



Hacking the Cloud

Exposition, Angriffsmöglichkeiten und Schutzmassnahmen

Afternoon Keynote
digicomp Hacking Day 2011

Consecom AG
Bleicherweg 64a
CH-8002 Zürich
<http://www.consecom.com>

Dr. Lukas Ruf
Lukas.Ruf@consecom.com
Büro +41-44-586-28-20
Mobil +41-79-557-20-20

Ihr Referent



Dr. Lukas Ruf

- Senior Security and Strategy Consultant, CEO, Consecom AG
- ISSS Vorstandsmitglied
- Member IEEE, ACM, SwissICT

➤ Consecom AG – ICT Security and Strategy Consulting

- Kombiniert Organisation mit Technologie
- Strategie, Governance, Prozesse, Lösungen und Technologien
- Konzeption und Definition; Implementation und Integration; Security Testing, Reviews und Audits

➤ Background Lukas Ruf

- Betriebssysteme und Netzwerke
- Software Engineering
- IT Sicherheit

The Cloud – Darstellung und Wahrnehmung

Verkäufer/Berater

Risikomanager

Betrieb

Visionär



Ist die Sicht vollständig?



Zentrale Risiken beim Cloud Computing

Verlust



Komplexität



Auflagen



Angriffsoberfläche



Cloud Computing Is Coming Whether IT like it or not!

- “Cloud computing technology is like a force of nature that security practitioners should embrace rather than fight”.

Symantec Corp. Chairman John Thompson, Cloud Security Alliance Congress 2010.

- Business-Motivation

- Kostenersparnisse und -kontrolle
- Zentralisierung des Personals mit entsprechendem Know-how

- Drei Key-Indikatoren:

(PC Magazine 01.06.2011, Avanda-Survey mit 573 C-level decision-makers)

- businesses have **increased investments** in resources to secure, manage, and support cloud computing;
- there is growing adoption and preference for **private clouds**;
- healthy **interest** in cloud computing for revenue-generating services

Hacking the Cloud – Agenda

- The Cloud Clouds Was ist eigentlich Cloud Computing?
- Angriffe auf, in und mit der Cloud
- Schutzmassnahmen beim «Leben» in der Cloud

Gibt es *die* Cloud?

Auswahl an Anbietern

➤ Global

- Amazon EC2
- Microsoft Azure
- Salesforce.com
- Apple iCloud am Horizont
- Google, Symantec, etc.
-

➤ In der Schweiz

- Swisscom
- T-Systems (Schweiz) AG
- Green.ch
- Nine Internet Solutions
-

Eigenschaften

➤ Klassische Cloud-Anbieter

- Bieten standardisierte Lösungen
- Verkaufen die Cloud als Wolke
- Ermöglichen *nahezu* anonyme Zugänge
- Bieten flexible, ad-hoc Lösungen (on-demand)
- Ermöglichen reservierte Ressourcen
- Verfügen über ein Ressourcen Trading-System

➤ Grundsätzlich dieselben Eigenschaften

- Stark im klassischen Outsourcing-Business
- Spezifische, lokale Lösungen
- Integration mit vorhandener legacy Infrastruktur
-

