



Cloud Computing und Recht

Was bedeutet Cloud Computing, welche Risiken verbergen sich dort und welche rechtlichen Aspekte sind hier besonders zu beachten?

Uli Emmert, Rechtsanwalt, ESB Rechtsanwälte

Jörg von der Heydt, Channel & Marketing Manager Fortinet

Agenda

- **Was?**
 - Definition „Cloud Computing“
 - Reale Umsetzung & Anbieter
- **Wieso?**
 - Motivation für Einführung/Nutzung von CC-Diensten
- **Unsicher?**
 - An welchen Stellen spielt Security eine besondere Rolle?
- **Womit ?**
 - Welche (Security-)Lösungen bieten sich an?

Was?

- **Definition**

- Cloud Computing umschreibt den Ansatz, abstrahierte IT-Infrastrukturen wie
 - Rechenkapazität
 - Datenspeicher
 - Netzwerkkapazitäten
 - Software

dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen.

(Def. lt. Forrester)

Woher?

- **Historie**

- z.B. Amazon und das Weihnachtsgeschäft
 - 10fache Kapazität der Infrastruktur erforderlich (2006)
 - Schaffung von Diensten und Architektur zur Bewältigung der hohen Nutzerzahl und Last
 - Angebot dieser Infrastruktur nach außen als Dienst
 - „Überkapazitäten“
- weitere „Treiber“
 - Google
 - Yahoo

Servicemodelle

- **IaaS**

- Infrastructure as a Service

- dynamische Bereitstellung von Rechenkapazität (Computer/Server), Netzwerken und Storage

- **PaaS**

- Plattform as a Service

- dynamische Bereitstellung von Plattform- oder Laufzeitumgebung(en)

- **SaaS**

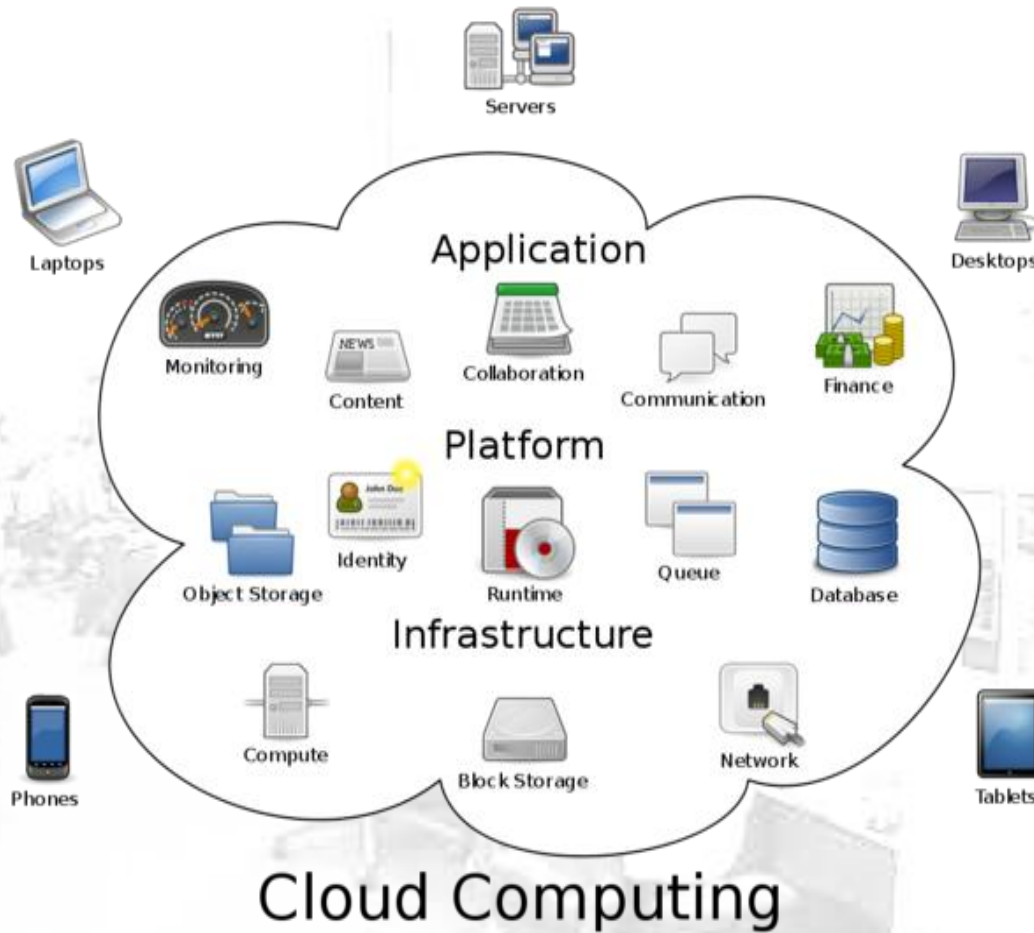
- Software as a Service

- auch *Software on Demand*
 - dynamische Bereitstellung von Anwendungen oder Software-Sammlungen

