IT-Sicherheitsaspekte beim Arbeiten mit webbasierten Lösungen

IKT-Forum: Cloud Computing – Chancen und Risiken

Hochschule Ansbach, 01.12.2011

Dr.-Ing. Rainer Ulrich
Fraunhofer-Institut für Integrierte Schaltungen IIS

Fraunhofer IIS

Fraunhofer-Institut für Integrierte Schaltungen IIS

- Ca. 750 Mitarbeiterinnen und Mitarbeiter
- Budget über 90 Mio €
- Finanzierung: > 75 % aus Projekten
- Geschäftsfelder
  - Audio und Multimedia
  - Bildsysteme
  - Digitale Rundfunksysteme
  - Eingebettete Systeme
  - IC-Design und Entwurfs-automatisierung
  - Kommunikationsnetze
  - Lokalisierung und Navigation
  - Logistik
  - Medizintechnik
  - Optische Prüfsysteme
  - Röntgentechnik

Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit AISEC

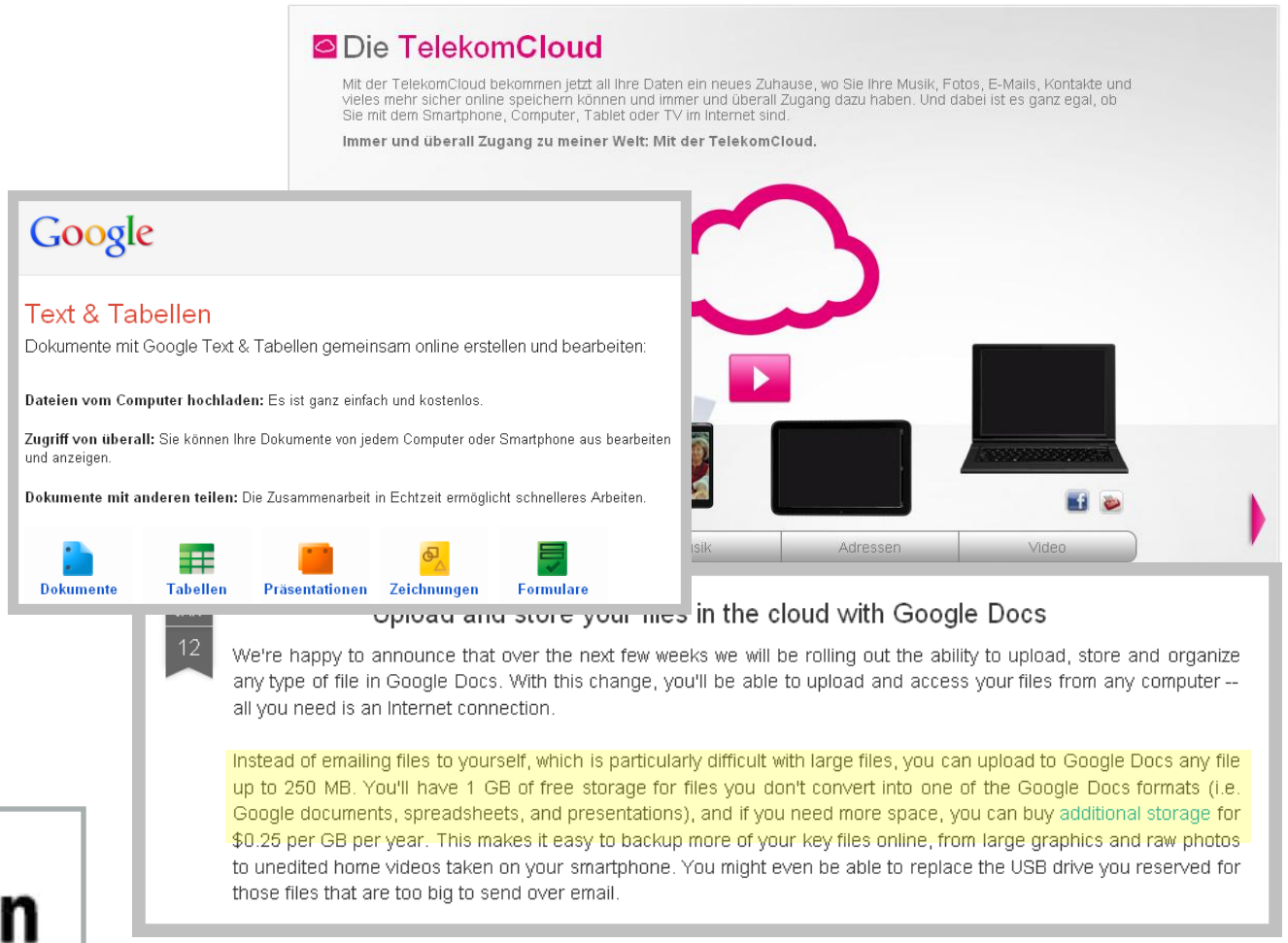
- Seit 1. Juli 2011 selbständiger Münchner Ableger des Fraunhofer SIT
- Ca. 60 Mitarbeiter
- Kompetenzen
  - Embedded Security
  - Cloud & Service Computing
  - Network Security
  - Security Evaluation
  - Smartcard & RFID
  - Automotive Security
  - Smart Grid Security

