Cloud Security
Introduction and Overview

Klaus Gribi
Senior Security Consultant

klaus.gribi@swisscom.com

May 6, 2015

swisscom

Cloud Security
Agenda

1. Cloud Security
   - Cloud Evolution, Service and Deployment models
   - Overview and the Notorious Nine
   - Concerns of the Cloud consumers
   - Traditional Security versus Cloud Security
   - The 14 Domains of Cloud Security
   - Best Practices and Guidelines
   - Some hints about Cloud Security
   - Information and Data classification
2. Introduction to Cloud Security Alliance (CSA)
   - CSA Global
   - CSA Switzerland Chapter

Cloud evolution

Which steps we need for Cloud Computing?

- **Dynamic provisioning**
  (Pay as you go, scale up and down)
- **Shared resources**
  (common workload profiles, multi-tenant)
- **Automation** (Self service, flexible deployment)
- **Standardisation** (Increase operational efficiency)
- **Virtualisation** (optimizing the utilization)
- **Consolidation** (physical infrastructure)

Preparatory steps

Traditional IT

Cloud definition
The 5 Cloud characteristics (NIST) I/II

Characteristic	Description
On-Demand Self-Service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically **without requiring human interaction** with each service provider.
Broad Network Access	Capabilities are available **over the network** and **accessed through standard mechanisms** that promote use by **heterogeneous thin or thick client platforms** (e.g., mobile phones, tablets, laptops and workstations)
Resource Pooling	The provider's computing **resources are pooled** to serve multiple consumers **using a multi-tenant model**, with different physical and virtual resources **dynamically assigned and reassigned** according to consumer demand. There is a **sense of location independence** in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

swisscom

Cloud definition
The 5 Cloud characteristics (NIST) II/II

Characteristic	Description
Rapid Elasticity / Scalability	Capabilities can be **elastically provisioned and released**, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning **often appear to be unlimited** and can be appropriated **in any quantity at any time**.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction **appropriate to the type of service** (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be **monitored, controlled, and reported**, providing transparency for both the provider and consumer of the utilized service

swisscom

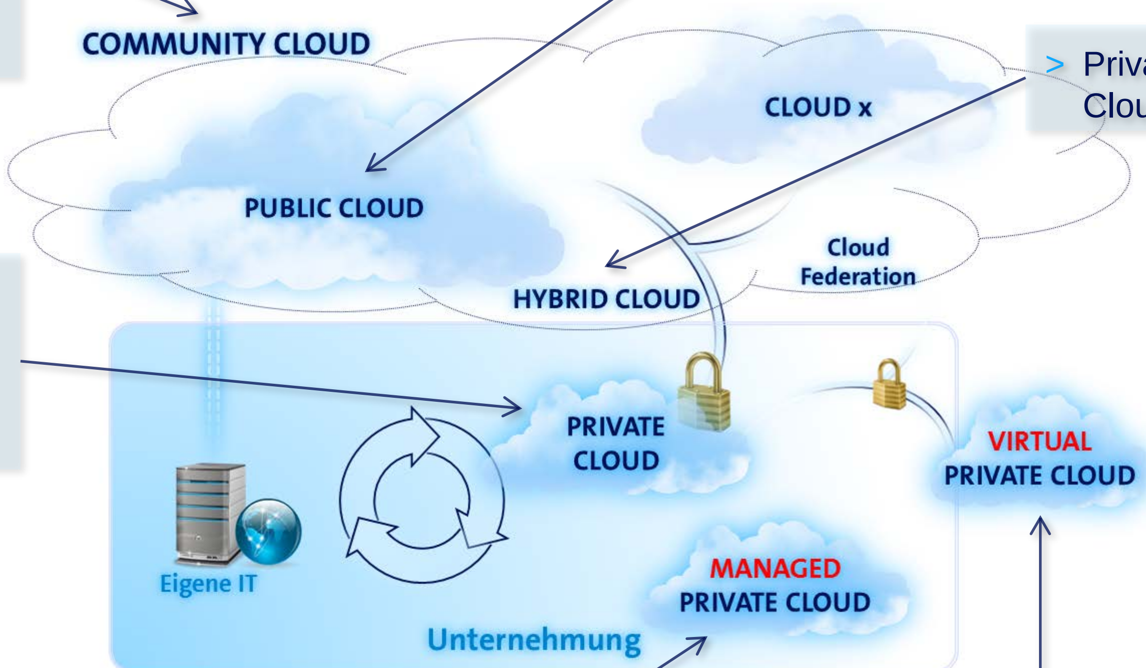
Cloud definition
Deployment models (NIST)

