Sicherheitsfragen und Probleme im Umfeld des Cloud Computing

IKT-Forum: Wolkig bis heiter – Cloud Computing im Unternehmen

Hochschule Ansbach, 10.12.2013

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

Fraunhofer IIS

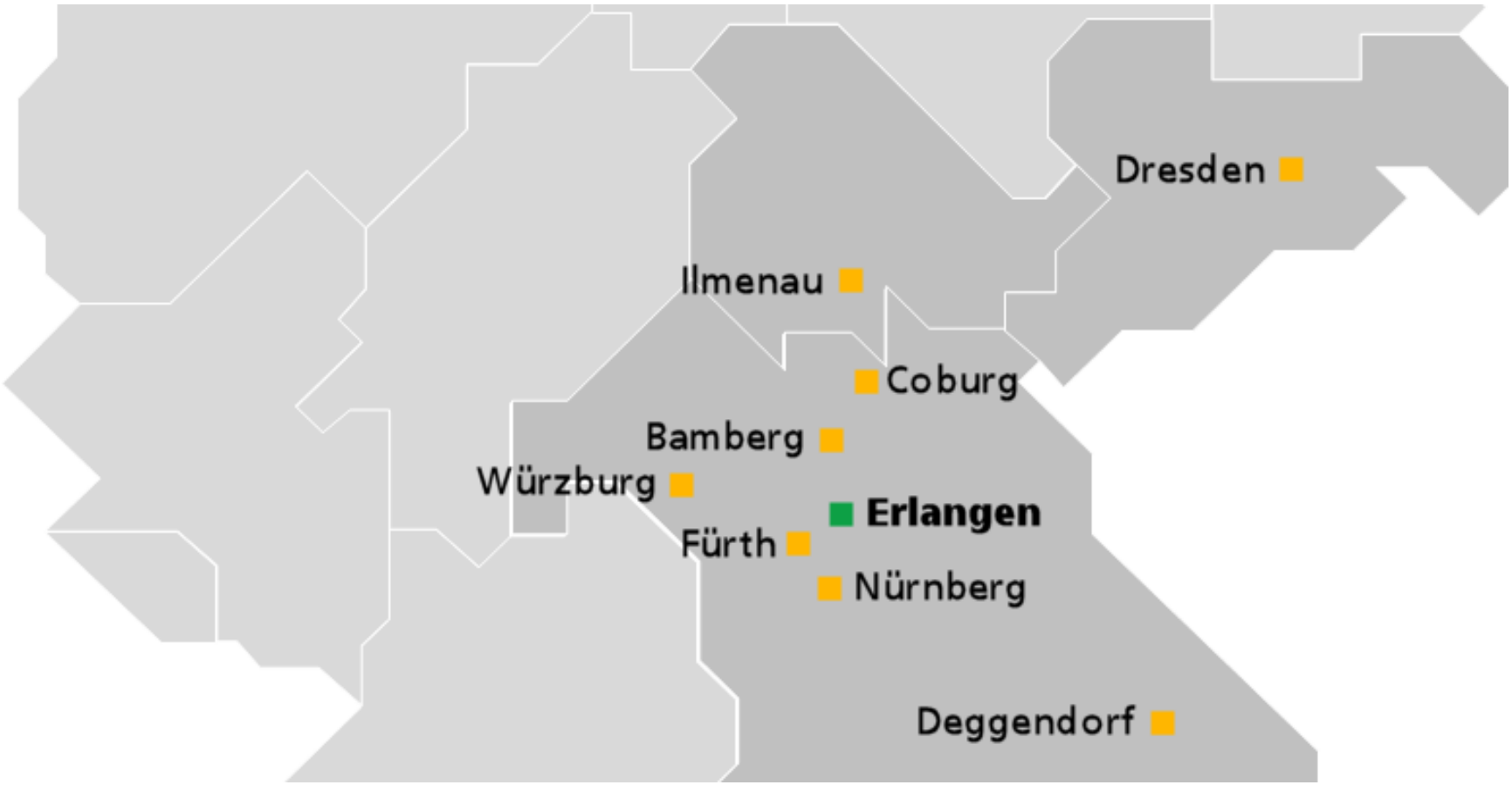
Fraunhofer-Institut für Integrierte Schaltungen IIS

