Compliance in Clouds
A cloud computing security perspective

Kristian Beckers, Martin Hirsch, Jan Jürjens

GI Workshop: Governance, Risk & Compliance on the 19th of March 2010
What is Cloud Computing?

Today:

(Source: IPVS, University Stuttgart)
What is Cloud Computing?

Services in the Cloud:

(Source: IPVS, University Stuttgart)
What is Cloud Computing?

The illusion of infinite resources available on demand
The elimination of an up-front commitment by Cloud users
The ability to pay for use of computing resources on a short-term basis as needed

(Source: Berkley, Above the Clouds, 2009)
Security is the Major Issue

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

- Security: 74.6%
- Performance: 63.1%
- Availability: 63.1%
- Hard to integrate with in-house IT: 61.1%
- Not enough ability to customize: 55.8%
- Worried on-demand will cost more: 50.4%
- Bringing back in-house may be difficult: 50.0%
- Regulatory requirements prohibit cloud: 49.2%
- Not enough major suppliers yet: 44.3%

©Source: IDC Enterprise Panel, August 2008, n=244
The NIST Cloud Definition Framework

Deployment Models
- Private Cloud
- Community Cloud
- Public Cloud

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Essential Characteristics
- On Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Common Characteristics
- Massive Scale
- Homogeneity
- Virtualization
- Resilient Computing
- Geographic Distribution
- Service Orientation
- Low Cost Software
- Advanced Security

(Source: NIST, Effectively and Secure using the Cloud Paradigm, 2009)
## Cloud Security Goals

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Data processing in the cloud is still unencrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Encrypted data storage in the cloud: Shared DB</td>
</tr>
<tr>
<td></td>
<td>Encrypted data exchange with the cloud: Secure Internet Link</td>
</tr>
<tr>
<td>Availability</td>
<td>Protection of the virtual space of the clouds from e.g. overwrites</td>
</tr>
<tr>
<td></td>
<td>Redundant clouds / data storage</td>
</tr>
<tr>
<td>Integrity</td>
<td>Prevent unwanted and unrecognized data modification in the cloud</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Authentication of cloud systems to users</td>
</tr>
<tr>
<td></td>
<td>and vice versa!</td>
</tr>
<tr>
<td>Non Repudiation</td>
<td>Business transactions in clouds require signatures</td>
</tr>
<tr>
<td></td>
<td>Independent checks of the signatures</td>
</tr>
<tr>
<td>Privacy</td>
<td>Prevent user profiling</td>
</tr>
<tr>
<td></td>
<td>Conflicting with Non Repudiation</td>
</tr>
</tbody>
</table>
Cloud Computing Security Issues

- Mistakes/Attacks from employees of the provider
- Attacks from other customers
- Attacks on the availability
- Mistakes in the provisioning and the management
- Misuse of the provider platform
- Web-Service based attacks

(Source: BSI, IT-Grundschutz und Cloud Computing, 2009)
Security in Clouds is a Trust Issue

A good way to generate trust for a cloud vendor is transparent security.
## GRC in Clouds

<table>
<thead>
<tr>
<th>Governance</th>
<th>Risk</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Policy design</td>
<td>- Risk strategy</td>
<td>- Policy enforcement</td>
</tr>
<tr>
<td>- Classification schema for data and processes</td>
<td>- Business Impact Analysis</td>
<td>- Legal compliance (SOX, SOLVENCY II)</td>
</tr>
<tr>
<td>- Trust chain in a cloud</td>
<td>- Threat and Vulnerability Analysis</td>
<td>- Control implementation</td>
</tr>
<tr>
<td></td>
<td>- Risk Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Remediation</td>
<td></td>
</tr>
</tbody>
</table>

The Cloud offers dynamic resource allocation  
→ For GRC in clouds we require the same dynamic
# Cloud GRC Related Standards

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Gartner</th>
<th>ISO</th>
<th>International Organization for Standardization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holistic Control Systems</td>
<td>COBIT</td>
<td>COSO</td>
<td></td>
</tr>
<tr>
<td>Security Standards</td>
<td>Common Criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency</td>
<td>Safe Harbor</td>
<td>SAS 70</td>
<td></td>
</tr>
</tbody>
</table>

© Fraunhofer ISST
Security Level Assurance (SLA)

- Precise description of the offered services and the expected limitations!
- Compare different SLAs for my needs.
  - Does a cloud vendor offer an SLA at all?
- What do the numbers mean: 99.8% per anno availability:
  - ~ 17.5 hours per year the cloud is offline!
- What are the penalties for SLA violations?
  - Can I monitor the performance of the cloud?
  - Does an early warning system exist?
- Is the cloud segregated into different security levels?
  - Do I need to separate my data before giving it to the cloud?
  - Should I avoid top secret data to enter the cloud?
Cloud Security Vendor Evaluation