- Clouds which serve a special purpose or which have special requirements (for example financial Clouds)

- **Off Premise**
- Provider Data Center
- Provider managed

- Private and Public Cloud interconnected

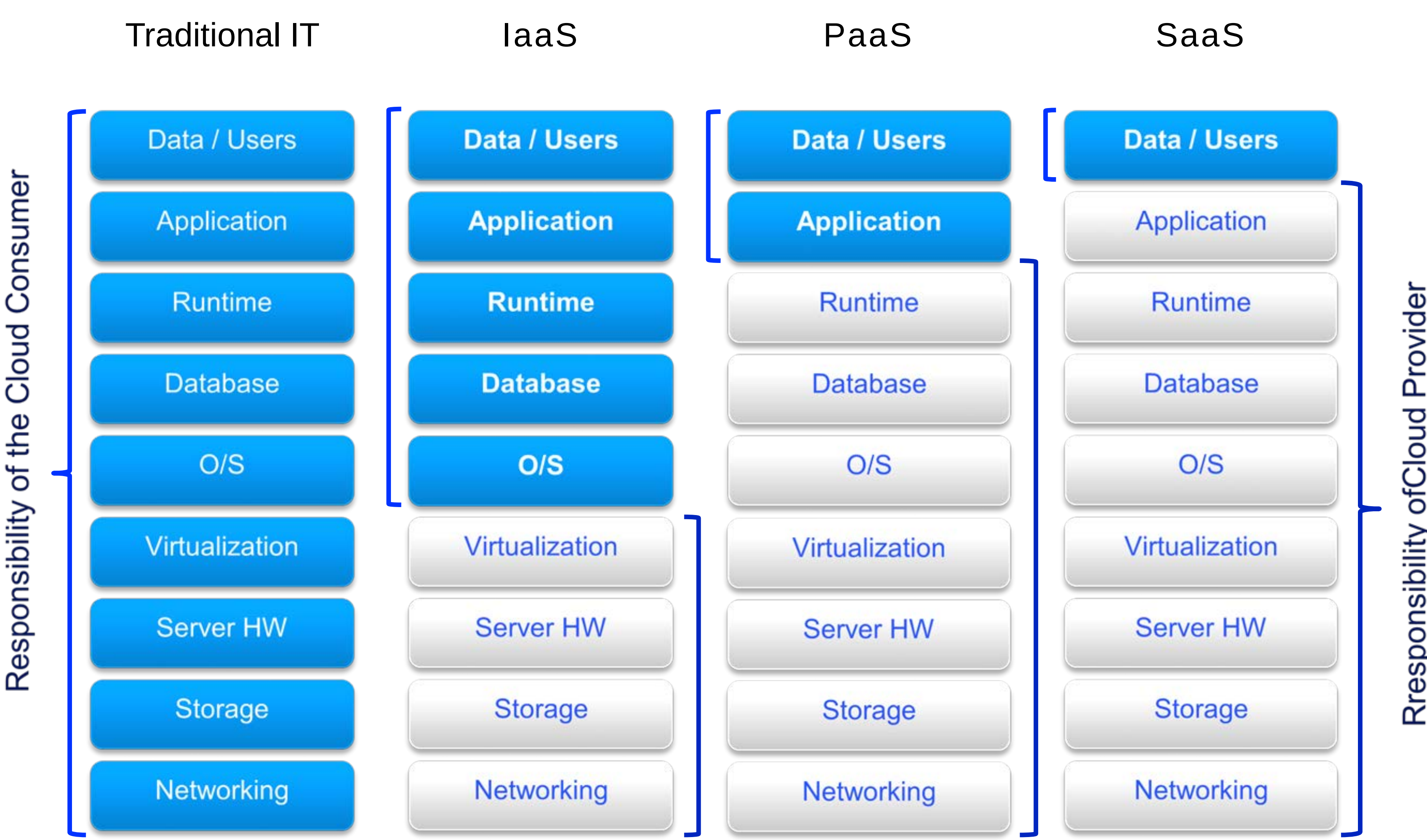
- **On Premise**
- Enterprise Data Center
- Self managed



