



Fraunhofer FOKUS

Fraunhofer Institute for Open
Communication Systems

Kaiserin-Augusta-Allee 31
10589 Berlin, Germany

www.fokus.fraunhofer.de



Cloud Computing – Potentiale für die öffentliche Verwaltung

Peter H. Deussen

Fraunhofer-Institut für Offene Kommunikationssysteme

01.12.2010, ILB, Potsdam



Agenda

- Was ist Cloud-Computing
- Gefahrenanalyse Cloud-Computing
 - Outsourcing
 - Datenschutz
 - BSI-Standpunkt
- Ausgestaltungsoptionen
 - Private Clouds
 - Community-Clouds
 - Hybride Clouds
- Zusammenfassung



Cloud-Computing ist ...

In a fully implemented Data Center environment, you can decide if an application runs on someone else's data center or on your own.

Most computer savvy folks actually have a pretty good idea of what the term "cloud computing" means: outsourced, pay-as-you-go, on-demand, somewhere in the Internet, etc.

Clouds are virtualized. On-demand requisitioning

Insgesamt finden sich mehr als 60 Definitionen des Begriffs Cloud-Computing!

- Welche Definition soll in einem politischen/wirtschaftlichen Entscheidungsprozess zugrundegelegt werden?
- Gibt es einen gemeinsamen Nenner?

The service SaaS, PaaS, and Cloud Computing Platforms

Put simply cloud computing is the infrastructural paradigm shift that enables the ascension of SaaS.

Cloud computing will be the user-friendly of grid computing

I would like to propose a 'Cloud Pyramid' to help differentiate the various Cloud offerings out there.



Was ist Cloud-Computing?

Definition des NIST

Eigenschaften

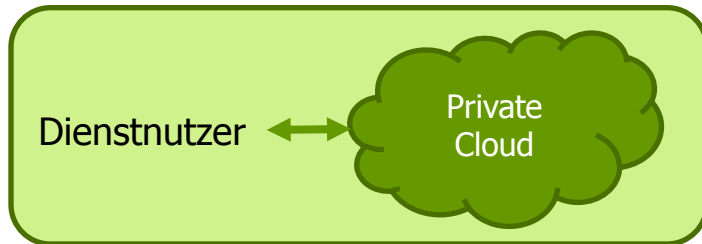
- Mandantenfähiger Bedarfsbetrieb mit Selbstbedienung
- Ortsunabhängige Ressourcenverfügbarkeit (Pooling)
- Breit verfügbarer Netzzugriff
(auch von unterschiedlichen Endgeräten)
- Schnelle Elastizität
(bedarfsgerechter Verbrauch mit dynamischer Skalierung)
- Überwachte Dienstnutzung (Dienstgüte)

Dienstklassen (*-as-a-service)

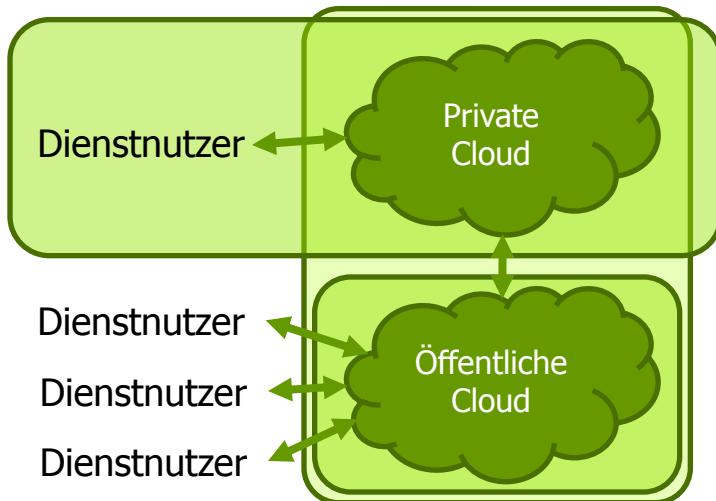
- Software (SaaS)
- Plattform (PaaS)
- Infrastruktur (IaaS)



