Privacy aspects of Cloud Computing
Survey of Dell and Intel (2012)

1500 interviewed persons of small companies:

28% are against Cloud Computing
35% are not familiar with the topic

→ “tremendous fear“ for sensible data

Survey of Dell and Intel (2012)

Quotes about Cloud Computing of those polled:

- “The structure of the Cloud is not convincing.“
- “The biggest problem is: the subject matter is not tangible for me.“ (head and founder of Devision Coding, Offenbach)
- “Every incidence shaking confidence (in the media) is throwing companies back in their decisions (about using Clouds).“ (head of Datev, Berlin)

Opinion of George Colony, head of market researcher Forrester Research about CC

• “Germany has the most conservative IT managers. Conservative companies need the possibility to give those services a trial.“

• “Europe is 24 months behind in IT trends. In Germany it takes even longer.“

• “Cloud Computing is the last IT trend to be established in Germany.“

Certificates: solution for the trust issue?

• In the US:
  SAS70 (Statement on Auditing Standard No. 70)
  → No validity period

• In the EU:
  ISO/IEC 27001 and 27002 issued by the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission)
  → 3 years validity

• Since 2011 first specific Cloud Auditing:
  EuroCloud (in coordination with German BSI)
EuroCloud

Requirements for a 4 stars “Seal of Approval“:

✔ providing of VPN access
✔ encryption on data level
✔ restrictions for administrator access
✔ authentication and authorization can be managed by the Cloud service customer

In order to get 5 stars (top grade):

✔ additionally perform a penetration test and hand the results in to the EuroCloud - commission
“Auditing of the Auditing“

This CC certificates still need to prove themselves in practice, because:

→ Specialized Cloud Auditing is new
→ Other auditing forms are not suited for CC

Consequence: may not solve trust issue
Server Locations

- Most Cloud providers are based in the US → Patriot Act/NSA – you know the story
- Also non American Cloud Providers have their servers situated in the US

⚠️ Transparency about server locations essential
Encryption variants used for storage

- No encryption at all e.g. CloudMe, Ubuntu One
- Client-sided encryption e.g. CrashPlan, Mozy, Wuala, TeamDrive
- Server-sided encryption e.g. Dropbox
  - Trust in provider?
- Local self-encryption
  - Not always supported
  - Conflicts may occur
Quote from Ubuntu One FAQs

„We do not store your files encrypted in our data storage since we need them unencrypted in order to send them to the people you choose to share with. If you are concerned about storing your files unencrypted in the Ubuntu One cloud, you could always store the files already encrypted so Ubuntu One never sees the plain text files.

Doing so may prevent the proper functionality of some Ubuntu One features such as multiple computer synchronization, web browser access, and sharing with others.“

Source: https://one.ubuntu.com/help/faq/what-security-and-privacy-policies-does-ubuntu-one-have/
European Cloud on the run?

- Cloud market dominated by American providers

- SAP is investing in its Cloud business and therefore is upsetting its investors

- Dreams of the future:
  A Cloud „made in Germany“, superior in issues of data privacy and safety
What has to be protected?

Privacy can be compromised at various points:

- physical systems
- operating systems
- middleware
- applications
- transport path
Trusted Cloud initiative of the BMWi

• Start: in September 2010 as a technological competition (innovative, secure, lawful)

• 14 winners (26 companies of different sectors and 26 science departments) started their projects in September 2011

• Investment: 100 million euros
  - one half of the German Bund:
  - one half of the participants
2 examples of Trusted Cloud

- **MimoSecco:** Middleware for Mobile and Secure Cloud Computing  
  → project duration: till March 2014

- **Sealed Cloud:**  
  → project duration: till March 2014

Web Privacy Service by *Uniscon* IDGARD already implemented infrastructure of Sealed Cloud
MimoSecco

Goal: both efficiency and confidentiality while working with encrypted files

→ Therefore, data is distributed between:

I. a data sever
II. several index servers
III. a trustworthy databank adapter server
Principle of MimoSecco

Abb. 2: Funktionsprinzip des Datenbankadapters
Different trust levels at MimoSecco

Abb. 1: Zonenmodell von MimoSecco
Sealed Cloud

Goal: an infrastructure to prevent insider attacks

→ Admin only gains access to application server after a data clean-up

→ System only reboots after maintenance after
  - software integrity
  - hardware integrity

is checked (+ permanent monitoring)
Sealed Cloud

Neue Basistechnologie für unternehmenskritische Anwendungen

Admin

herkömmliche Cloud-Technik

Standard Heute
Verschlüsselte Übertragung

Wunschdenken vertrauenswürdiger Administrator

Best-Practice Heute
Verschlüsselte Datenbank

Admin

Sealed Cloud

echte Betreibersicherheit

Versiegelte Verarbeitung
Principle of Sealed Cloud

Cloud User A

Computer/Device
Browser/App.
Crypt.

Cloud User B

Computer/Device
Browser/App.
Crypt.

Static & Dynamic Testing
External Auditors

Cloud Operator

Sealed Cloud
Sealing Control
Encrypted Database
Data Clean-up Area
Application Server
App. Software
Encrypt. File System/Mass Storage
Cloud Control & Perimeter Security

Static & Dynamic Auditing
Certification
Technical Dynamic Examination

Application Operator

Application SW Development
Application SW Production

Static Auditing

Technical & Organizational Static examination

SW Deployment
Canonical set of technical measures... safeguarding against insider attacks:
The Web Privacy Service of Uniscon (universal identity control GmbH) provides:

- an Email/chat option
- a proxy option for browsing
- a Cloud storage system based on Sealed Cloud

“designed for the secure exchange of data between business partners” (Uniscon)
No escapin´this?

Research program “Penetrating Hard Targets” of NSA includes plans to built a quantum computer.

“With such technology, all current forms of public key encryption would be broken,(...)

(The Washington Post)

VS.

“It seems improbable that the NSA could be that far ahead of the open world without anybody knowing it.”

(Scott Aaronson, associate professor MIT)