

Cloud Security im Überblick **IT-Sicherheit, Compliance und Forensik in der Cloud**

Dr. Christoph Wegener
wecon.it-consulting

Hannover, 5. März 2012

Der Referent stellt sich vor Dr. Christoph Wegener

- ▶ Horst Görtz Institut für IT-Sicherheit (HGI)
- ▶ Gründer der **wecon.it**-consulting
- ▶ Gründungsmitglied der Arbeitsgruppe "Identitätsschutz im Internet" (a-i3)

- ▶ Auditor und Sachverständiger
- ▶ CISA, CISM, CRISC, CCSK
- ▶ bDSB (GDDcert, TÜV)
- ▶ Fachautor/-lektor/-gutachter
- ▶ Verschiedene Lehrtätigkeiten



- ▶ E-Mail: wegener@wecon.net
- ▶ Web: www.wecon.net

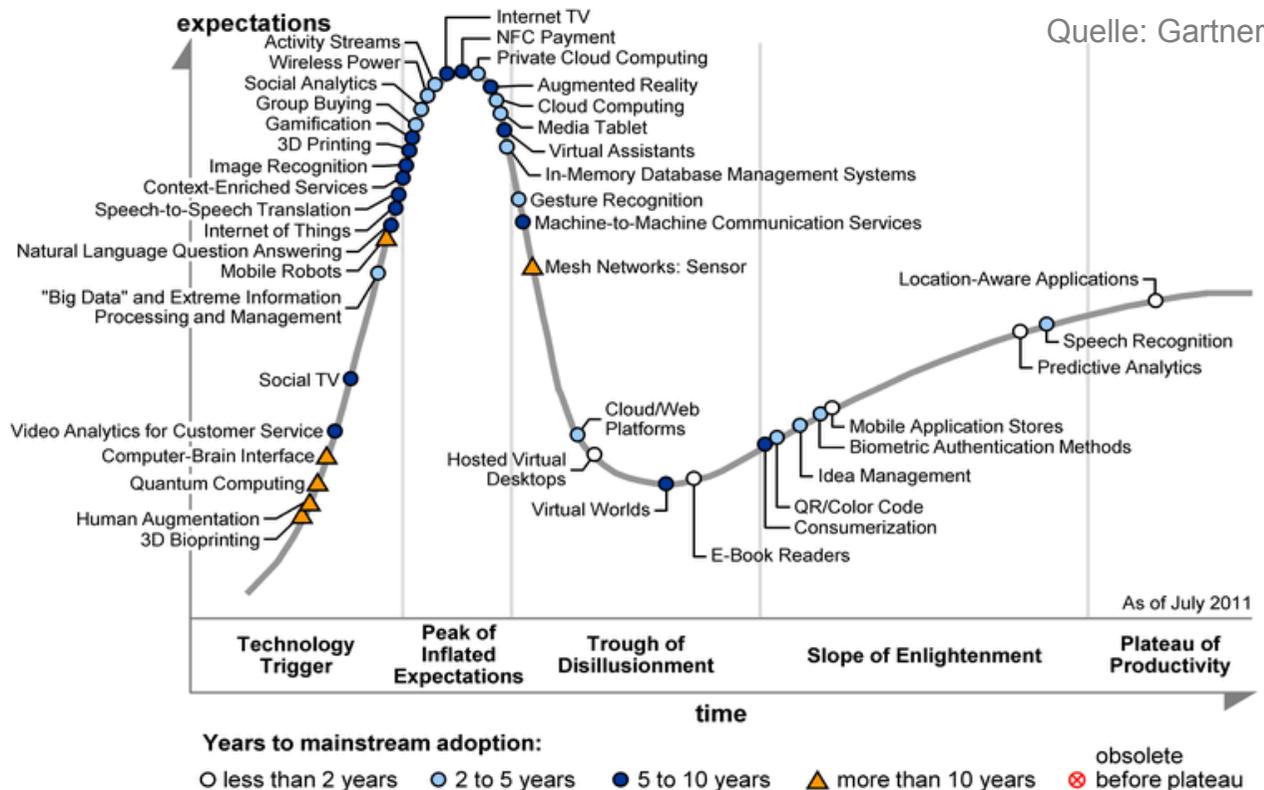
Was werde ich heute vorstellen?