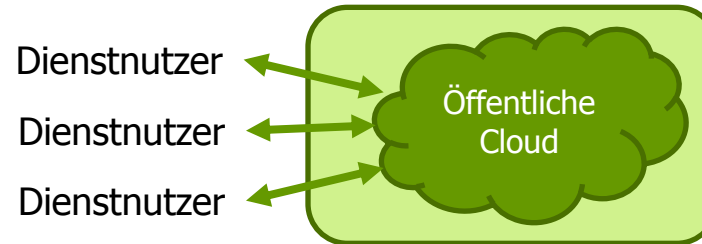
Cloud-Betriebsmodelle



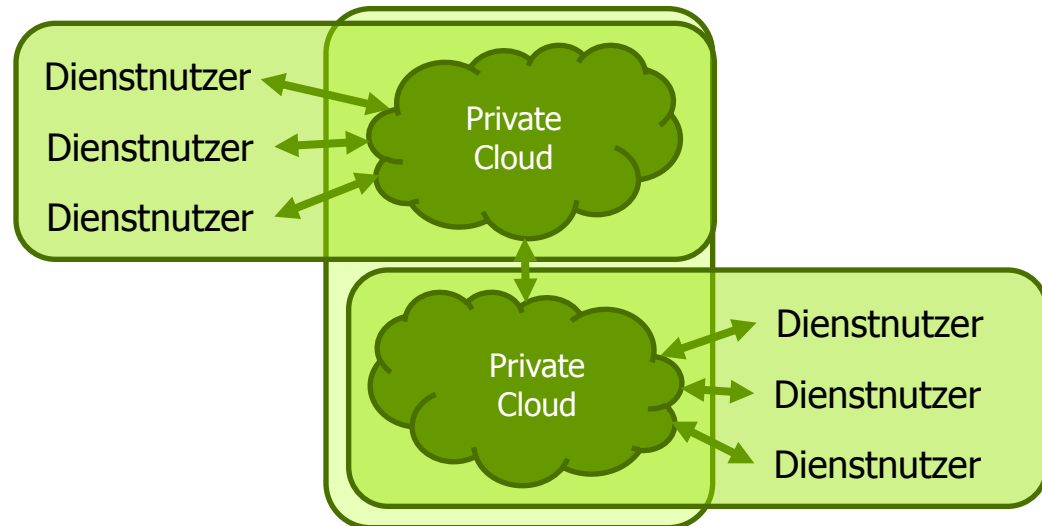
Private Cloud: Hauseigenes RZ oder dedizierter Dienstleister