- Physical Security of the data center:
  - Googles Security Operations Center
  - Amazon: Two factor authentication
- Attacks on the networks level, e.g., Denial-of-Service:
  - Amazon uses Denial-of-Service Prevention, but the method is secret
  - Microsoft uses Load-Blanacer and Intrusion Prevention Systems
- Backup Solutions:
  - Google, Amazon execute Backups on different physical locations
  - FlexiScale executes Backups, but users cannot retrieve lost data
  - Amazon stores data in an unencrypted fashion
  - Amazon stores data permanent → after it is 5 Minutes in the cloud
## Security certificates of the cloud vendors

<table>
<thead>
<tr>
<th>Vendor</th>
<th>TRUSTe</th>
<th>Safe Harbor</th>
<th>SAS 70 Type II</th>
<th>ISO/IEC 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Google</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Salesforce</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PingIdentity</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Postini</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CohesiveFT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalr</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RightScale</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>GoGrid</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>FlexiScale</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rackspace</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LongJump</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Source: Fraunhofer SIT, Cloud Computing Sicherheit, 2009)
Security as a Service

- Google Message Security
  - 12$ per anno - per user

- Identity Management von PingIdentity
  - 1€ per user - per application - per month

- VPN-Cubed for EC2 von CohesiveFT
  - Connection of 2 Servers are for free
  - Connection of 4 Servers are 0.05$ per hour
Compliance

Compliance is the adherence of regulations. These can be legal regulations, governance regulations or regulations of any other kind. In the context of this work we use compliance as the goal to adhere to laws and security goals.

The automated verification of security goals supports the build up of trust between a cloud vendor and its customers.

Compliance checks can also verify the business processes of a cloud user for legal issues: SOX, EURO-SOX, BASEL II, SOLVENCY II

Business process compliance is possible in two ways:

- Compliance by design, Compliance generation
- Compliance validation
Compliance Scenarios

- Customer → Cloud:
  - Security Compliance:
    - Check the security processes of the cloud to compliance with SLA
  - Legal Compliance:
    - Check the business process for SOX, MaRisk compliance
- Cloud → Cloud:
  - Contract Compliance:
    - Check the interaction of two business partners in the cloud
- Cloud → Customer:
  - Security Compliance:
    - Inspect the processes for cloud behavior violation
Trust is good, Compliance is better

- Business Process Analysis of the clouds IT security properties.
Example Cloud Authentication

- We aim towards an automated compliance analysis
- The analysis will work in two phases:
  1. A structure analysis of the EPC for a possible compliance violation pattern
  2. Second a text-based analysis of the word in the EPC functions
Example Cloud Authentication

- A structure analysis of the EPC for a possible compliance pattern
- The EPC needs to be augmented
- Verification against a control pattern against the (Meta-)Model of the EPC

Customer requests a connection

Cloud system asks for credentials

Customer sends credentials

Cloud system checks credentials

Customer

Credentials

Credentials are correct

Cloud system grants access

Customer

Credentials are wrong

Cloud system refuses access

Customer

: Cloud System

: Customer

: Login

: Credentials
Example Cloud Authentication

- A text-based analysis of the word in the EPC functions
- The functions of the EPC are checked for the words

Identify an compliance relevant task:
Look for words: Credentials, Login, Check, Verification that hint towards an authentication
Automated cloud risk identification and aggregation

Risk-Data Repository

- Risk_A
- Risk_E
- Risk_F
- Risk_B
- Risk_G
- Risk_C
- Risk_D
- Risk_H

Customer requests a connection

Cloud system asks for credentials

Customer replies

Cloud system checks credentials

Risk factor 25

Credentials are correct

Cloud system grants access

Credentials are wrong

Cloud system refuses access

Application

\(=P(X)\)
CloudAudit (A6) Overview

A6 is the geeky byline for the working group of CloudAudit and stands for:
Automated Audit, Assertion, Assessment, and Assurance API

The goal of CloudAudit is to provide a common interface that allows Cloud providers to automate the Audit, Assertion, Assessment, and Assurance of their environments and allow authorized consumers of their services to do likewise via an open, extensible and secure API.

(Source: Cloud Audit A6 Group)
A simple cloud check list

- Is the security of the vendor documented?
  - How are security levels maintained?
- Is it possible to withdraw from the cloud with little effort?
- What Guarantees / Service Level Agreements (SLA) exist?
  - Can they be tailored to the customers need?
  - Which penalties are in the standardized SLAs?
  - How can the vendor enforce an SLA?
- What kind of cloud monitoring capabilities exist?
- Where is the physical location of the cloud?
  - Which laws apply there?
  - Can I enforce the usage of German law ("Rechtswahl")?
  - Are German privacy laws enforced?
“Trust is a concept as old as humanity, and the solutions are the same as they have always been. Be careful who you trust, be careful what you trust them with, and be careful how much you trust them. Outsourcing is the future of computing. Eventually we'll get this right, but you don't want to be a casualty along the way.”

(Source: Bruce Schneier, Schneier on Security: Cloud Computing, 2009)
Where can I learn more?

- IT-Grundschutz und Cloud Computing, SECMGT Workshop, BSI, 2009
- Cloud Security, TÜV Informationstechnik GmbH, 2009
- Effectively and Securely Using the Cloud Computing Paradigm, NIST, 2009