3. Nürnberger Unternehmer-Kongress

Gesprächskreis 4

Cloud Computing –
Herausforderung für den Mittelstand ?

Nürnberg, den 21. Januar 2013

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission, Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission, Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Vorteile …

- Die Anbieter ergänzen laufend ihr Portfolio und bieten immer neue Cloud-Leistungen an.
- Ausgangspunkt der Anbieter
  - Erweiterung bestehender Angebote (IBM, 1&1, Host Europe, Deutsche Telekom, Zimory)
  - Markteintritt mit neuen Produkten (Microsoft [Azure], Salesforce)
  - Nutzung und Vertrieb bestehender Infrastrukturen (Amazon, NTT, Google)
- Die Leistungsfähigkeit wird im Wesentlichen von 3 Faktoren bestimmt:
  1. Sicherheit der Infrastruktur
  2. Anbindung der Services
  3. Expertise des Anbieters

… und dennoch Vorbehalte

Begünstigende Faktoren	Kritische Faktoren
Kostenvorteile	Sicherheit und Datenschutz
Geringer Administrationsaufwand	Fehlende Vereinbarungen zu Beendigung und Anbieterwechsel
Benutzerfreundlichkeit	Risiko des Systemausfalls
Ubiquität der Anwendungen	Bandbreite
Aktualität der Anwendungen	Verfügbarkeit
	Kontrollverlust / Verlagerung
	Total Cost of Ownership

es bestehen **noch** deutliche Vorbehalte / Bedenken hinsichtlich

- Nachhaltigkeit des Anbieters
- technische Sicherheit und Vertraulichkeit der Daten (Datenschutz)
- Rechtsunsicherheit, Komplexität der AGBs
- Praxiseignung und insb. Integrationsfähigkeit der Cloud-Lösungen
- Kosteneinsparungen

Quelle: DATEV

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission, Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Sicherheit: Datenschutz, Vorfälle, Angriffe, Vertragsgestaltung

WindowsPro

Windows, Virtualisierung und Cloud für Profis

Home Marktübersichten Produktvergleiche Praxis Tests Know-how

Datenschutz in der Cloud: USA können auf europäische Daten zugreifen

Bernd Reder, 08.07.2011

Tags: Sicherheit, Office, Cloud-Computing, Cloud

Interessiert Sie Windows und Virtualisierung? Bestellen Sie unseren Newsletter!

Nach Angaben der britischen Rechtsanwaltskanzlei Pinsent Masons, die international tätig ist, können amerikanische Behörden persönliche Daten von Nutzern von Cloud-Computing-Diensten in Europa ohne deren Wissen abfragen. Die Voraussetzung ist, dass die User einen Cloud-Service verwenden, den eine Firma mit Sitz in den USA bereitstellt, wie etwa Microsoft, Amazon und andere.

- Wer hat Zugriff auf die Daten?
- Safe Harbor Agreement und US Patriot Act
- Systemausfälle
- Angriffe
- Vertragssicherheit

RUHR-UNIVERSITÄT BOCHUM

PRESSEINFORMATION

RUB » Pressestelle » Presseinformationen » Kategorie Allgemeines » Presseinformation 336

Nummer 336 - Bochum, 24.10.2011

Cloud Computing: „Wolke" mit Lücken

Massive Sicherheitsmängel bei Amazon Web Services entdeckt und behoben

RUB-Wissenschaftler präsentieren Angriff auf dem ACM Cloud Computing Security Workshop in Chicago

Eine massive Sicherheitslücke haben Forscher der Ruhr-Universität Bochum beim Cloud-Anbieter Amazon gefunden. Mit verschiedenen Angriffsmethoden (Signature Wrapping und Cross Site Scripting) testeten sie das als „sicher" geltende System. „Anhand unserer Forschungsergebnisse bestätigte Amazon die Sicherheitslücken und schloss sie umgehend", so Prof. Dr. Jörg Schwenk, Lehrstuhl für Netz- und Datensicherheit der RUB. Amazon Webservices (AWS) bietet seinen Kunden das so genannte Cloud Computing an und hostet u. a. die Dienste Twitter, Second Life und 4Square.

netzwoche

Management Strategie Infrastruktur Software Web Telekommunikation

THEMA

crm

Ausgefallene Instanzen

Panne bei Salesforce.com

Salesforce.com konnte seine Cloud-Dienstleistungen gestern nicht durchgehend garantieren. Mittlerweile ist der Anbieter von Lösungen für das Management von Kundenbeziehungen (CRM) wieder vollständig erreichbar.