Cloud Definition und Terminologie

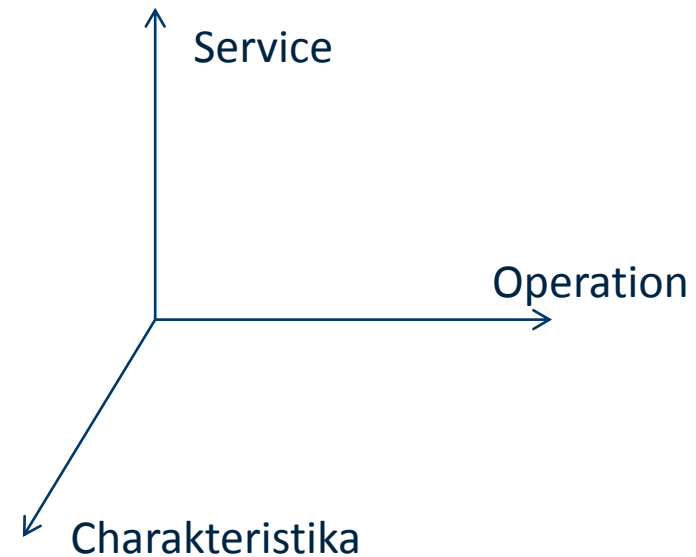


➤ NIST – US National Institute of Standards and Technologies

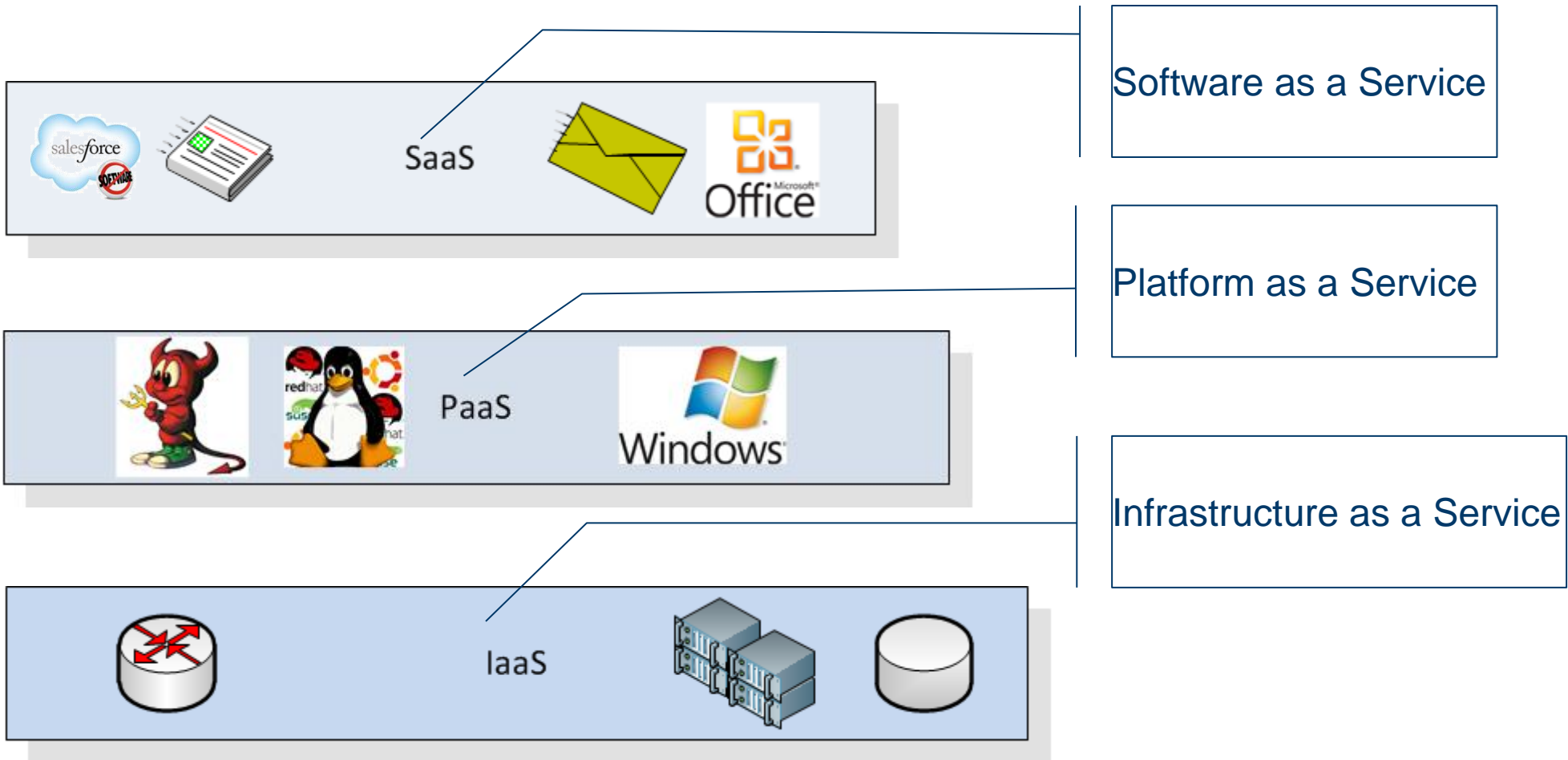
- Eine der weltweit führenden Institutionen zur Standardisierung
- Wesentliche Vorgaben im Bereich der IT
- Massgebende Sicherheitsanforderungen, z.B.
 - NIST SP800-53 (Security Controls)
 - FIPS 140-2 (Cryptography)