- ▶ Motivation und Definition
 - ▶ Was ist die Cloud und warum ist das Thema wichtig?
 - ▶ Welche Konzepte und Cloud-Services gibt es?
- ▶ Compliance, Governance und Security
 - ▶ Physische Sicherheit, Verschlüsselung und Web-Services
 - ▶ Datenschutz, PCI DSS, Audits und SLA
- ▶ Forensik in der Cloud
 - ▶ Verfügbare Datenquellen und Methoden
 - ▶ Verwertbarkeit der Daten
- ▶ Fazit und Zusammenfassung

Einführung in die Cloud

Warum überhaupt die Cloud? Analyse des Gartner Hype Cycle

- ▶ Cloud Computing ist immer noch ein enorm wachsender Markt



Interessante Eigenschaften

- ▶ Selbstbedienung und Dienste nach Wunsch
 - ▶ Schnelles Ausrollen durch "On-demand self-service"
 - ▶ Extrem leichte Erweiterbarkeit, Provisioning in Echtzeit

- ▶ Extrem gute Verwaltung der Ressourcen
 - ▶ Skalierbarkeit ("Resource Pooling"), Flexibilität
 - ▶ Monitoring und automatisches "Fail-over"

- ▶ Extrem gute Netzwerkanbindung der Ressourcen
 - ▶ Hängt aber vom eigenen "Status" ab
 - ▶ Achtung: Datentransport ist (noch) der "Preistreiber"!

- ▶ Sicherheit wird ermöglicht/bezahlbar

Aber: Was ist Cloud Computing?

- ▶ Nicht überall, wo "Cloud" draufsteht, ist auch Cloud drin ;)

1&1 DYNAMIC CLOUD SERVER
Heute 10 und morgen 1.000 Kunden?

DIE INDIVIDUELLE SERVER-LÖSUNG!
Server-Konfiguration nach Bedarf ändern!
Jederzeit, während der gesamten Vertragslaufzeit

- Eigene dedizierte Serverumgebung mit vollem Root-Zugriff
- CPU-Anzahl, Festplattenspeicher und Arbeitsspeicher jederzeit flexibel nach Bedarf einstellbar
- Linux- oder Windows-Betriebssystem, Parallels Plesk Panel 10 vorinstalliert
- 24/7 Hotline und Support

NEU!
Ihren Server jederzeit mobil managen mit unserer kostenlosen iPhone App!

Konfigurieren Sie Ihren 1&1 Dynamic Cloud Server

Betriebssystem: Linux Windows

CPU-Anzahl: 1 2 3 4

Festplattenspeicher (GB): 100 300 500 700

Arbeitsspeicher (GB): 1 5 10 15

Traffic (GB): **AKTION: UNLIMITED** unlimited

29.99 €/Mon. Für 3 Monate
0 €/Mon. danach 39.39 €/Mon.

auswählen



- ▶ Der Versuch einer (zu) simplen Definition:
"Cloud Computing ist weltweit verteiltes Outsourcing unter Nutzung von Virtualisierungstechnologien."

Cloud-Konzepte im Überblick

- ▶ Konzept "Private Cloud"
 - ▶ Exklusiver Betrieb für einzelne Organisationen
 - ▶ Im Vergleich geringe(re) Skalier- und Verfügbarkeit
- ▶ Konzept "Community Cloud"
 - ▶ Betrieb für Gruppe von "Interessensgleichen"
 - ▶ Mittelding zwischen "Private" und "Public"
- ▶ Konzept "Public Cloud"
 - ▶ Für Jedermann verfügbar, kein exklusiver Betrieb
 - ▶ Daten (meist) nicht lokalisierbar
 - ▶ Extrem hohe Skalier- und Verfügbarkeit
- ▶ Konzept "Hybrid Cloud"
 - ▶ Mischung aus "unterschiedlichen" Cloud-Typen

