



synergetic AG Open House 2011

Rechtssicherheit statt
Wolkenkuckucksheim –
Rechtliche Anforderungen und
Lösungen des Cloud Computings

Ein Überblick über diese Themen

Markus Krämer

- CEO synergetic AG
- Verantwortlich für Strategie, Business Development und ISP Produktentwicklung innerhalb der synergetic Gruppe
- 1993 einer der Gründer von synergetic
- Bis 2000 Geschäftsführer der synergetic, seit 2000 nach der Umwandlung zur synergetic AG Vorsitzender des Vorstands (CEO)
- Heute werden nahezu 80.000 ISP-Kunden am Standort Wendlingen betreut, davon nutzen heute bereits ca. 10.000 Kunden Cloud-Services



Rechtssicherheit vs. Cloud Computing

**Zu Risiken und
Nebenwirkungen von
Cloud Computing lesen
Sie bitte die SLAs und
fragen Sie Ihren
Provider oder
Rechtsanwalt.**



Was ist Cloud Computing?

Cloud Computing ist der Ansatz, abstrahierte IT-Infrastrukturen dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen.

Hierbei kann es sich um Infrastrukturen (IaaS), Rechenkapazität, Speicherplatz, Applikationen (SaaS) oder beliebig andere Dienste (XaaS / Everything as a Service) handeln – also nahezu das komplette Spektrum der Informationstechnik.

„Cloud Computing“ steht also dafür, *alles* als dynamisch nutzbaren Dienst in der Wolke Internet zur Verfügung zu stellen und zu nutzen.



Cloud Computing zusammengefasst

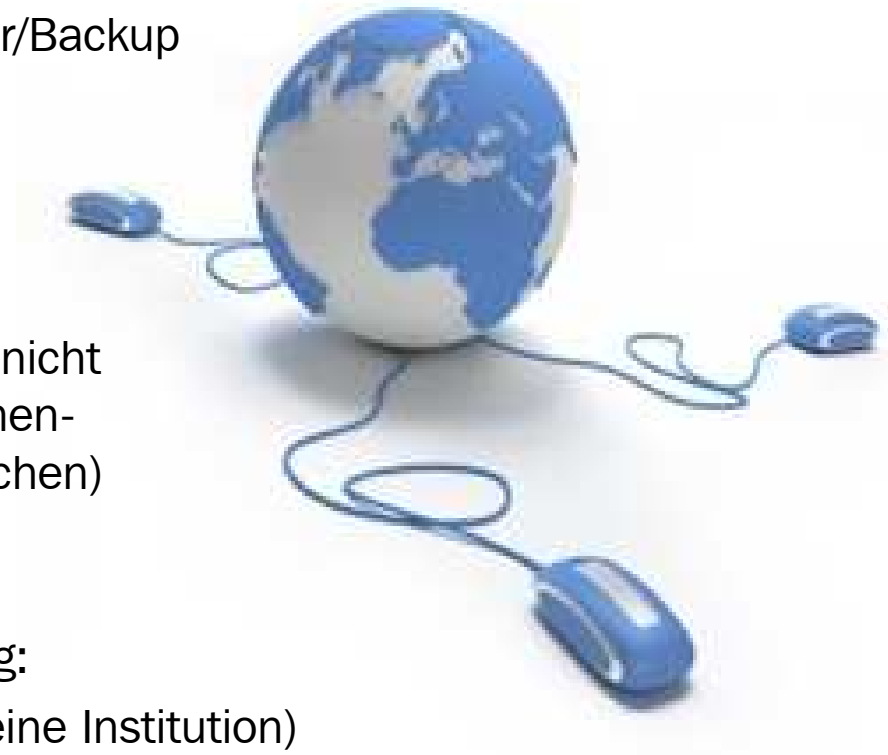
Die herkömmliche IT-Landschaft wird als Dienst gemietet:

- Rechenzentrumsbetrieb/Infrastruktur
- Hardware/Server und/oder Datenspeicher/Backup
- Software/Anwendungen wie Mail- oder Kollaborationssoftware
- Spezialsoftware wie CRM oder BI

Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der (metaphorischen) Wolke (engl. „Cloud“).