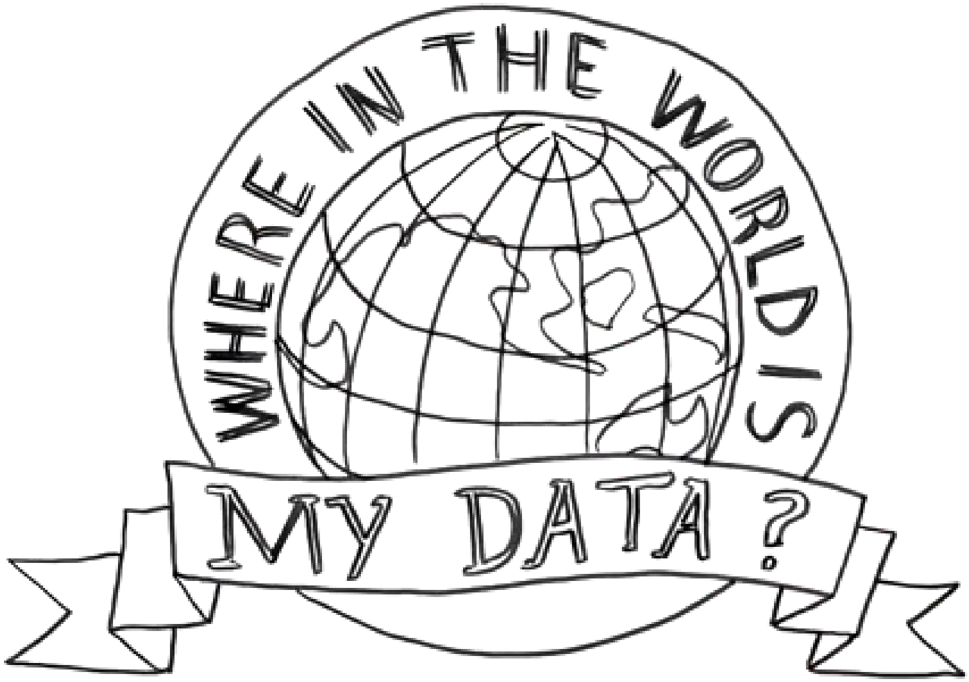
- **On Premise**
- Enterprise Data Center
- Provider managed

- **Off Premise**
- Provider Data Center
- Self- or provider managed

Cloud definition
Service models (NIST)



Cloud Security
A movie says more than 1000 words



Cloud Security
Overview over the Cloud consumers view

40%
der Unternehmen in Deutschland nutzen Cloud-Computing, weitere 29 Prozent planen oder diskutieren den Einsatz.

51%
der Unternehmen haben Konsequenzen aus dem NSA-Überwachungsskandal gezogen.

24%
des IT-Budgets werden durchschnittlich für Private Cloud-Lösungen ausgegeben. Der Anteil der Aufwendungen für Public Cloud-Lösungen ist mit 12 Prozent halb so groß.

83%
der Private Cloud-Nutzer und 67 Prozent der Public Cloud-Nutzer beurteilen ihre bisherigen Erfahrungen als positiv.

61%
der Cloud-Nutzer haben seit den NSA-Enthüllungen weniger Vertrauen in ihre Cloud-Anbieter.