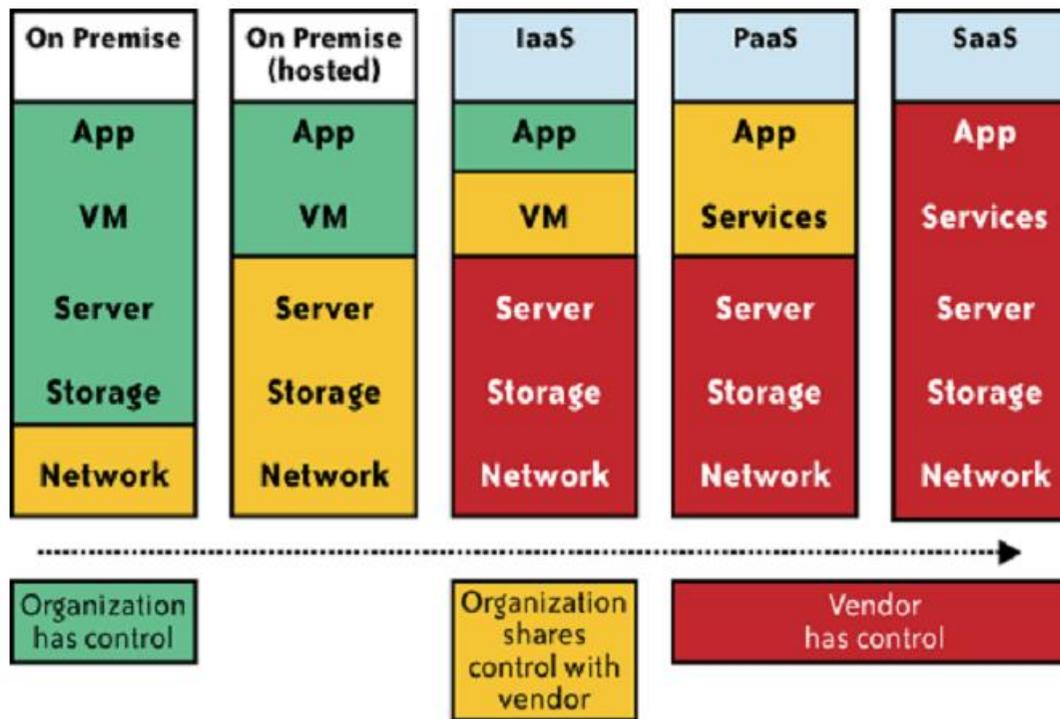
Cloud Services im Überblick

- ▶ Infrastructure as a Service (IaaS)
 - ▶ Keine Kontrolle über "Hardware"
 - ▶ Beispiel: Amazon EC2, Dropbox
- ▶ Platform as a Service (PaaS)
 - ▶ Keine Kontrolle über Betriebssystem
 - ▶ Beispiel: MS Azure, Salesforce, Google AppEngine
- ▶ Software as a Service (SaaS)
 - ▶ Keine Kontrolle über Betriebssystem und Anwendungen
 - ▶ Beispiel: GoogleDocs, GoogleMail, Twitter

- ▶ Diese Ansätze haben zum Teil völlig unterschiedliche Auswirkungen auf die Informationssicherheit!

Governance in der Cloud

- ▶ Wer hat die Kontrolle über Ihre Ressourcen?



Quelle des Originals: Tim Mather "Cloud Security and Privacy"

Transparenz in der Cloud

- ▶ Warum ist die Cloud so dunkel?
 - ▶ Anbieter wollen nicht, dass ihr System/Modell bekannt wird
 - ▶ Systemproblem: Flexibilität und Skalierbarkeit erfordern ein gewisses Maß an Intransparenz

- ▶ Dies führt insgesamt zu einem intransparenten Angebot
 - ▶ Standorte der Cloud-Rechenzentren
 - ▶ Betriebs- und Sicherheitskonzepte
 - ▶ Speicherort der Daten

- ▶ Und verhindert auch "eigene" Audits
 - ▶ Problem bei vielen Fragestellungen im Bereich Informationssicherheit und Datenschutz