➤ NIST SP800_145: Cloud Definition

- Modell mit drei Dimensionen



NIST Cloud Modelle | 1: Services



Logos are trademarks of their respective owners

NIST Cloud Modelle | 2: Operation

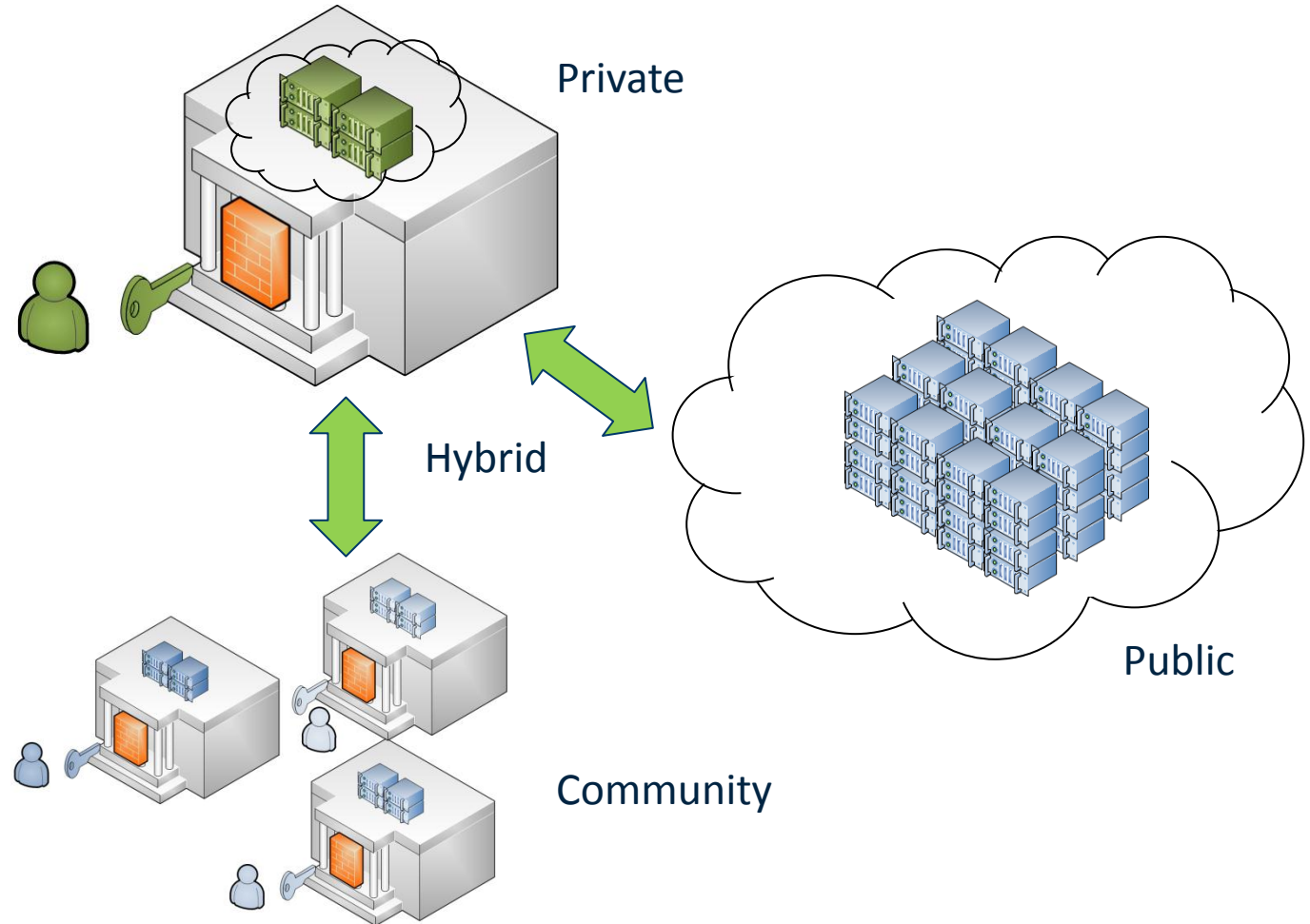
Vier Typen

➤ Private

➤ Community

➤ Public

➤ Hybrid



NIST Cloud Model | 3: Charakteristika

Wesentliche Charakteristiken

- On-demand self-service
- Kontrollierbare Dienstqualität (Measured Service)
- Breite Verfügbarkeit via Netzwerk (Broad Network Access)
- Ressource Pooling (Resource Pooling)
- Effiziente Elastizität (Rapid Elasticity)

Zentrale Charakteristik aus Sicherheitssicht^(*)

➤ Delegation der finalen Administrationshoheit

- Die Cloud gehört dem Anbieter
 - Beschränkte Einflussnahme
- Letztendlich keine Vermeidung von Interessenkonflikten

➤ Ressourcen-Sharing unter mehreren Parteien

- Gefahr der Dienste-Beeinträchtigung
 - Durch andere Parteien
 - Durch Angriffe auf andere Parteien

(*) für non-private Clouds

Cloud Computing – Alter Wein in neuen Schläuchen?