Abgrenzung

- Private Cloud
  - Nur innerhalb einer Institution
- Public Cloud
  - Gleiche Infrastruktur oder Services für viele Nutzer
  - Hochdynamische Anforderungen
- Cloud Computing, Cloud Web Servers oder Cloud Storage?

Die Cloud als Lösung für alle Probleme?

- Flexibel
- Skalierbar
- Kosteneffektiv
- Sicher
- Verlässlich



amazon web services™

»Die Cloud, auf die Sie sich verlassen können«

Fraunhofer IIS

Gewitter in der Cloud
Der Fall Amazon

amazon web services™

News

Home Newsticker 7-Tage-News News-Archiv Leserforum

heise online > News > 2011 > KW 17 > Wolkenbruch bei Amazon: Datenverlust in der Cloud

28.04.2011 16:30 « Vorige | Nächste »

Wolkenbruch bei Amazon: Datenverlust in der Cloud

vorlesen / MP3-Download

Die Panne des Cloud-Service Amazon EC2 hat schwerwiegende Folgen. Beim Crash des Angebots vergangene Woche ging eine unbekannte Anzahl an Daten unwiederbringlich verloren. Das geht aus einer von Amazon an betroffene Kunden verschickten Mail hervor, welche das US-Magazin Business Insider veröffentlichte. Amazon räumt darin ein, Versuche zur manuellen Wiederherstellung der Kundendaten seien gescheitert.

Nach wie vor hat sich das Unternehmen aus Seattle nicht dazu geäußert, wie es zum mehrstündigen Ausfall der Serverwolke kommen konnte. "Die Cloud, auf die Sie sich verlassen können" (Produktbeschreibung) war bislang nicht zuletzt in der US-Technologieszene äußerst beliebt; zahlreiche viel besuchte Internetdienste wie Foursquare, Quora und Reddit waren von der Störung betroffen und mehrere Stunden lang offline.

Wie viele Unternehmen Daten verloren, ist noch nicht bekannt. Der Webanalyse-Dienst Chartbeat informierte bereits seine Nutzer per Mail, infolge der Panne fehlten für ungefähr elf Stunden Datenaufzeichnungen. (jh)

BUSINESS INSIDER

Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data

Henry Blodget | Apr. 28, 2011, 7:10 AM | 82,801 | 76

Tweet 1,304 Email A A A

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's huge EC2 cloud services crash permanently destroyed some data.

The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is.

(And a small loss on a percentage basis for Amazon, obviously, could be catastrophic for some companies).

Um...

Fraunhofer IIS

Was ist passiert?