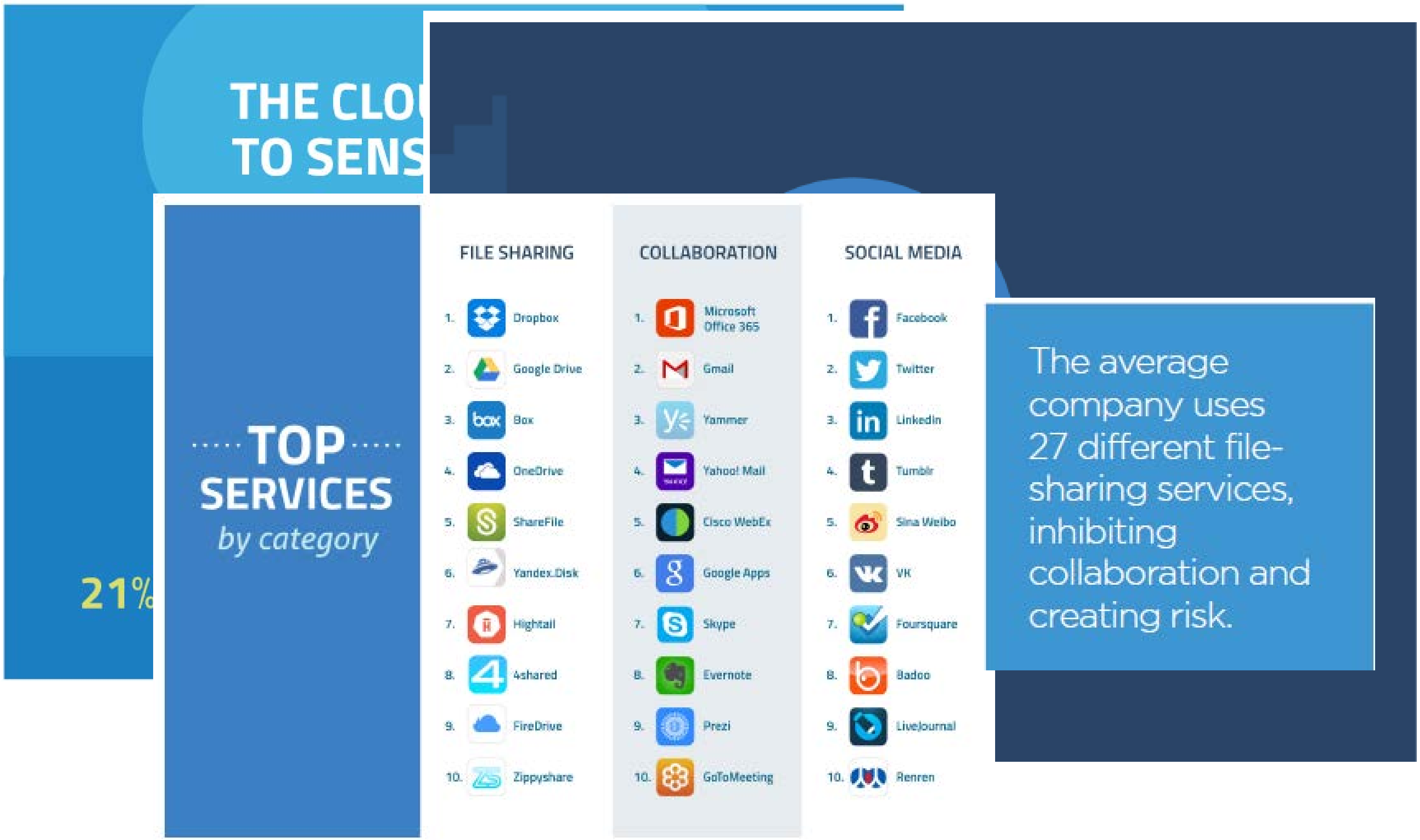
74%
der Unternehmen sehen Angriffe auf ihre Computer und Datennetze durch Cyberkriminelle oder Geheimdienste als reale Gefahr.

49%
der Unternehmen sagen, dass die NSA-Affäre ihre Einstellung zum Public Cloud-Computing negativ beeinflusst hat. Für die Private Cloud ist der Wert mit 44 Prozent fast genauso hoch.

25%
der Befragten befürworten eine nationale Cloud, auch wenn sie mit Mehrkosten verbunden ist.