Ihre Meinung?

- Ja: Alter Wein
- Nein: Etwas Neues

Einsatz von Cloud Computing?

- Private Clouds
- Public Clouds
- Community Clouds
- Hybrid Clouds

ANGRIFFSMÖGLICHKEITEN

ANHAND AUSGEWÄHLTER BEISPIELE

Hacking the Cloud

➤ Angriffe folgen grundsätzlich dem bekannten, zyklischen Muster:

- Schwachstelle
- Verwundbarkeit
- Exploit

➤ Höhere Kompetenz und Energie der Angreiferin bei eingeschränkten Schnittstellen

- Mehrdimensionale Angriffsformen (Social Engineering, Technisch, Organisatorisch)

➤ Vier Angreiferstandorte werden unterschieden:

- Extra: Angriffe auf die Cloud
- Intra: Angriffe von einer Partie auf eine andere innerhalb derselben Cloud
- Inter: Angriffe von einer Cloud auf eine andere Cloud
- Meta: Verwendung der Cloud zur Kontrolle anderer Angriffe

Charakteristika und mögliche Schwachstellen

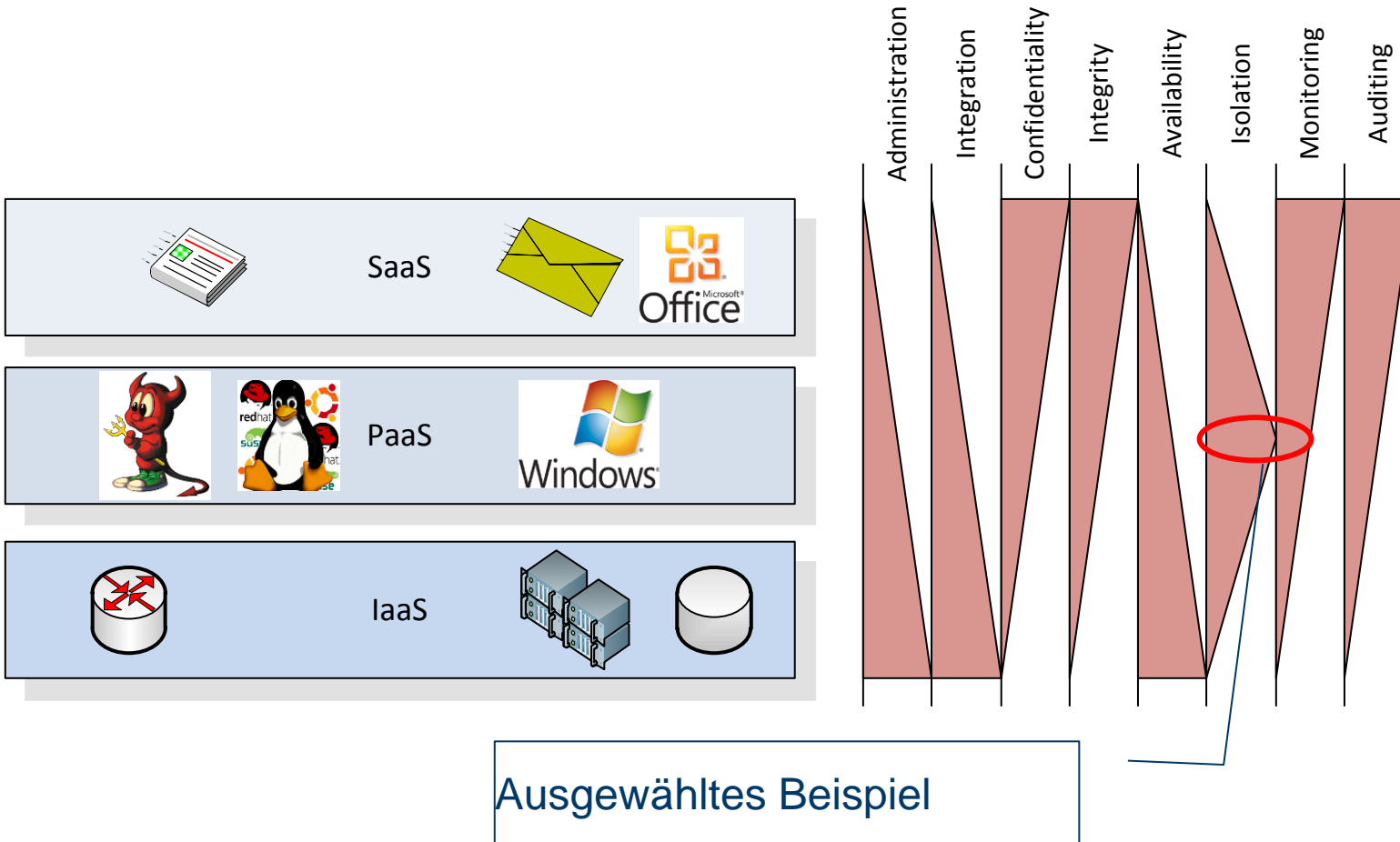
Charakteristika

- On-demand Self-service
- Measured Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity

Abgeleitete Schwachstellen

- Schwache Authentisierung
- Geringe Kontrollmöglichkeiten