- Theoretisch können Nutzer ihre Daten auf verschiedene Regionen verteilen. Aus Performancegründen tut das aber kaum jemand.
- Amazon teilte seine Datencenter deshalb in Zonen auf, die trotz räumlicher Nähe redundant und abgeschottet sind.
- Das Amazon EC2 Cloud Computernetzwerk stürzte während eines Routine-Updates der Server ab.
- Der komplette Traffic wurde durch den Fehler eines Technikers auf ein Backup-System weitergeleitet, welches die Anfragen nicht verarbeiten konnte ebenfalls abstürzte.
- Ein falsch konfigurierter Ausfall-Mechanismus führte daraufhin zu einer Selbstduplizierung sämtlicher Festplatten. Dies resultierte zu einer Fehlerausbreitung innerhalb der Zonen, die das Datenvolumen nicht mehr auffangen konnten.

Déjà-vu?
Heise-Ticker vom 12.10.2009

Datenverlust Sidekick / T-Online

»Der US-amerikanische Mobilfunkanbieter T-Mobile USA hat an diesem Wochenende bekannt gegeben, dass einigen Kunden des Dienstes Sidekick persönliche Daten abhanden gekommen sind und diese voraussichtlich nicht wiederhergestellt werden können. T-Mobile hat in den USA rund 1 Million Sidekick-Geräte verkauft, bei denen Push-E-Mail, Internetzugang oder das Fotoalbum ausschließlich über die Server der Microsoft-Tochter Danger abgewickelt werden.

…

Danger hatte ein Upgrade seines Storage Area Network für Sidekick dem Unternehmen Hitachi überlassen. Beim Start des Upgrades habe es Probleme gegeben, es seien Daten gelöscht worden – und bei Danger gebe es kein Backup.«

Sicherheit in der Cloud generell schlecht bestellt?

NEIN

- Gegenüber kleineren Unternehmen haben CSPs mehr Ressourcen zur Sicherstellung von Sicherheit und Verfügbarkeit.
- Durch die Verteilung in der Cloud sind Anwendungen schwerer durch Denial-of-Service-Angriffe zu stören.

ABER …

- Der Einsatz von Cloud-Services ist häufig kostengetrieben.
- Die Systeme sind komplexer.
- Der Kunde kennt die Infrastruktur des CSPs nicht.
- Der CSP kennt die Anforderungen des Kunden nicht.

Wahl des geeigneten Cloud Service Providers
Sicherheitsaspekte

- Risikoanalyse: Schutzbedarf festlegen
  - Vertraulichkeit
  - Verfügbarkeit
- Auswahlkriterien: Sicherheitsempfehlungen von BSI und NIST
  - Rechenzentren: Lage, Redundanz, bauliche Sicherheit
  - Server: Patchmanagement, Intrusion Detection, Virtualisierung
  - Netze: Firewall, Redundante Anbindung, Schutzzonen, Verschlüsselung
  - Anwendungen: Sandbox, Patchmanagement, Code Review
  - Datensicherheit: Nachvollziehbares Backup, Verschlüsselung
  - Rechtemanagement: Rollenkonzept, Need-to-Know-Prinzip

Vertrauen in den Cloud Service Provider?

- Service Level Agreement (Verhandelbar?)
  - Leistungen
  - Verfügbarkeit
  - Monitoring
  - Reaktionszeiten
  - Backup-Strategie
  - Notfallmanagement
  - Abrechnungsmodell
- Zertifikate und Audits (SAS 70 Type II Audit, ISO/IEC 27001)?