Überblick

Fraunhofer IIS

Fraunhofer-Institut für Integrierte Schaltungen IIS

Standorte



Fraunhofer IIS

Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit AISEC

- Ca. 70 Mitarbeiter
- Kompetenzen
  - Embedded Security
  - Cloud & Service Computing
  - Network Security
  - Security Evaluation
  - Smartcard & RFID
  - Automotive Security
  - Smart Grid Security

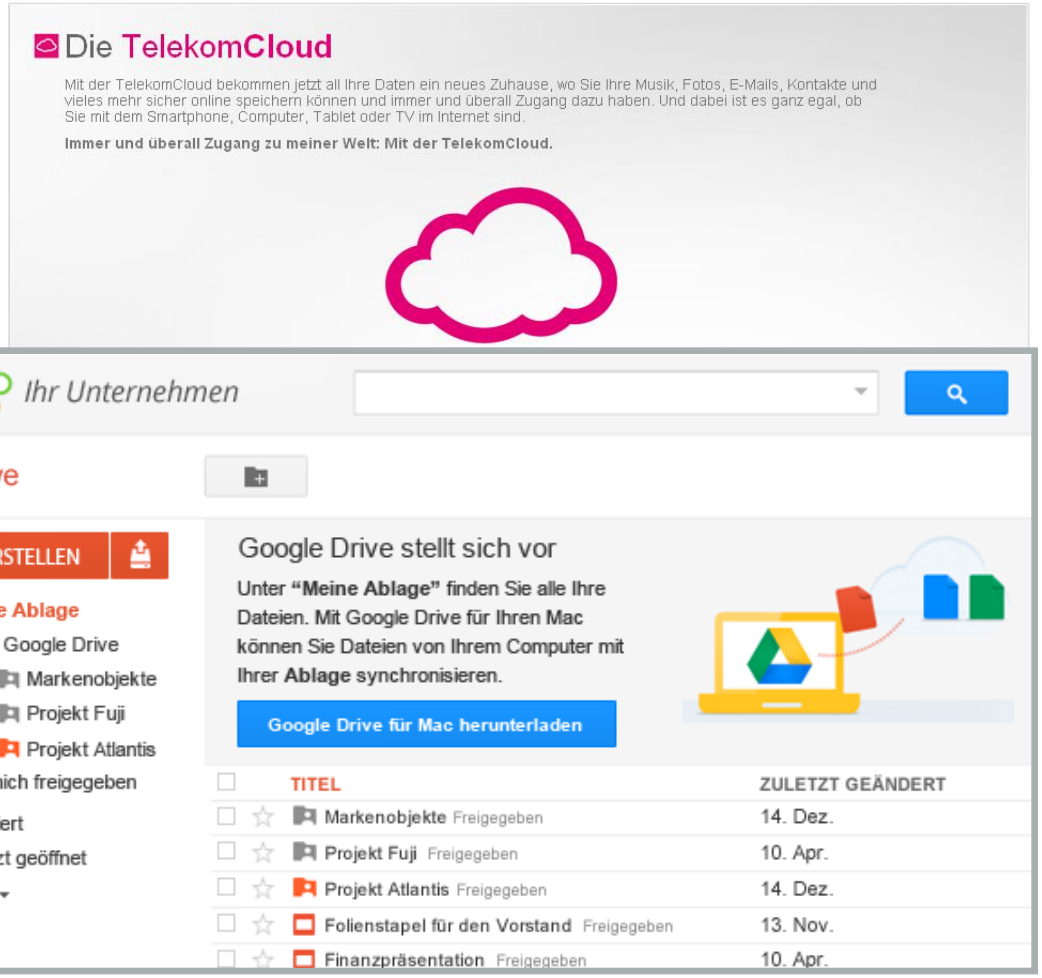
Abgrenzung

- Private Cloud
  - Nur innerhalb einer Institution
- Public Cloud
  - Gleiche Infrastruktur oder Services für viele Nutzer
  - Hochdynamische Anforderungen
- Hybrid Cloud

- Cloud Computing, Cloud Web Servers oder Cloud Storage?

Die Cloud als Lösung für alle Probleme?