- Hohe Exposition
- Schwache Isolation
- Hohe Abhängigkeiten
- Unsichere Applikationen

Entwicklung von Angriffszielen durch Analyse der Risikoexposition



Extra: Angriffe auf die Cloud | 1

➤ Service-, Admin- und User-Interfaces von Diensten in der Cloud

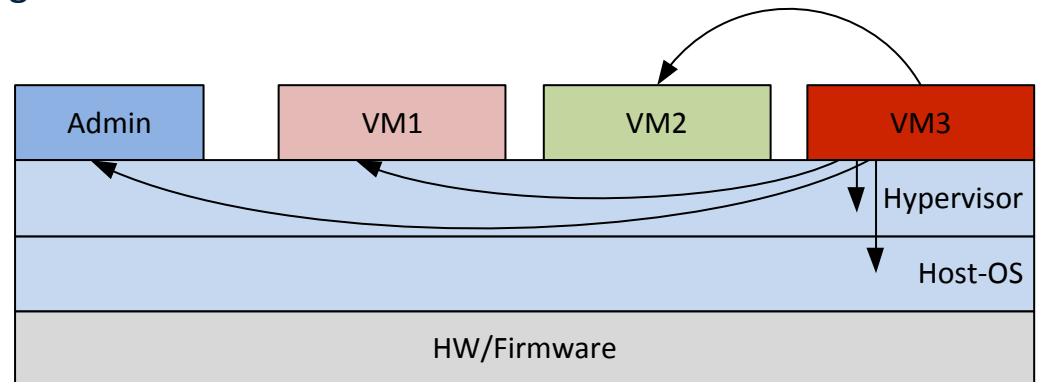
- Primäre Angriffsziele
 - von «ausen» erreichbar
 - schwierig zu kontrollieren
- Leiden an denselben Schwachstellen, wie inhouse-betriebene Dienste
 - Mangelnde Inputvalidierung: Beispiel Sony-PSP-Hack
 - Ungenügende Best-Practices: Beispiel RSA SecurID
 - Ungenügende Authentisierung: Beispiel Lockheed Martin-Hack
 - Fehlerhafte Autorisierung

Intra: Angriffe auf die Cloud | 2 – Angriffe auf andere Systeme

➤ Virtualisierer (Hypervisor, Virtual Machine Monitors)

- nur eine logische Isolation
- Leiden an Schwachstellen und bieten Verwundbarkeiten
- Verwundbarkeiten in Hypervisors können ausgenutzt werden

- Zum Zugriff auf die Kontrollfunktionen
- Zum Zugriff auf andere Systeme auf demselben System
- Zum Zugriff auf System-Netzwerkverkehr