Hybride Cloud: Private Cloud mit öffentlichem Anteil



Öffentliche Cloud: Standardisierte Dienstleistungen für Jedermann



Community-Cloud: Zusammenschluss/Kooperation privater Clouds

Cloud-Computing

System- und Dienstmanagement

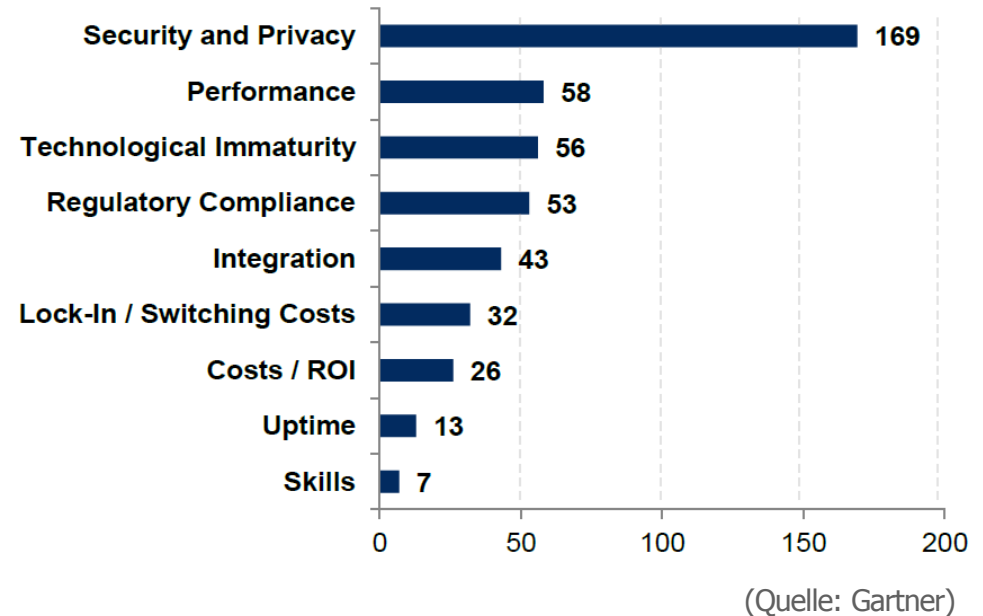
- Virtualisierung, Ressourcen-Pooling
 - **Homogenisiertes Systemmanagement**

- Selbstbedienung, messbare Dienstqualität, Elastizität, verbrauchsgerechte Abrechnung
 - **Automatisiertes Dienstmanagement**
 - Provisioning & Deprovisioning
 - Monitoring
 - Lifecycle Management
 - Event- & Failure-Management, etc.
 - **Weitreichende Protokollierungsmechanismen**
 - **Automatisierte Ressourcenallokation**



Beherrschbarkeit von Risiken in der Cloud

- Risikofragestellungen nehmen einen breiten Raum in der öffentlichen Diskussion ein
- Für den **öffentliche Sektor** gelten besondere Anforderungen
 - Kontrolle über die Aufgabenwahrnehmung und -durchführung
 - Datenschutz, etc.
- Wirtschaftliche Überlegungen sind erst an zweiter Stelle



Die Frage nach der **Anwendung von Cloud-Technologien im öffentlichen Sektor und die **Auslagerung von Diensten** in die Cloud muss deshalb in erster Linie aus der Perspektive der **Beherrschbarkeit der verbundenen Risiken** betrachtet werden**



Sicherheitsanforderungen aus heutiger Sicht

BSI-Grundschatz als „Benchmark-Test“ für Cloud-Computing

Grundschatz

- Katalog konkreter Gefährdungen und Maßnahmen
- Gegliedert in thematische Bausteine
- Grundlage für ISO 27001 Zertifizierung

Bausteine „Outsourcing“ und „Datenschutz“

- Bewertung von Cloud-Computing bzgl. zentraler Aspekte
- Notwendige (nicht hinreichende!) Anforderungen
 - Ergänzt durch ein „Eckpunktpapier“ des BSI (ENTWURF)