Gestern Dienstag sind einige Dienste auf Salesforce.com ausgefallen. Auf einer Statusseite, die zwischenzeitlich selbst nicht mehr erreichbar war, nennt der Cloud-Anbieter als Grund Probleme mit der Stromversorgung. Die Störung dauerte rund zwölf Stunden.

Rechts- und Datensicherheit – Top Risiken

Verletzung der Datenvertraulichkeit und -integrität	Datenlöschung „right to be forgotten“	Mangelhafte Mandantentrennung
Unklarheit über anwendbares Recht	Unsichere Rechtsdurchsetzung	Kontrollverlust
Intransparenter Subunternehmereinsatz	Eingriffe und Beschlagnahme Insolvenz des Providers	Erpressung / Diebstahl/ Angriffe

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission, Cloud-Strategie
- Verlagerung in die Cloud
- Fazit
- Fundstellen
- Kontakt

Konsultationen der Kommission

- Die Kommission hat umfangreiche Konsultationen in 2011 und 2012 durchgeführt.
- Befragt wurden Anbieter, Öffentlichkeit (web-based), Industrie, Vertreter SME, Telekommunikationsanbieter, Verbraucherverbände, Europäische CIO-Organisation.
- Fazit: Die Unternehmen sind zurückhaltend, weil
  - das anwendbare Recht und die Durchsetzbarkeit der gesetzlichen und vertraglichen Rechte oft unklar ist
  - Datenverlust und Verstöße gegen den Datenschutz befürchtet werden
  - die Gewährleistungen und Garantien der Anbieter unscharf sind
  - die Übertragbarkeit der Daten bezweifelt wird („vendor lock-in“)
  - weitere Risiken gesehen werden (loss of governance, isolation failure, insecure data deletion, malicious insiders, …)
- Fundstelle: Brussels, 27.9.2012 SWD (2012) 271 final

Cloud-Strategie der Kommission

- Vorschlag der EU-Kommissarin für die Digitale Agenda und Vize-Präsidentin der Kommission Frau Neelie Kroes für eine Cloud Strategie:
  - Mindestens europaweite einheitliche Verfahren zur e-Identification und Authentifizierung
  - Einführung eines einheitlichen Schemas zur Zertifizierung von Anbietern und ihren Leistungen bis Ende 2014
  - Bis Ende 2013 Entwicklung von einheitlichen und fairen Vertrags-bedingungen/-Mustern
  - Vereinheitlichung des Datenschutzrechtes in der EU und mit Nicht-EU-Ländern
  - Einbindung der öffentlichen Hand als Vorreiter in der Nutzung der Cloud
  - Fundstelle: Brussels, 27.9.2012 COM (2012) 529 final „Unleashing the Potential of Cloud Computing in Europe“

RölfsPartner

CORDIS
Community Research & Development Information Service

CORDIS – Forschungs- und Entwicklungsinformationsdienst der Gemeinschaft, ist eine Informationsplattform für europäische Maßnahmen im Bereich Forschung und Entwicklung (FuE) und Technologietransfer.

Innerhalb von CORDIS besteht die Cloud Expert Group, die laufend aktuelle Analysen und Empfehlungen veröffentlicht.

Zuletzt im Dezember 2012 die Recommendations by the Cloud Expert Group:
A ROADMAP FOR ADVANCED CLOUD TECHNOLOGIES UNDER H2020

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission; Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Verlagerung in die Cloud – schon heute?

- Angemessene **vertragliche Vereinbarungen** unter Berücksichtigung von Datenschutz und Datensicherheit sind **schon heute** möglich.
- Die vertraglichen Regelungen sind maßgeschneidert zu entwickeln, abhängig von
  - dem erforderlichen **Schutzniveau** der Daten
  - der angestrebten **Anwendung** und
  - dem **Geschäftsmodell** des Anbieters
- IT-Manager, Datenschutzbeauftragter, Rechtsabteilung, Revision, Compliance-Beauftragter und Leiter Einkauf müssen zusammenarbeiten, externe juristische Beratung ist zu empfehlen.
- Regelungssachverhalte sind:

Quelle: PwC

Verlagerung in die Cloud - Sicherheitscheck

Planung
- Sicherheitsanalyse
- Definition der Sicherheitsanforderungen
- Auswahl des Dienstleisters