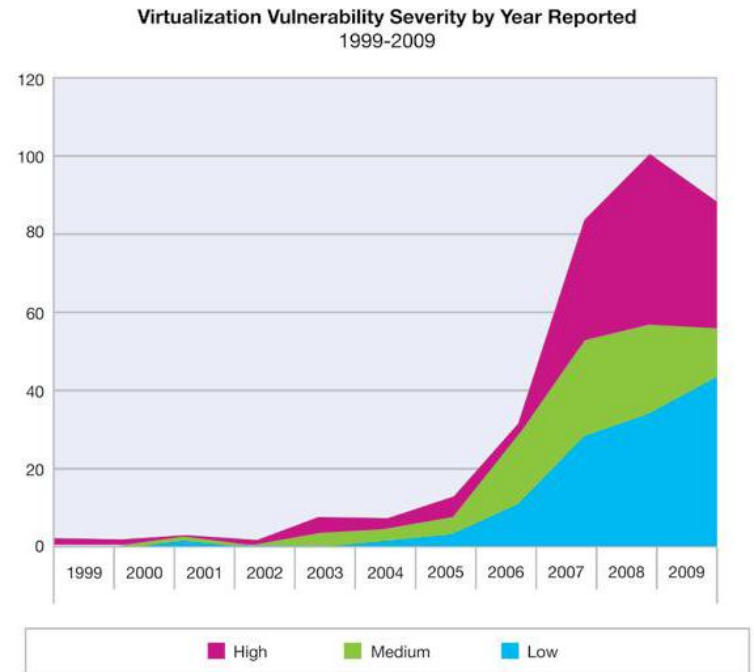
Intra: Angriffe auf die Cloud | 4: Verwundbarkeiten sind real

➤ Eine hohe Anzahl von kritischen Verwundbarkeiten

- kritisch: Einfach auszunutzen, grosser Impact
- Beispiele
 - CVE-2009-2267: A bug in the handling of page fault exceptions inVMware ESX Server could allow a guest VM user to gain kernel mode
 - CVE-2009-1244: An error in the virtual machine display function on VMware ESX Server allows an attacker in a guest VM to execute arbitrary code in the hypervisor

➤ Exploits für 14% aller Verwundbarkeiten öffentlich verfügbar

- «ready for script-kiddies»



Inter: Angriffe aus der Cloud | 1

➤ Direkte Angriffe aus der Cloud sind grundsätzlich möglich.

➤ Jedoch Überwachung und Limitierungen

- Monitoring durch Cloud Provider
- Traffic-Limitierungen durch Cloud Provider
- Angriffe à la Advanced Persistent Threats (APT)
 - Nur bedingt erkennbar
 - «Low-volume – below radar»

Meta: Verwendung der Cloud zur Angriffsunterstützung | 1

- Als Beispiel: Knacken von NTLM-Passworten
- Kurze Passworte werden auf heutigen Prozessoren in Sekunden gebrochen:
 - Das Knacken von 'fjR8n' auf einer CPU dauert 24 Sekunden.
 - Auf einer GPU (Graphikprozessor) wird weniger als 1 Sekunde benötigt.

| Passwort[länge] | 1 CPU | 1 GPU |
|-----------------|--------|-------|
| fjR8n [5] | 24s | <1s |
| pYDbL6 [6] | 1h 30m | 4s |
| fh0GH5h [7] | 4d | 17m |
| qwX0H5a12 [9] | 43y | 48d |

<http://it.slashdot.org/story/11/06/05/2028256/Cheap-GPUs-Rendering-Strong-Passwords-Useless>

Meta: Verwendung der Cloud zur Angriffsunterstützung | 2

- Passwortknacken lässt sich sehr gut, nahezu linear parallelisieren
- Grosse Farmen von GPUs können gemietet werden

| Passwortlänge | 1 CPU | 1 GPU | 1000 GPUs |
|---------------|--------|-------|------------|
| fjR8n [5] | 24s | <1s | «realtime» |
| pYDbL6 [6] | 1h 30m | 4s | «realtime» |
| fh0GH5h [7] | 4d | 17m | 1s |
| qwX0H5a12 [9] | 43y | 48d | 1h 10min |