Analyse der Grundschutzanforderungen

Gefährdung	Öff.	Priv.	Comm.
G 1.10 Ausfall eines Weitverkehrsnetzes	🟢	🟡	🟡
G 2.1 Fehlende oder unzureichende Regelungen	—	—	—
G 2.7 Unerlaubte Ausübung von Rechten	—	—	—
G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren	🔴	🟢	🟢
G 2.47 Ungesicherter Akten- und Datenträgertransport	🟢	🟢	🟢
G 2.66 Unzureichendes Sicherheitsmanagement	🟢	🟢	🟢
G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	🔴	🟡	🔴
G 2.83 Fehlerhafte Outsourcing-Strategie	Vgl. § G 2.83 auf S. 76		
G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister	🔴	🟡	🟡
G 2.85 Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens	🔴	🔴	🔴
G 2.86 Abhängigkeit von einem Outsourcing-Dienstleister	🔴	🔴	🔴
G 2.88 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben	—	—	?
G 2.89 Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase	🟢	🟢	🟢
G 2.90 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister	🔴	🟡	🟡
G 2.93 Unzureichendes Notfallvorsorgekonzept beim Outsourcing	🟢	🟢	🟢
G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten	—	—	?
G 4.33 Schlechte oder fehlende Authentifizierung	🟢	🟢	🟢
G 4.34 Ausfall eines Kryptomoduls	🟢	🟢	🟢
G 4.48 Ausfall der Systeme eines Outsourcing-Dienstleisters	🟢	🟢	🟢
G 5.10 Missbrauch von Fernwartungszugängen	🔴	🟡	🟡
G 5.20 Missbrauch von Administratorrechten	🔴	—	—
G 5.42 Social Engineering	—	—	—
G 5.71 Vertraulichkeitsverlust schützenswerter Informationen	🔴	🟢	🔴
G 5.85 Integritätsverlust schützenswerter Informationen	🔴	🟡	🟡
G 5.107 Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister	—	—	—

Beispiel: Gefahrenanalyse für „Outsourcing“

- Für jede der 25 Gefährdungen wurde eine Einschätzung erarbeitet:
 - Ist das **vermutliche** Sicherheitsniveau in Clouds **höher**, **gleich**, oder **niedriger** als in Rechenzentren ohne Cloud-Technologien?
 - **Bewertungsfaktoren:**
 - Spezifische Schwachstellen
 - Cloud-Eigenschaften
 - Betriebsmodell
 - Für private, öffentliche und Community-Clouds
- Entsprechend für Maßnahmen:
 - **Leichter**, **gleich schwierig**, oder **schwieriger** implementierbar?



Gefahrenlage Outsourcing

Private Cloud

- Situation im wesentlichen vergleichbar mit Auslagerung von IT-Dienstleistungen an einen herkömmlichen Dienstleister
- Virtualisierung und konsolidiertes, homogenes Management mindern viele Gefahren und machen Maßnahmen leichter implementierbar, z.B.
 - Änderungsmanagement
 - Kontrolle/Qualitätssicherung
- Allerdings: Verwendung herstellerspezifischer Cloud-Technologien erschwert u.U. Anbieterwechsel (*lock-in*)



Gefahrenlage Outsourcing Community-Cloud

- Ähnlich wie bei privaten Clouds
- Zusätzliche Schwierigkeiten aufgrund fehlender Ansätze für föderiertes Management
 - Prozesse und Daten durchlaufen mehrere Verwaltungsdomänen mit unterschiedlichen Policies, Rollenstrukturen, usw.
 - Identitätsmanagement
 - Fehlermanagement
 - Änderungsmanagement, etc.



Gefahrenlage Outsourcing

Öffentliche Cloud

■ Selbstbedienung + Netzwerkzugang

- „Perimeter“-Ansatz (Firewalls, physikalische Abschottung) nur bedingt verwendbar
- Resultierende Gefährdungen sind z.B.
 - Unzureichende Authentifizierung
 - Missbrauch von Fernwartungszugängen, etc.

■ Selbstbedienung

widerspricht Transparenz- und Kooperationsanforderungen

- Enge **personelle** Kooperation zwischen Auftraggeber und Anbieter gefordert:
 - Sicherheitskonzept
 - Notfallkonzept
 - Offenlegung und Bewertung interner Prozesse beim Anbieter (ISO 27001 Zertifikat nicht hinreichend), etc.
- Nur schwer in AGBs (oder generische SLA-Templates) zu fassen



Gefahrenlage Datenschutz

Private/Community-Clouds

- Für private/Community-Clouds ergibt die Analyse eine Einschätzung, die bzgl. des erreichbaren Datenschutzniveaus grundsätzlich positiv ausfällt.
 - Prozesse und Mechanismen sind in Clouds leichter implementierbar als in heterogenen Infrastrukturen mit einem hohen Anteil an manuellen Administrationstätigkeiten
 - Gleichzeitig besteht (nach wie vor) der Vorteil eines „geschlossenen“ Systems, in dem klassische Abschottungsmechanismen greifen