Typische Liefermodelle von Cloud Computing:

- Private Cloud (Z.B. Infrastruktur nur für eine Institution)
- Public Cloud (Z.B. Services für die Allgemeinheit)
- Hybrid/Community Cloud (Mischformen)



Cloud Computing in der Praxis – Wer nutzt bereits Cloud Computing?

Wer hat seine kompletten IT-Infrastrukturen noch Inhouse?

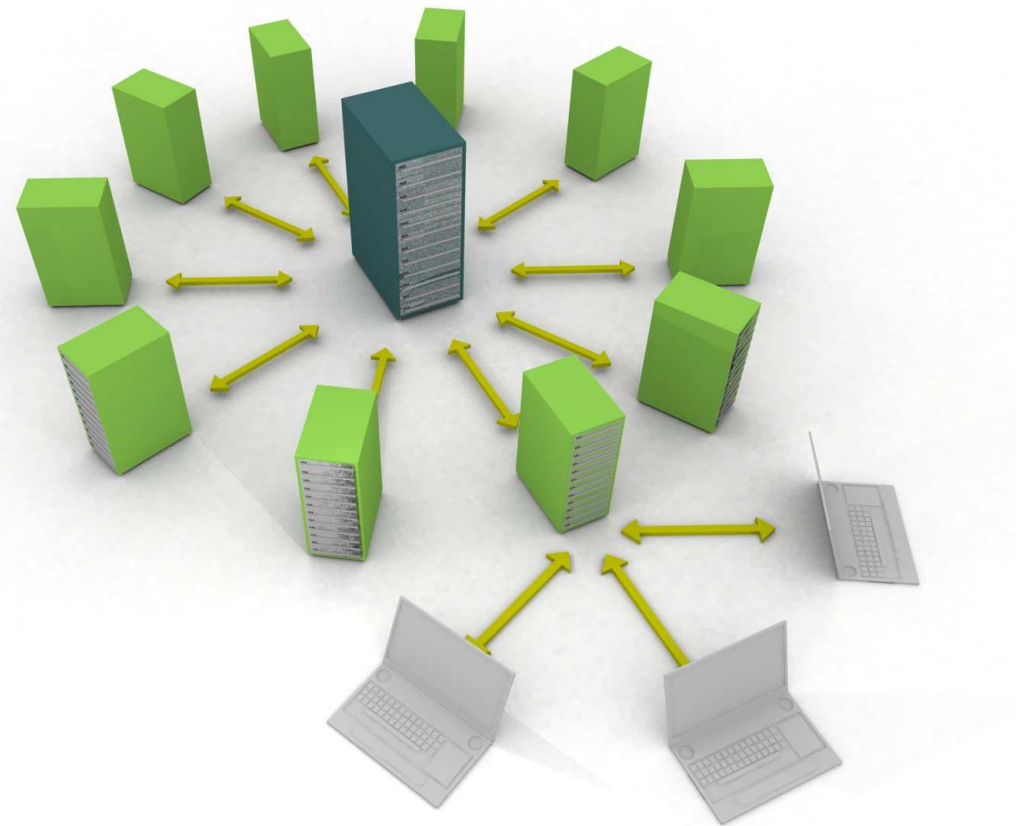
- E-Mail/ISP-Services
- Anbindungen/Standortvernetzungen

Wer nutzt IT-Outsourcing?

- Auslagerung von IT-Teilfunktionen
- Auslagerung der gesamten IT

Wer ist schon in der Cloud?

- Website/Web-Applikationen
- Hosted Exchange Server
- Hosted CRM
- Hosted CMS
- Backup



Rechtsfragen bei Cloud Computing...

Kontrolle

Compliance

Auftragsdatenverarbeitung

Wem gehören die
Daten?