- Nicht zu vergessen Moore's law: Performance Verdoppelung alle 1.5y

Meta: Verwendung der Cloud zur Angriffsunterstützung | 3

➤ Command and Control von Bot-Netzen

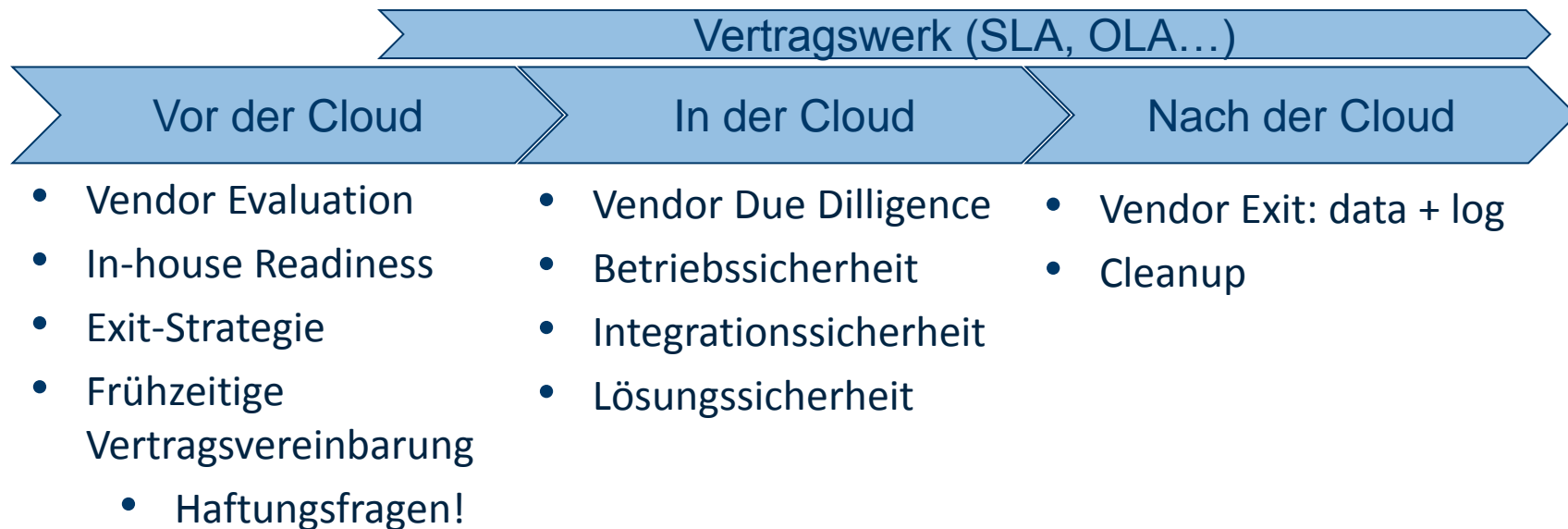
- Web-service basierte Interfaces bieten perfekte Integrationsmöglichkeiten
 - Nahezu keine Filterung von Web-Traffic bei Firmen
- Ideal für Man-in-the-Browser basierte Angriffe auf Online Banking und eCommerce Sites
 - Durch hohe Autonomie von Browsern werden Requests nahezu andauernd ausgeführt
 - Zwei, drei weitere sind «below radar»

Schutzmassnahmen

“The transition to outsourced, cloud computing environments is in many ways an exercise in risk management”, US federal CIO Vivek Kundra, Cloud Security Alliance Summit at the RSA Conference 2011

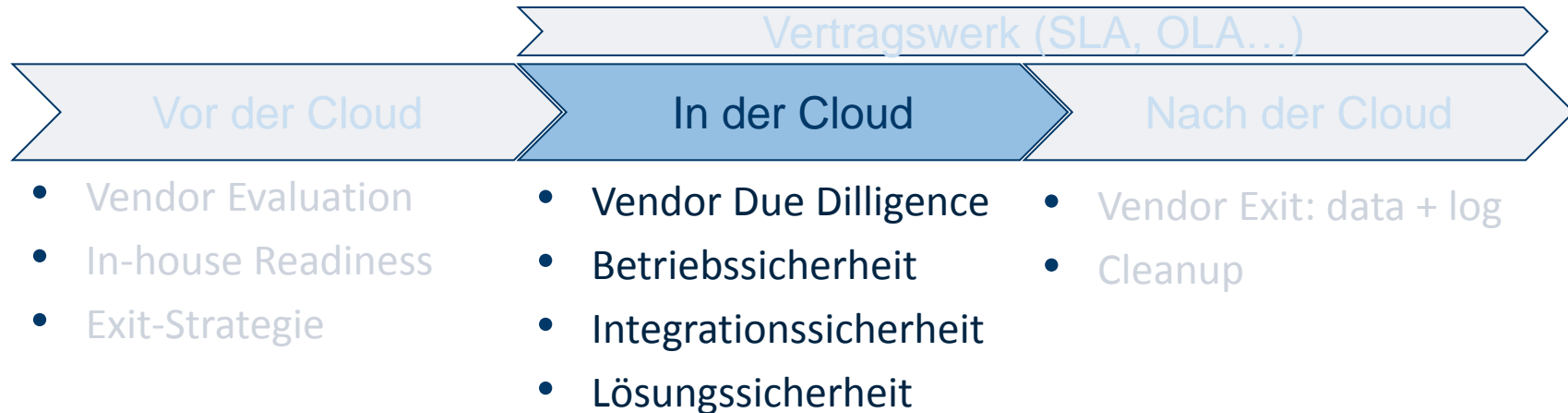
➤ Definieren Sie eine Cloud-Strategie für Ihr Unternehmen