Gefahrenlage Datenschutz

Öffentliche Cloud

- Ortsbindung
 - Alle Anbieter erlauben eine Beschränkung auf die EU
 - Wie steht es aber mit der Kontrolle?
- Kontrolle
 - Einhaltung der Rechtsgrundlage und der Zweckbestimmung
 - Die Sicherstellung der Rechte des Betroffenen (Auskunft, Berichtigung, Sperrung, . . .)
 - Verpflichtung der Mitarbeiter bzgl. Datenschutz
 - Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen
 - Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle
 - Zuständig sind Landesdatenschutzbeauftragte: Ortsbindung ?



Gefahrenlage Datenschutz

Öffentliche Cloud

- Kontrolle: Beispiel Protokollierung von Ereignissen (Maßnahme 2.110):
 - Modifikation von Systemparametern
 - Einrichten von Benutzern
 - Erstellung von Rechteprofilen
 - Einspielen und Änderung von Anwendungssoftware
 - Änderungen an der Dateioorganisation
 - . . .
- Umfassende Offenlegungspflicht
 - Mandantenfähigkeit ist nicht hinreichend, da auch Protokollierungen auf Systemebene gefordert ist



Mindestanforderungen an Cloud-Anbieter

Sicht des BSI

- ITIL/COBIT (Gewaltiger Nachholbedarf)
- Technische und organisatorische Maßnahmen, z.B.
 - Gesicherte Netze (Firewalls, IDS, IPS, DDoS-Abwehr, . . .)
 - Spezielle Anforderungen bzgl. Virtualisierung (z.B. Umgang mit Images, Absicherung von Hypervisoren)
 - Anforderung an Verschlüsselung
 - Identitäts- und Rechtemanagement
 - Multifaktor-Authentifizierung
- Transparenz
 - Standorte müssen bekannt sein
 - Subunternehmer (Vertragsgestaltung!)
 - Validation von Sicherheitsmaßnahmen (z.B. Penetrationstests)
- Vermeidung von lock-in Situationen
 - Interoperable und portierbare Anwendungen und Daten
 - Aktuell nur wenige Standards verfügbar



Mehr Sicherheit in der Cloud

Organisation

- Multiple Standorte
 - Redundante Daten und Prozesse
- Verteilte Datenhaltung
 - Absicherungsmechanismen auf Netzwerkebene
- Einheitliches Sicherheitskonzept
 - Zeitnahe Aufdeckung von Schwachstellen und Durchsetzung von Gegenmaßnahmen
- Dediziertes Expertenteam
 - Konsolidiertes und effektives Bedrohungsmanagement
 - Verkürzte Reaktionszeiten

Cloud-Technologie

- Sofortige und adaptive Ressourcenskalisierung
 - DDOS
- Vereinfachte Audits und Spurensicherung
 - Virtualisierung

Sicherheit als Marktfaktor

- Notwendigkeit für robustere Dienste
 - Unbekannter Sicherheitskontext
- Standardisierte Schnittstellen für Sicherheitsmanagement
- Security-as-a-service