Vertrag
- Vertragsgestaltung
- Definition messbarer Kennzahlen
- Sicherstellung ausreichender Audit-Rechte

Migration
- Sicherheitskonzepte
- Migration gemäß der Sicherheitskonzepte
- Definition der Verantwortlichkeiten

Betrieb
- Überwachung des Betriebes
- Schadensmanagement und Ausstieg

- Die individuellen Sicherheitsanforderung sind zu definieren und im Rahmen des nebenstehenden Prozesses dem Anbieter aufzuerlegen.
- Der Kunde bleibt Eigentümer der Daten und ist verpflichtet, für die Daten-sicherheit zu sorgen.
- Besonderes Augenmerk ist auf den Umgang mit Schadensfällen und die Beendigung des Vertrages zu richten.

Vertragliche Gestaltung: Orientierungshilfen

Ausgangspunkt sind die bekannten vertraglichen Werkzeuge

- IT-Outsourcing-Vereinbarungen
- die Allgemeinen Geschäftsbedingungen der Anbieter
- die allgemeinen gesetzlichen Rahmenbedingungen
- insbesondere die Datenschutzgesetzte
- branchenspezifische Vorschriften
  (z.B. KWG und MaRisk)

Der Einsatz allgemein zugänglicher Anwendungshinweise und Checklisten ist zu empfehlen.

1. Checkliste für Technik & Prozessabläufe

Encryption Key Management	IS-19	IS-19.1	Do en
		IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?
		IS-19.3	Do you have a capability to manage encryption keys on behalf of tenants?
		IS-19.4	Do you maintain key management procedures?
Vulnerability / Patch Management	IS-20	IS-21.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?
		IS-20.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?
		IS-20.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?
		IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?
		IS-20.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?
		IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?
Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support your cloud service offerings?
		IS-21.2	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?
Incident Management	IS-22	IS-22.1	Do you have a documented security incident response plan?
		IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?
		IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?

Die **Consensus Assessment Initiative** ist eine Non-Profit Organisation in den USA die sich um Best-Practice-Lösungen im Bereich Cloud bemüht, sie bietet

einen umfangreichen Fragebogen für die Vertragsverhandlungen mit einem Anbieter betreffend

- die internen Prozesse und Abläufe des Anbieters
- mit aktuell 210 Fragen und eine
- Checkliste mit allen einschlägigen amerikanischen Normierungen

Mit der Anwendung dieses Fragebogens und der Checkliste werden die wesentlichen Aspekte erfasst, allerdings nicht

- die spezifischen Bedingungen des Anwenders,
- das europäische Datenschutzrecht und
- Fragen der Rechtswahl und Rechtsdurchsetzung

2. Orientierungshilfe Service Level Agreements

Das Dokument „**procure secure**“ (Stand 2012) der **ENISA** European Network and Information Security Agency bietet:

- umfangreiche Empfehlungen für die Entwicklung, die Gestaltung und Überwachung von SLA`s in der Cloud
- eine Checkliste für die Regelungsinhalte des SLA
- Vorschläge für Ausschreibungen (RfP)
- Parameter zur Messung der Leistung
- technische Hinweise für die Vertragsbeendigung
- Anmerkungen zur Vertragsgestaltung

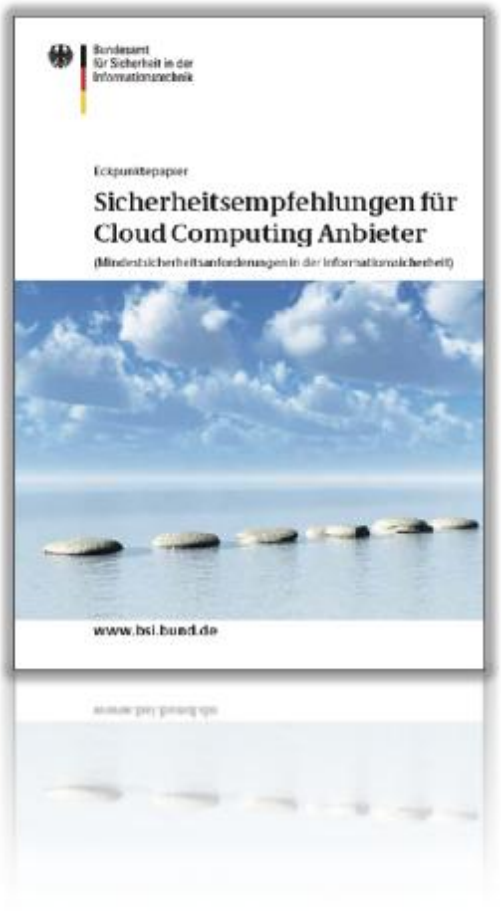
3. Leitfaden für Vertragsschwerpunkte im Cloud Computing

