EU-Datenschutz
Verordnungsentwurf

- Harmonisierung !
- Verbot mit Erlaubnisvorbehalt ?
- „Meine Daten gehören mir ?“
- Bereichsspezifika ?
- Internationale Vereinbarungen ?
- Die Katze im Sack ?

Cloud Computing aus Sicht Datensicherheit und Datenschutz

Danke für Ihre Aufmerksamkeit!