Private Clouds

Technologischer Upgrade für behördliche Rechenzentren

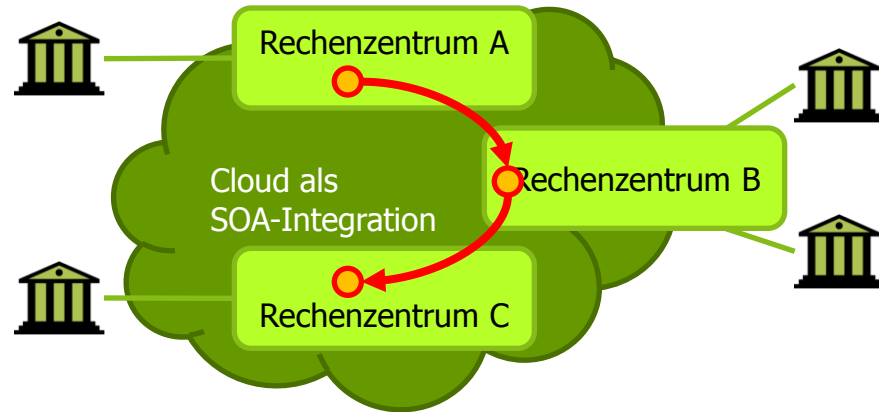
- Grundsätzliche Option zur Modernisierung behördlicher Rechenzentren
- Umsetzungen werden bereits vollzogen
 - IaaS (allerdings ohne Elastizität)
 - wird von vielen Shared-Service Centern angeboten („Services anstelle von Servern“)
 - PaaS: Verzeichnisdienste z.B. für Geodaten
 - Vermessungsämter,
 - Behörden für Stadtentwicklung, etc.
 - SaaS:
 - „Thin Clients“
 - Fachverfahren (ERP, CRM, Finanzen, etc.)



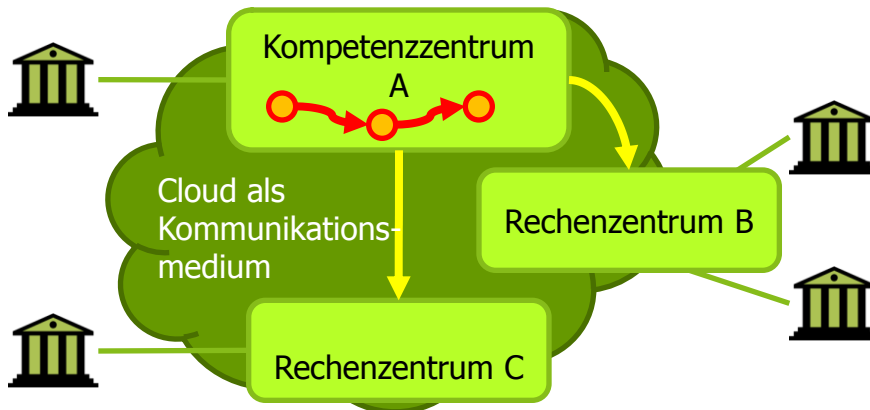
Community-Clouds

Ausgestaltungsoptionen

- **Übergreifende Kooperation**
 - Kollaboratives Bereitstellen von Dienstleistungen
 - Prozesse durchlaufen verschiedene Rechenzentren