Der Verband der deutschen Cloud Computing-Industrie **EuroCloud Deutschland_eco e.V.** bietet in seinem

„**Leitfaden Cloud Computing**“ (Stand Nov. 2010)

- Hinweise zum Datenschutz
- eine Checkliste zur Vertragsgestaltung
- und Hinweise zu Besonderheiten aus
  - dem Bankaufsichtsrecht
  - dem Steuerrecht
  - dem Berufsrecht (Ärzte, Anwälte, …)

4. Sicherheitsempfehlungen zum Datenschutz



- Das **Bundesamt für die Sicherheit in der Informationstechnik** erläutert die Gewährleistung des Datenschutzes nach deutschem Recht > BDSG
- Speicherung und Verarbeitung der personenbezogenen Daten nur zulässig innerhalb der Mitgliedsstaaten der EU oder eines Vertragsstaats des EWR
- Außerhalb der EU oder eines Vertragsstaats des EWR, wenn ein angemessenes Datenschutzniveau gewährleistet werden kann
  z. B. durch:
  - Entscheidung der EU-Kommission (Argentinien)
  - Beitritt zum Safe-Harbor-Agreement (USA)
  - EU-Standardvertragsklauseln
  - Genehmigung der Aufsichtsbehörde
- In der Regel handelt es sich um eine Auftragsdatenverarbeitung nach § 11 BDSG.

5. Orientierungshilfe für grenzüberschreitenden Datenschutz

Die **Arbeitskreise Technik und Medien** der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben die „**Orientierungshilfe Cloud-Computing**“ (26.9.2011) entwickelt mit Definitionen und Hinweise zu

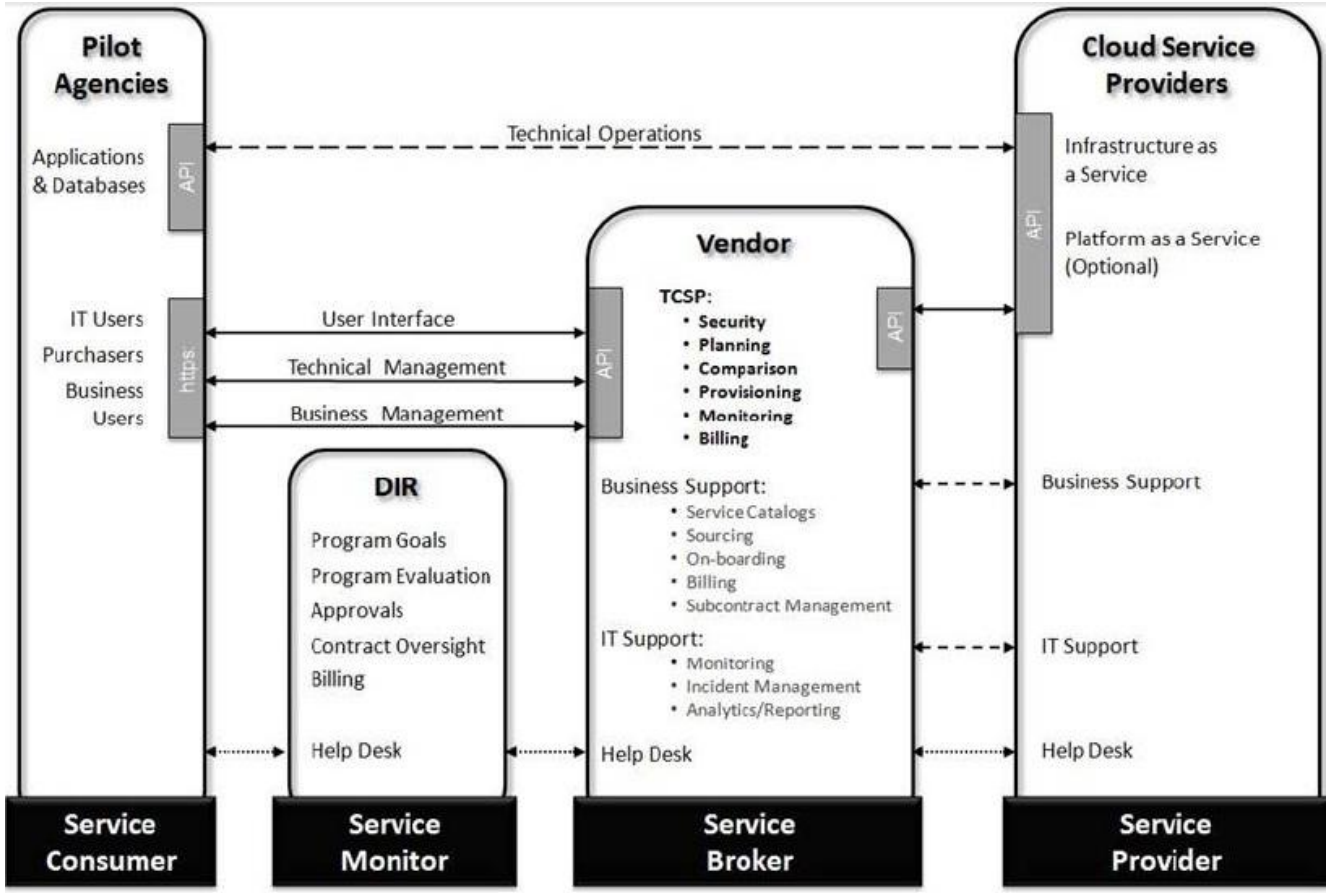
- allen datenschutzrechtlichen Aspekten
- den Verantwortlichkeiten und Kontrollen der Anbieter
- den Betroffenenrechten
- und Besonderheiten des grenzüberschreitenden Datenverkehrs