Source: KPMG Cloud Monitor 2014

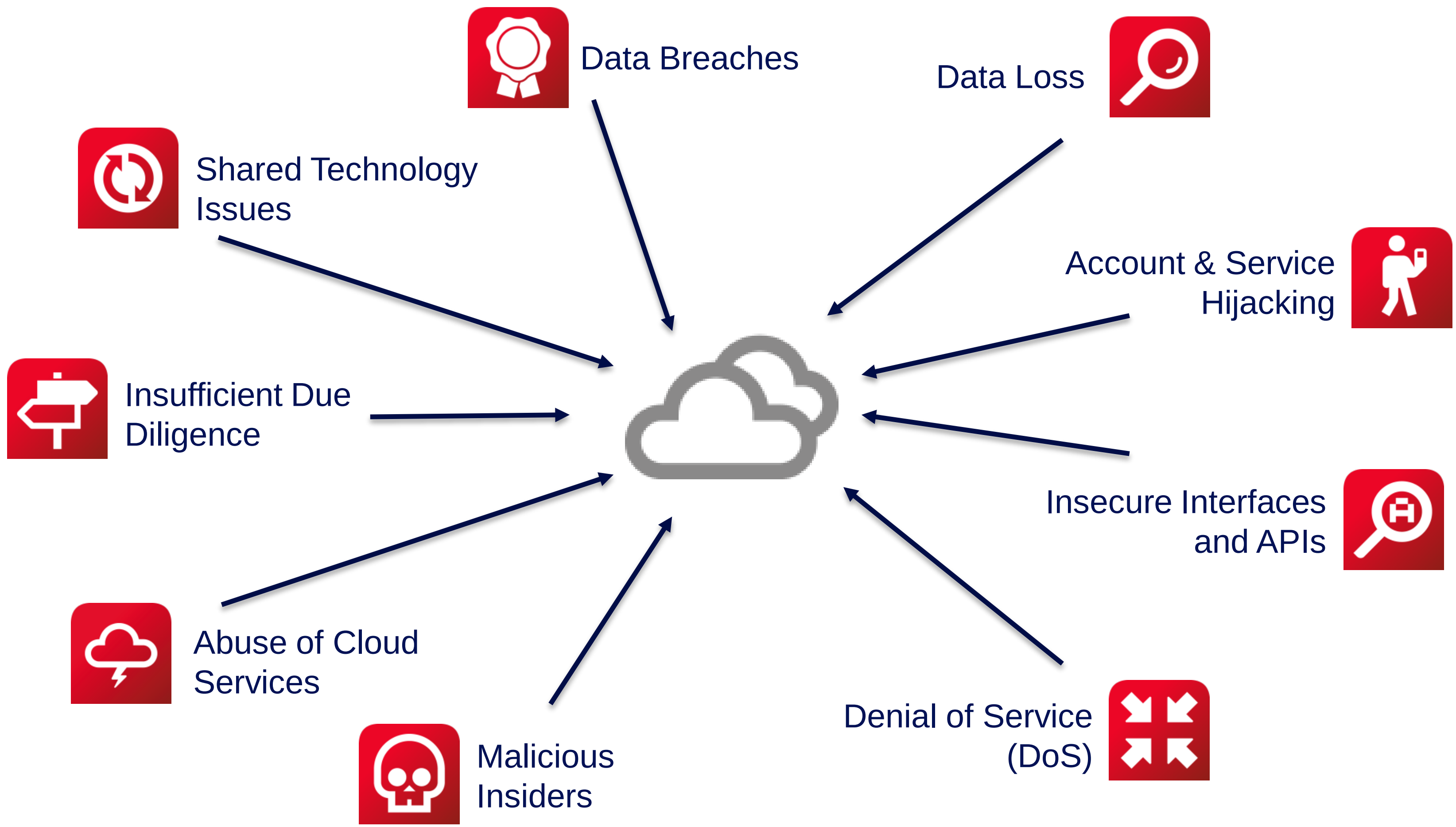
Cloud Security
Some information from a Cloud Security company



Source: Skyhigh Networks Cloud Adoption and Risk Report: Q4 2014

Cloud Security

The Notorious Nine



Source: Cloud Security Alliance - The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013

Cloud Security

Security concerns of the Cloud consumers

- Missing trust to the Cloud Service Provider
- Loss of control and Know How
- Physical control over the data is lost
- Data access by unauthorized persons
- The classical security perimeter is lost
- The well known and reliable IT operation takes no longer place on premise
- Complex technologies vulnerabilities (strong virtualization)
- Economic espionage taking place
- Compromised encryption
- Lack of accountability, unclear responsibilities of the CSP's
- Questioning the reliability and transparency of the CSP's
- Secure integration into the own on premise IT can be difficult
- Secure interoperability with other cloud services is not given

Cloud Security

Traditional Security vs. Cloud Security I/II

- Adaption of the Security organization and processes
  - How to extend the CSIRT to the Cloud?
  - Monitoring security incidents
  - How to do forensics in the Cloud?
- Which external and internal Governance and Compliance aspects must be taken into account (for example PCI/DSS in the Cloud)?
  - Cloud Usage Policy
  - Outsourcing Policy
- The safe operation of the IT platform is no longer on premise
  - Loss of control and know how (IT operation, problem analysis)
  - Loss of important operating and monitoring data (for example Firewall-, IPS- and Proxy Server logs)
  - Loss of Data retention and Data deletion control

Cloud Security

Traditional Security vs. Cloud Security II/II

- The Cloud consumer may be subject to international law, for example
    - Data Privacy Law (look at the Federal Data Protection and Information Commissioner states list)
    - Business Books Regulation in Switzerland
    - Patriot Act / Foreign Intelligence and Surveillance Act (FISA)
- Ensuring Information Security at high virtualization- and automation degrees (Server-, Network, Client-, Storage-, Application-Virtualisation)
    - Access Control
    - Tenant isolation in a Cloud platform
- Which additional standards must be met (ISO 27018 – PII protection in the Cloud, ISAE 3402 - Effectiveness of the internal Control Systems, ISO 37500 – Guideline Outsourcing, ISO 27017 – Cloud Security etc.)?