- Cloud-Strategie erfordert eine gesamthafte Betrachtung des Outsourcing Life Cycles
- Analysieren Sie alle Phasen ihrer Cloud-Strategie

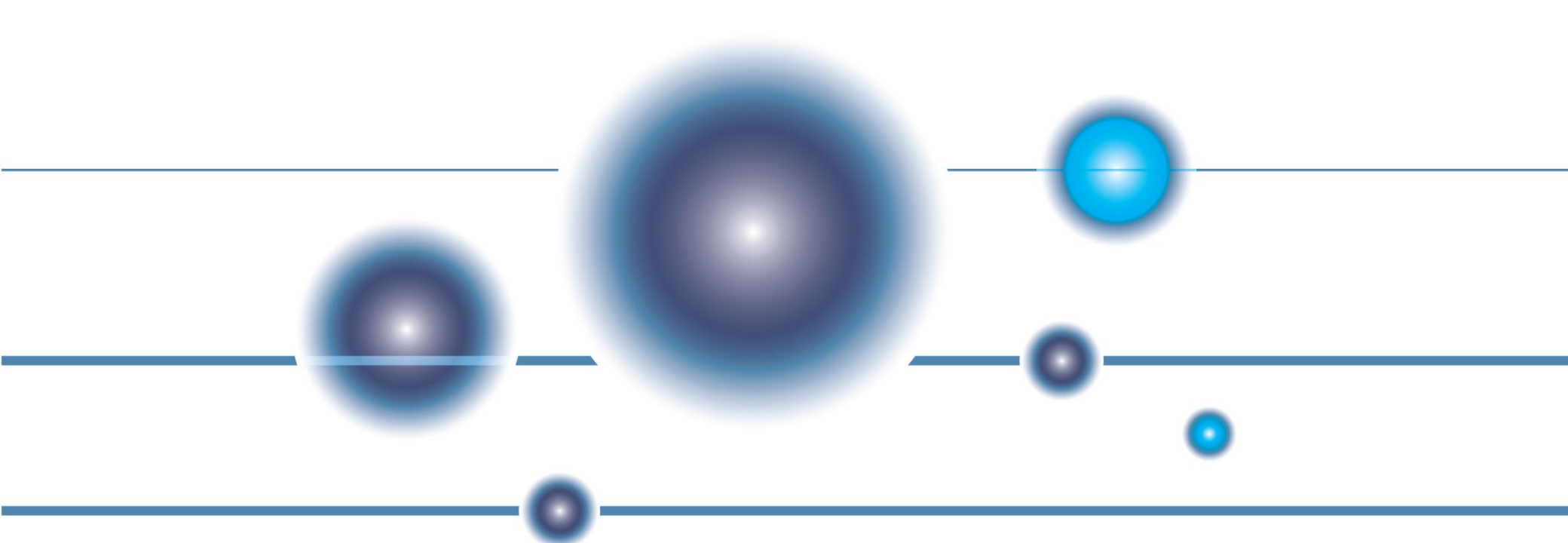


Schlussfolgerungen

“Having trust in the system will allow them to realize the cost savings and future of the cloud.”, ANS Federal



- Fordern Sie von Ihrem Cloud-Provider (Vendor) den Nachweis der erforderlichen und vertraglich eingeforderten Sorgfalt
 - Vermeiden Sie Überraschungen à la Amazon oder Microsoft Sidekick!
- Stellen Sie sicher, dass möglichst keine Schwachstellen in Ihren Lösungen vorliegen.
 - Lassen Sie sich von den nachfolgenden Vorträgen inspirieren!



Vielen Dank für Ihre Aufmerksamkeit

Consecom AG
Bleicherweg 64a
CH-8002 Zürich
<http://www.consecom.com>

Dr. Lukas Ruf
Lukas.Ruf@consecom.com
Büro +41-44-586-28-20
Mobil +41-79-557-20-20