- Flexibel
- Skalierbar
- Kosteneffektiv
- Sicher
- Verlässlich



amazon web services™

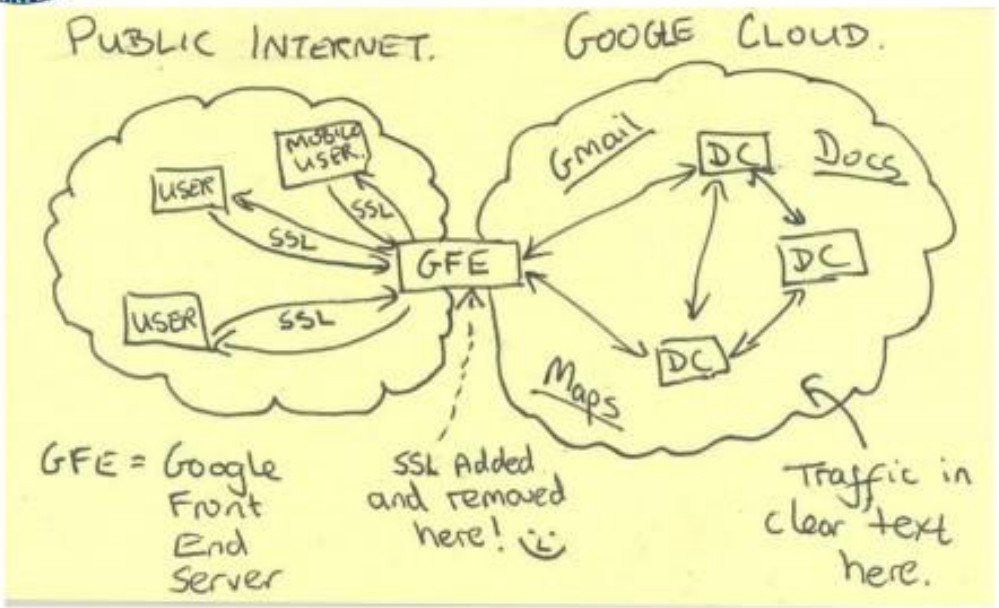
»Die Cloud, auf die Sie sich verlassen können«

2013: Big Brother Is Watching You

Was können NSA und GCHQ?

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

Quellen: Heise, Spiegel, Washington Post

2011: Gewitter in der Cloud

Der Fall Amazon

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...

Was war 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 komplex.
- Transportverschlüsselung allein ist nicht ausreichend.
- Die Verbindung zu Cloud ist eine kritische Infrastruktur.

Wahl des geeigneten Cloud Service Providers
Sicherheitsaspekte

- Business Impact Analyse: Schutzbedarf festlegen
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
- Auswahlkriterien: Sicherheitsempfehlungen von BSI, NIST, Fraunhofer
  - 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
  - Umgang mit sensitiven Daten

Vertrauen in den Cloud Service Provider?

- Service Level Agreement (Verhandelbar?)
  - Leistungen
  - Ort der Leistungserbringung, Gesetze
  - Verfügbarkeit
  - Monitoring
  - Reaktionszeiten
  - Backup-Strategie
  - Notfallmanagement
  - Abrechnungsmodell
  - Regelungen zu Betriebseinstellung und Vertragsende
- 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 ist weitgehend wertlos:
  - Speicherort der Daten nicht transparent
  - US-Sicherheitsbehörden habe Zugriff auf die in US-Clouds gespeicherten Daten
  - Ausländisches Recht erlaubt es, allgemeine Geschäftsbedingungen jederzeit einseitig zu ändern

Anmerkungen zur Verschlüsselung

- Verschlüsselung ist sicher, wenn
  - der Angreifer die Schlüssel errechnen muss
  - die Algorithmen ohne Fehler implementiert wurden
  - die Schlüssel lang genug sind
  - aus der Kenntnis eines Schlüssels nicht alle bisherige Kommunikation entschlüsselt werden kann

Anmerkungen zur 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.
- 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.

Einige Quellen im Internet

Dell: Der Umgang mit veränderten IT-Anforderungen
http://i.dell.com/sites/doccontent/business/smb/sb360/de/Documents/17595-Servers-Storage-Report-Feb-2012-PDF-V02-SM-LR-de.pdf

BSI: Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter
https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

BSI: Notfallmanagement mit der Cloud für KMUs
https://www.bsi.bund.de/DE/Themen/CloudComputing/Studien/Studien_node.html#doc2532408bodyText1

Fraunhofer AISEC: Cloud-Security 2009
http://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/studie-CloudComputingSicherheit.pdf

NIST: Guidelines on Security and Privacy in Public Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

EuroCloud: Cloud-Verträge: Was Anbieter und Kunden besprechen sollten
http://www.eurocloud.at/fileadmin/userdaten/dokumente/broschuere-cloud-vertraege.pdf

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