Assetmanagement

Sicherheit

Datenschutz

Risikomanagement

Mögliche Risiken bei Cloud Computing

Risiken beim Auftragnehmer

- Eingeschleuste Schadprogramme/Trojaner
- Unsichere Schnittstellen
- Zugriff auf sensible Daten/unberechtigte Zugriffe
- Gelöschte Daten
- Verletzung von Richtlinien/Rechtsordnungen
- Diebstahl und Entwendung von Accounts

Risiken beim Auftraggeber

- Missbrauch durch unternehmensinterne Vertrauenspersonen
- Haftung der Sicherheitsverantwortlichen
- Datenverlust/Kontrollverlust über Daten
- Unzureichendes Risikomanagement
- Lock-In-Effekt (Wechseln des Anbieters)



Mögliche rechtliche und vertragliche Anforderungen bei Cloud Computing

Allg. Anforderungen

- Sicherheit und Risikomanagement
- Verfügbarkeiten/Quality of Service
- Compliance

Anforderungen Datenschutz

- Haftung der Sicherheitsverantwortlichen
- Speicherung personenbezogener Daten
- Auftragsdatenverarbeitung nach § 11 BDSG
- Eventuelle Internationalität

Anforderungen Vertragsrecht

- Mietrechtliche Regelungen/Garantien/SLA
- Unterauftragsverhältnisse (Subunternehmer)
- Lizenz-/Assetmanagement



Cloud Computing – Anforderungen an Sicherheit und Risikomanagement

Anforderungen an die Sicherheit und das Risikomanagement

- Typische Risiken und Sicherheitsanforderungen:
 - Ausfall der Verfügbarkeit: Geschäftsbetrieb steht/ist massiv gestört
 - Gravierende Fehler: Geschäftsbetrieb ist gestört
 - Datenverlust/Datenwiederherstellung
 - Datendiebstahl/Datenmanipulation
 - Unautorisierte Datenlöschung
- Minimierung der Verwundbarkeiten der IT bspw. nach ISO 17799/27000 oder dem IT-Grundschutz-Katalog:
 - Implementierung zu begründender Schutzmaßnahmen zur Sicherstellung fortgesetzter IT-Services innerhalb sicherer Parameter: Vertraulichkeit, Integrität und Verfügbarkeit.



Cloud Computing – Rechtliche Anforderungen an die IT-Security

Gesetzliche Grundlagen und Regelungen

- KonTraG (Gesetz zur Kontrolle und Transparenz) als Ergänzung zum HGB und zum AktG:
 - Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit für den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden (§ 91 Abs. 2 AktG).
 - Gilt nach herrschender Meinung analog auch für größere GmbHs, die gleichen Pflichten werden aus §43 Abs.1 GmbHG abgeleitet.
- Diese Anforderungen, die sich auf die IT-Security und das Risikomanagement ableiten lassen, müssen auch beim Cloud Computing erfüllt werden. Daraus ergeben sich entsprechende Haftungen für den Auftraggeber.



Cloud Computing – Rechtliche Anforderungen an den Datenschutz

Gesetzliche Grundlagen und Regelungen

- BDSG soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
 - Relevant §11 BDSG: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
 - Der **Auftraggeber** ist für die Einhaltung des Datenschutzes verantwortlich.
 - § 11 BDSG macht detaillierte Vorgaben dazu, welche Punkte in einer Vereinbarung zur Auftragsdatenverarbeitung **schriftlich** geregelt sein müssen (10 Gebote).
 - Der **Auftraggeber** ist für die schriftliche Auftragserteilung, die Definition der technischen und organisatorischen Maßnahmen, deren Kontrolle, den Umfang der Weisungsbefugnisse sowie der Pflichten des Auftragnehmers verantwortlich.



Cloud Computing – Definition „Personenbezogene Daten“

Regelungen des BDSG

- Daten sind personenbezogen, wenn sie persönliche oder sachliche Verhältnisse einer natürlichen Person beschreiben. Dazu genügt es, wenn die Person nicht namentlich benannt wird, aber bestimmbar ist.
- Bspw. durch Telefonnummern, E-Mail, IP-Adresse, etc.
- Nicht in den Geltungsbereich des BDSG fallen per Wortlaut Daten über juristische Personen (GmbH, AG). Einzelne Verwaltungsgerichte haben jedoch Datenschutzgesetze auch auf juristische Personen angewandt.
- Jede nichtöffentliche Stelle (z. B. Unternehmen), in der zehn oder mehr Personen ständig mit der Bearbeitung personenbezogener Daten mittels elektronischer Datenverarbeitung beschäftigt sind, benötigt einen Datenschutzbeauftragten.