Cloud Security

The 14 Cloud Security domains

Cloud Security

D1: Secure Cloud Architecture

Governing in the Cloud

- D2: Governance and Risk Management
- D3: Legal Issues
- D4: Compliance a
- D5: Information M
- D6: Interoperabilit

Operating in the Cloud

- D7: Traditional Security and BCM / DR

ations

e

rity

Key Management

ent and Access Mgmt

rvice

Cloud Trust Model

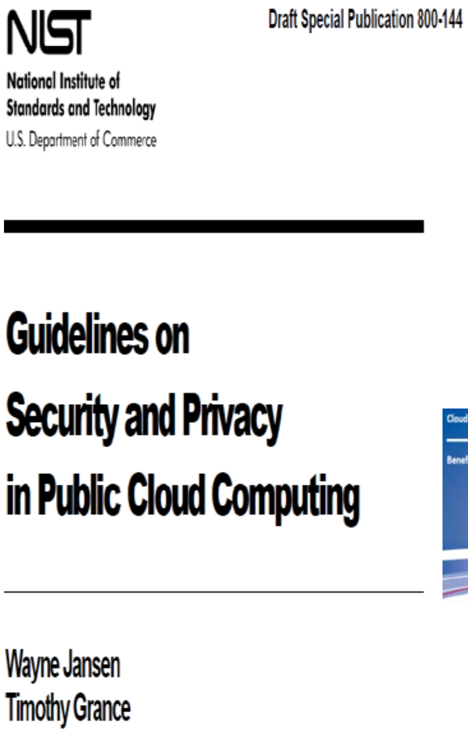
L3	Trust to good encryption
L2	Trust to the Cloud Service Provider
L1	Trust to the Legal System

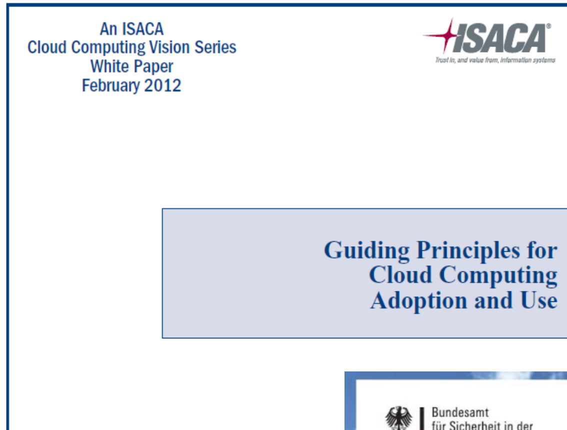
Source: Cloud Security Alliance – Security Guidance for Critical Areas of Cloud Computing

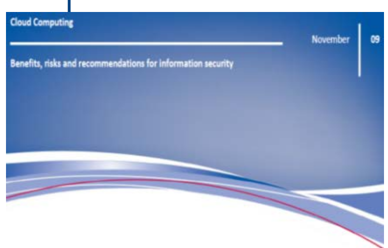
swisscom

Cloud Security

Best Practices and Guidelines







Implementation of Cloud Security

Some hints (I/II)

- Consideration of Best Practices (for example BSI, CSA, EuroCloud Swiss)
- Situational assessment of the Cloud risks (for example best on ENISA)
- Careful evaluation of a Cloud Service Provider (due diligence)
  - Existing Security measures (physical and logical)
  - Terms and Conditions (for example the SLA)
  - Reputation
  - Certifications (Standards etc.)
  - Location / Country (-> to know the legal implications)
- Secure Cloud Architecture (technology and organisation)

Implementation of Cloud Security

Some hints (II/II)