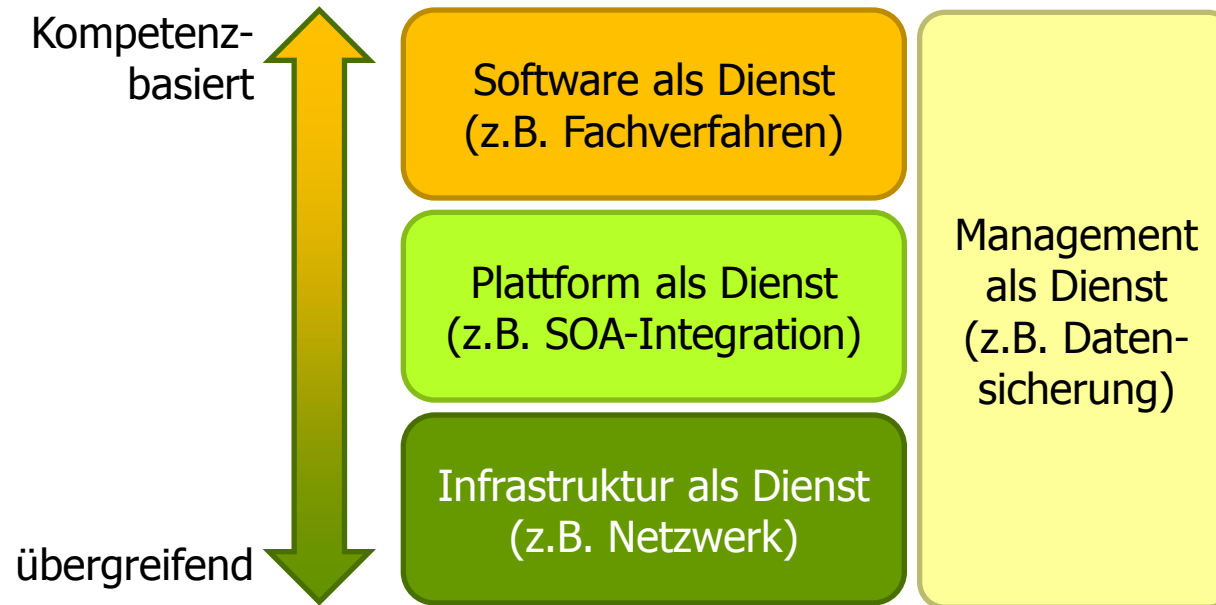


- **Kompetenzbasierte Kooperation**
 - Einzelne Rechenzentren treten als Kompetenzzentren gegenüber anderen Partnern im Verbund auf



Community-Clouds

Ausgestaltungsoptionen



- Übergreifende Kooperation für generische Dienste
 - Netzwerk, SOA-Integration, Unterstützung (Backup, Event-Management, etc.)
- Kompetenzbasierte Kooperation für spezifische Dienste
 - Fachverfahren



Öffentliche bzw. hybride Clouds

Modell für ÖPP

- Dienst-Auslagerung in öffentliche Clouds (bzw. den öffentlichen Anteil einer hybriden Cloud) ist kritisch zu bewerten (Datenschutz, Transparenz, etc.)
- Allerdings offeriert der privatwirtschaftliche Sektor ein großes Potential an Ressourcen und Know-how
- Optionen
 - Auslagerung öffentlicher Daten in die Cloud
 - Verkehrsinformationen, Wetterdaten, Wirtschaftsdaten, Finanzdaten, digitale Karten, etc.
 - Entwicklung „sicherer Dienste“
 - Elektronische Safes für Daten & Dokumente (verschlüsselt, fragmentiert)
- Anforderungen
 - externe IT-Audits und Kontrollen durch den Auftraggeber
 - Protokollierungs- und Zusammenarbeit
 - Portabilität zwischen verschiedenen Clouds (»lock-in«-Situationen)
 - transparentes, standardkonformes Dienst- und Systemmanagement
 - Transparenz bezüglich der Standorte
 - Offenlegung von Subunternehmern und Verträge



Zusammenfassung

- Private Cloud
 - Bezüglich heutiger Standards eine grundsätzliche Option zur Modernisierung behördlicher Rechenzentren
- Community-Cloud
 - Kooperationsmodell zur IT-Konsolidierung
 - Föderierte Managementansätze werden benötigt, um ggf. heterogene Technologien und Organisationsformen zu vereinheitlichen
- Öffentliche Cloud/hybride Cloud
 - Probleme:
 - Selbstbedienung/Netzwerkzugang
 - Transparenz & Kontrolle
 - Potentiale: Open Data



Studie: Cloud-Computing für die öffentliche Verwaltung

■ Förderer



■ Ausführende



■ Zielsetzung

Untersuchung von Cloud-Computing als Alternative und Perspektive kooperativen eGovernments in Deutschland:

- Rahmenbedingungen
- Ausgestaltungsszenarien
- Migrationsbedingungen

■ Download

http://www.fokus.fraunhofer.de/de/elan/_docs/cloud_studie_vorabversion_20101129.pdf



Q & A