Cloud Computing – Anforderungen an die Compliance

Anforderungen an die Kontrolle der Einhaltung von Gesetzen

- Kontrolle und Beherrschung nach § 11 BDSG:
Die Regelkonformität bzw. Einhaltung von Gesetzen (Regeltreue) muss regelmäßig kontrolliert werden.
- Eine „Beherrschung“ bei einer Public Cloud ist nahezu unmöglich und nicht praktikabel.
- Bei einer Public Cloud kann ggf. über ein GU-Modell mit einem Vertragspartner eine angemessene Lösung erreicht werden.
- Eine Prüfung einer möglichen Lösung durch Realisierung als Private Cloud vs. Public Cloud ist empfehlenswert.
- Berichts- und Dokumentationspflichten sind vertraglich zu regeln.
- Kontrollrechte des Auftraggebers sind vertraglich zu regeln.
- Alle individuellen Services sind vertraglich zu regeln.



Cloud Computing – Vertragliche Anforderungen

Anforderungen an die vertragliche Ausgestaltung

- Anforderungen sind möglichst detailliert in einem Pflichtenheft zu definieren.
- Alle Themen des Outsourcings sollten berücksichtigt werden.
- Als vertraglicher Überbau empfiehlt sich ein Master Service Agreement (Rahmenvertrag), in denen einzelne Teilleistungen in Leistungsscheinen definiert sind.
- Insbesondere Anforderungen eigener Kunden und Lieferanten sind ebenfalls zu berücksichtigen.
- Im Detail sollten die Themen Datensicherheit und Datenschutz geregelt werden.
- Ggf. sind auch Subunternehmer in das Regelwerk mit einzubeziehen.



Cloud Computing – Sonstige vertragliche Anforderungen

Lizenz- und Asset-Management

- Art der Lizensierungen von Programmen.
- In der Cloud sind oftmals spezielle Lizenzierungsverfahren notwendig.
- Berücksichtigung von Über-/Unterlizensierungen und Projektspitzen.
- Durch Outsourcing in die Cloud können u.U. vorhandene Assets vernichtet oder überflüssig werden

Verfügbarkeiten/SLA

- Leistungsbeschreibungen und Verfügbarkeiten müssen geregelt sein.
- Reporting und Monitoring bzgl. Verfügbarkeiten müssen ebenfalls geregelt werden.
- Eine entsprechende Dokumentation muss berücksichtigt werden.



Cloud Computing – Die Praxis

Gehen wir in die Cloud?

- Inhouse vs. IT-Outsourcing vs. Cloud:
Welche Ressourcen sollen ausgelagert werden? Wird durch die Auslagerung ein Service- oder Kostenvorteil erreicht?
- Private Cloud vs. Public Cloud:
Welche Ausprägung des Cloud Computing entspricht den Anforderungen der Auslagerungsstrategie am besten?
- Datensicherheit und Datenschutz:
Welche Vertragswerke werden benötigt?
- Verantwortlichkeiten:
Haftungen werden nicht einfach auf den Cloud Provider verlagert.



Cloud Computing in der Praxis - Am Beispiel synergetic AG

Sicherheit

- Sitz und Betrieb in Deutschland in eigenen RZ
- Deutsches Recht wird angewendet
- Individuelle kundenorientierte SLA
- Ganzheitlicher Ansatz LAN/WAN/Cloud

Integrative Cloud Strategie

- Weder eine reine Online Strategie ist zukünftig ausreichend noch wird Software zukünftig nur noch lokal installiert.
- Integration/Anpassung an bestehende Infrastrukturen und Lösungen.

Know-how und Erfahrung

- Cloud Services seit 1995
- SaaS seit 2003

Cloud Computing - Fragen?

**Vielen Dank für Ihre
Aufmerksamkeit!**