- Seek law advice within your legal department
- Do Information- and Data classification
  - **Not all your data is ready and suitable for the Cloud!**
  - From the perspective of information and data protection
  - From the perspective of availability and confidentiality
- Use Encryption
  - End to End (Data on move, Data at rest, before leaving the workstation)
  - Use the right encryption variant: regular, format preserving, searchable, order preserving, selective encryption
  - Use Data Tokenization if possible
  - According to the actual technical status, **keep the keys in your hands!**

Implementation of Cloud Security

Data Classification – Baseline for proper handling

	C1	C2 (internal default)	C3 (customer default)	C4
Label	**Public**	**Internal**	**Confidential**	**Strictly confidential**
Descripti-on	Information intended for the **public**.	Information intended for **all employees.**	**Confidential** information which is only intended for a	**Secret** information which is only intended for **a defined** …**ıp or individual persons**.
				…**sscom's own**, internal …**rmation** and **information** …**e treated confidentially** …ut **employees, customers** …ne **company**.

Directive on Security Requirements
Cloud Usage
C2 - Internal

Directive on Security Requirements

Cloud Usage

Requirements	**Private Cloud**	**Hybrid**	**Community**	**Private Cloud**	**Hybrid / Community**	**Public Cloud**
	Operated internally at Swisscom			Operated externally at a 3rd party		
C1 / P1 (public, no privacy requirements)						
C2 (internal)					mandatory encryption	mandatory encryption
C3 / P2 (confidential / standard privacy)			mandatory encryption	mandatory encryption		
C4 / P4 (strictly conf. / special privacy req.)						

Cloud Security Alliance (CSA)
Introduction

Cloud Security Alliance
What is the CSA

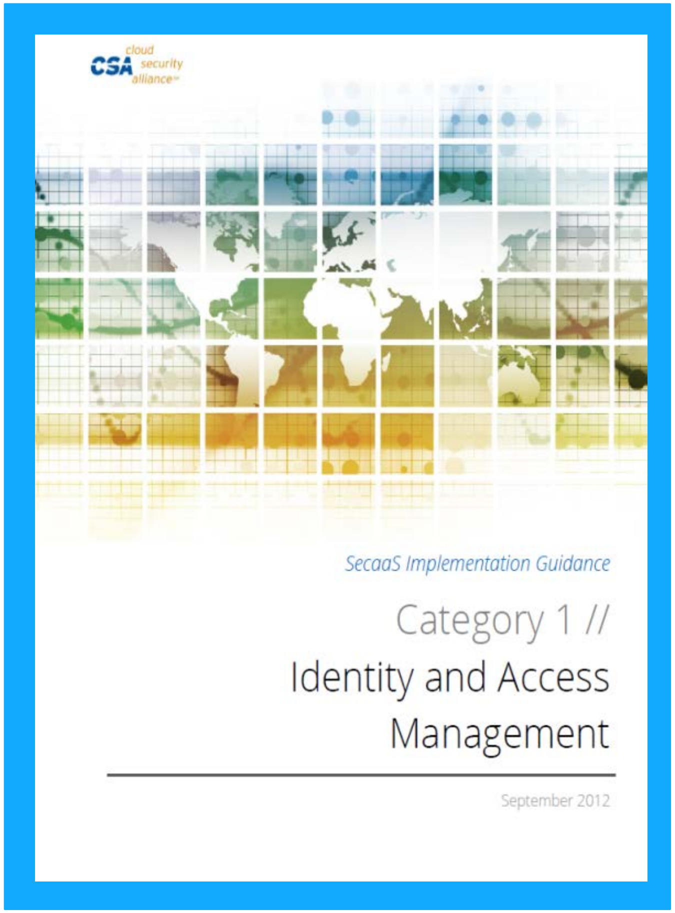
- Worldwide not for profit organisation
- Headquarter in the USA (CSA Global)
- Worldwide distributed regional chapters (~70 chapters)
- Strong relationship in Europe (EU) with BSI in Germany and ENISA
- Some examples of the CSA Corporate members (~162):

Cloud Security Alliance
Products

Source: Cloud Security Alliance

Cloud Security

SecaaS Category 1 – IAM in the Cloud



Content

- > Centralized Directory Services
- > Access Management Services
- > Identity Management Services
- > Identity Federation Services
- > Role Based Access Control
- > Privileged User Management
- > Segregation of duties
- > IAM Reporting Services

Quelle: Cloud Security Alliance – SecaaS Category 1

Cloud Security
Switzerland Chapter

- Introduction

Thanks for your attention!