Best Practices für Cloud-Nutzer

- Ganzheitliches Sicherheitskonzept erstellen
- Vertrauensbeziehung zum CSP schaffen
- Notfallplan erstellen
- Daten verschlüsseln, nicht nur während der Übertragung
- Client-Seite sichern (Firewall, Virenscanner)
- Backup auf Nutzer-Seite
- Redundante Internetanbindung
- Starke Authentifizierung
- Zugriffsrechte einschränken, Funktionstrennung
- SLAs kritisch hinterfragen

Anmerkungen zum Datenschutz

- Rechtliche Bestimmungen
  - Auftragsdatenverarbeitung? Nicht der Normalfall!
  - Die Verantwortung für die Daten bleibt beim Cloud-Nutzer
  - Safe Harbor-Zertifizierung von CSPs muss überprüft werden

Verfügbarkeit

- Für jeden Nutzer stellt die verfügbare Verbindung zu seiner Cloud eine kritische Infrastruktur dar, ohne nahezu arbeitsunfähig ist. Aus Kostengründen wird meist keine lokale Verarbeitungs- oder Speichermöglichkeit vorgesehen.
- Stuxnet-ähnliche Angriffe auf große Clouds:
  Mit bis zu einer halben Million physischer Rechner sind große Clouds ein strategisches Ziel. Die Monokultur von Hard- und Software verschärfen die potentiellen Auswirkungen. Viele Kunden würden einen längeren Ausfall wirtschaftlich nicht überleben.
- Was tun, wenn der CSP einfach das Licht ausmacht?
  2009 stellte der Cloud Service Provider Coghead aus wirtschaftlichen Gründen den Betrieb ohne lange Vorwarnung ein.

Datenschutz?
Google sorgt für Irritationen

- Die ersten Fassung der deutschsprachigen AGBs von Google Docs räumten Google das Recht ein, die vom Benutzer erstellten Dokumente weiterzuverwenden.
- Das war wohl ein Übersetzungsfehler, denn in den englischsprachigen AGBs fand sich derartiges nicht.
- Aber: Google unterliegt kalifornischem Recht, AGBs sind jederzeit änderbar und erstrecken sich auch auf alte Datenbestände:

  »**8. Änderungen dieser Nutzungsbedingungen**
  Google kann diese Bedingungen von Zeit zu Zeit anpassen, beispielsweise um rechtliche oder regulatorische Anforderungen umzusetzen oder Funktionsänderungen der Dienste zu berücksichtigen. Sie sollten daher regelmäßig einen Blick auf diese Nutzungsbedingungen werfen. […] Wenn Sie mit den geänderten Bedingungen nicht einverstanden sind, müssen Sie die Nutzung der Dienste einstellen. «

Datenschutz?
Weitere Irritationen

- Das Safe-Harbor-Abkommen ist in der Praxis wirkungslos, wenn sich die Unternehmen nicht an die vereinbarten Grundsätze halten:
  Google speichert Daten nicht nur in den USA, sondern angeblich auch in Toronto, Moskau, Sao Paolo, Tokyo, Hong Kong, Beijing.
  Für den Nutzer ist nicht zu ermitteln, wo sich seine persönlichen Daten befinden, und ob sie tatsächlich vor unbefugtem Zugriff geschützt sind.

- Welches Landesrecht gilt im Fall einer Strafverfolgung?

- In den USA führte die Nichtlokalisierbarkeit der vom Durchsuchungsbeschluss betroffenen Daten bereits zur Beschlagnahme eines kompletten Cloud-Rechenzentrums (in Texas, nicht von Google!).

Einige Quellen im Internet

BSI: Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf

NIST: Guidelines on Security and Privacy in Public Cloud Computing
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

Fraunhofer AISEC: Cloud-Security 2009
http://www.aisec.fraunhofer.de/content/dam/sitmuc/de/pdf/studien/studie-CloudComputingSicherheit.pdf

Galexia: The US Safe Harbor - Fact or Fiction?
http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

EuroCloud Deutschland_eco
http://www.eurocloud.de

Fragen?

Dr.-Ing. Rainer Ulrich

Fraunhofer-Institut für Integrierte Schaltungen

IT-Security

Am Wolfsmantel 33

91058 Erlangen

rainer.ulrich@iis.fraunhofer.de

+49 9131 776-2740