6. Orientierungshilfe für Datenschutz aus europäischer Sicht

Die **Article 29 Data Protection Working Party** bietet in ihrer „**Opinion 05/2012 on Cloud Computing**“ (1.7.2012)

- Leitlinien für die Zusammenarbeit zwischen Kunde und Anbieter
- Mindestanforderungen an die Vertragsgestaltung
- Hinweise für die technischen Anforderungen und
- die organisatorische und
- prozessuale Gestaltung der Zusammenarbeit der Vertragspartner

7. Alternative Einbindung eines Cloud Services Brokers (CSB) (auch Cloud Management Broker)



Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission; Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Fazit

1. Aufgrund der technischen und wirtschaftlichen Potenziale wird sich Cloud Computing **am Markt durchsetzen**, wenn Fragen der **angemessenen IT-Sicherheit** geklärt und die Verfügbarkeit/Anbindung verbessert werden.
2. Mit zunehmender Verbreitung in der Fläche wird das **Konzept** für **Angreifer attraktiver**.
3. Belange des **Datenschutzes** sind zu beachten, die **Kontrolle über die Daten** ist unter allen Umständen zu wahren.
4. Es können heute schon **vertragliche Vereinbarungen** getroffen werden, diese sind allerdings aufwendig.
5. Die Implementierung von **Standards** für **Interoperabilität** und **Informationssicherheit** wird eine der zentralen Aufgaben in den kommenden Jahren sein.

Fundstellen

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Vorhaben der EU-Kommission; Cloud-Strategie
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Fundstellen

- www.trusted-cloud.de
- www.sienainitiative.eu
- www.nist.gov
- www.etsi.org
- www.enisa.europe.eu
- blogs.ec.europa.eu/neelie-kroes/
- www.bsi.bund.de
- www.aisec.fraunhofer.de
- www.cordis.europa.eu

Agenda

- Vorteile und Vorbehalte
- Rechts- und Datensicherheit in der Cloud
- Akzeptanz und Praxistauglichkeit aktueller Cloud-Angebote
- Verlagerung in die Cloud, Praxishinweise
- Fazit
- Fundstellen
- Kontakt

Kontakt

Rechtsanwalt

Felix Weidenbach

Partner

RölfsPartner
Nymphenburger Straße 3 b
80335 München

Telefon: **+49 89 55066-320**
Fax: **+49 89 55066-166**
Mobil: **+49 151 1504 9304**

felix.weidenbach@roelfspartner.de
www.roelfspartner.de