Liefermodelle

- **Public Cloud**
 - offenes Nutzungsmodell für „jeden“
 - pay per use
- **Private Cloud**
 - geschlossenes Modell für (unternehmens-)interne Nutzung
- **Hybrid Cloud**
 - Mix aus public und private Cloud
- **Community Cloud**
 - gemeinsame Nutzung von Ressourcen durch eine beschränkte Gruppe
 - z.B. Behörden, Universitäten, Forschungsgemeinschaften usw.

oder so:



Security?

Vor- und Nachteile

- **PRO**

- geringe(re) Kosten
 - pay-as-you-use/need Modelle
 - besonders attraktiv für nur selten benötigte Services
 - keine eigene Investition in
 - Hardware
 - Software
 - Personal
- einfachste (und automatische) Skalierbarkeit
- sofortige Verfügbarkeit
 - keine aufwändigen Planungs- und Beschaffungs- und Implementierungsprozesse
- keine aufwändigen Update-Prozesse
- standortunabhängiger Zugriff

Vor- und Nachteile

• KONTRA

- Daten-Hoheit liegt bei Dritten
 - u.U. in Regionen mit anderer als der deutschen Rechtslage
- hoher Verschlüsselungsaufwand
 - Performance-Verluste
- keine 100% Verfügbarkeit garantiert
 - 99.9% bzw. 99.95% je nach Anbieter
 - 99.99% in vielen Fällen erforderlich
 - entspricht 52 Minuten Ausfall pro Jahr
- keine Standardisierung
 - unterschiedliche Implementierungen und Schnittstellen bei Providern
- unklare Regelung von Verantwortlichkeiten

Cloud Computing und Security

- **PRO**

- hoher Security-Spezialisierungsgrad bei CC-Anbietern
 - Know How und geschäftsentscheidende Verantwortung
- up-to-date Technologie
- Verfügbarkeit
- Backup & Recovery
- Endgeräte-Unabhängigkeit
 - i.d.R. browserbasierende Applikationen
- zusätzliche Security-Services
 - deren Anschaffung & Betrieb für einzelne (v.a. kleinere) Unternehmen zu kostspielig wäre

Cloud Computing und Security

• KONTRA

- Daten befinden sich nicht mehr auf unternehmensinterner Hardware
 - Verschlüsselung
 - zeit-/rechenintensiv = Performanceverlust
- Applikationen sind u.U. auf verschiedene Anbieter verteilt
 - einheitliches Konzept der userbasierenden Nutzung von Anwendungen oder Teilen davon komplex
- Zugriff auf verteilte Hardware mit u.U. unterschiedlichen Betriebssystemen, Patches
 - Schutz wird komplex
- Größere Angriffsfläche
 - „7 auf einen Streich“
- Kontrollverlust
- Infrastruktur zwischen einzelnen Hardwarekomponenten = Internet
 - Internet wird zum „PC-Bus“
 - Performance !!!
 - Verteilte Security erforderlich
 - u.U. um ein Vielfaches höhere Laufzeiten

Security Empfehlungen

Area	Precautions
Governance	Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet these requirements.
Trust	Incorporate mechanisms into the contract that allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Institute a risk management program that is flexible enough to adapt to the continuously evolving and shifting risk landscape.
Architecture	Understand the underlying technologies the cloud provider uses to provision services, including the implications of the technical controls involved on the security and privacy of the system, with respect to the full lifecycle of the system and for all system components.
Identity and Access Management	Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions.
Software Isolation	Understand virtualization and other software isolation techniques that the cloud provider employs, and assess the risks involved.
Data Protection	Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned.
Availability	Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed and that all operations can be eventually reinstated in a timely and organized manner.
Incident Response	Understand and negotiate the contract provisions and procedures for incident response required by the organization.

Fortinet und Cloud Computing

- **Lösungen für**
 - Cloud Computing Provider UND Nutzer*
 - RZ Absicherung
 - UTM
 - High Performance
 - Application Control
 - Web Application Security
 - Mail Security
 - Datenbank Security
 - Verschlüsselung
 - VPN
 - Mail-Encryption
 - Authentifizierung
 - Token
 - Authentication Gateway

* da immer nur teilweise Auslagerung von Diensten oder Infrastruktur



Fragen ?

Vielen Dank !

Für weitere Informationen besuchen Sie bitte
<http://www.fortinet.com> oder www.sicher-sein.net

Fortinet GmbH

Jörg von der Heydt

Channel Manager Germany

Mail: jvdheydt@fortinet.com

Tel.: +49 2331 924609 oder +49 163 2925774