Informationssicherheit in der Cloud

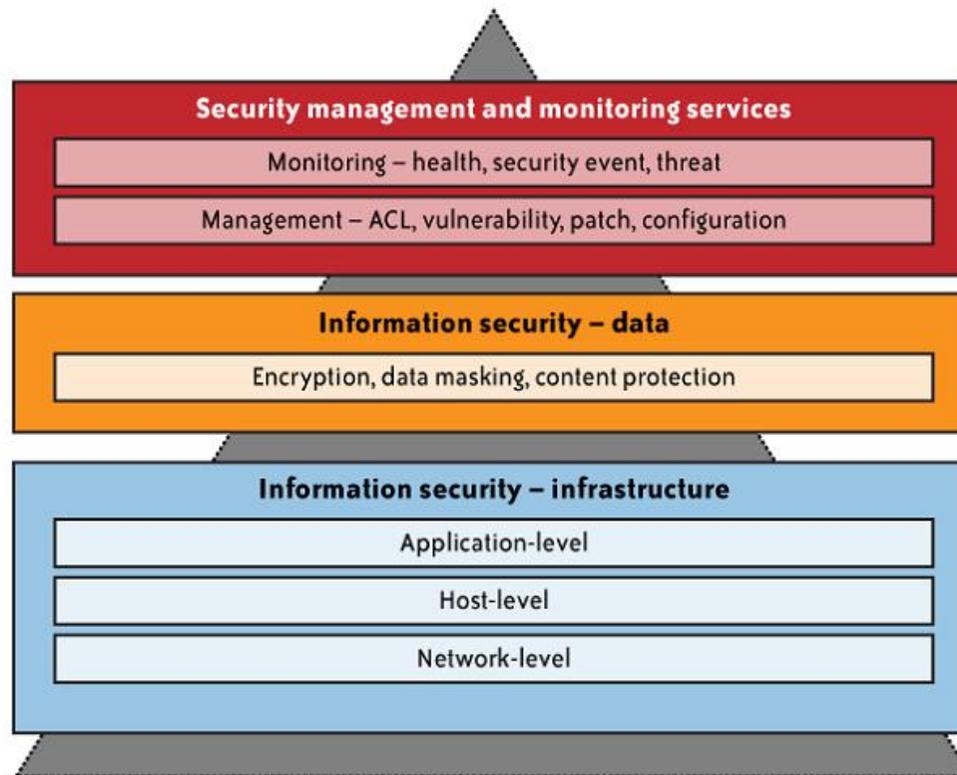
Informationssicherheit in der Cloud

- ▶ **Verschiedene Ebenen**
 - ▶ Übergeordnet: Vertrauen gegenüber dem Cloud Service Provider (CSP)
 - ▶ Netzwerk: Transport und (physischer) Speicherort der Daten
 - ▶ System: Zugriffskontrolle durch die Plattform
 - ▶ Applikation: Datenverarbeitung durch die Anwendung

- ▶ **"Typische" Schutzziele**
 - ▶ Vertraulichkeit: "Kein unbefugter Zugriff"
 - ▶ Verfügbarkeit: "Daten in angemessener Zeit verfügbar"
 - ▶ Integrität: "Datenveränderungen werden bemerkt"

Layered Defense

- ▶ Sicherheit auf allen Ebenen ist ein wichtiges Konzept



Quelle des Originals: Tim Mather "Cloud Security and Privacy"

Physische Sicherheit

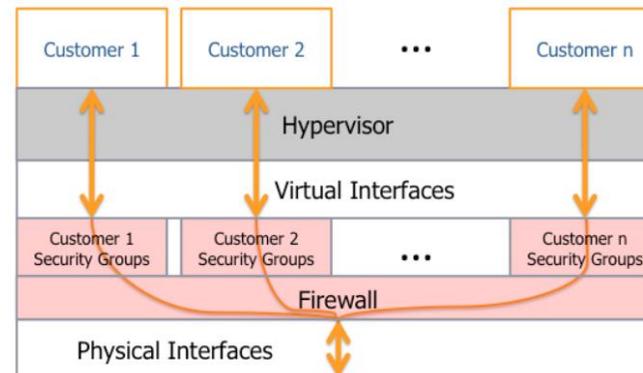
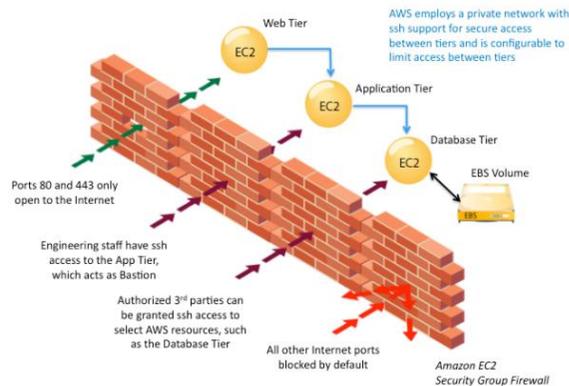
- ▶ Physische Sicherheit der Cloud-Rechner/Netzinfrastruktur
 - ▶ Gefahr durch Manipulation/Abhören
 - ▶ Gilt für IaaS, PaaS und SaaS!

- ▶ Physische Sicherheit ist aber nur ein Aspekt
 - ▶ Kein Schutz vor "logischen" Angriffen
 - ▶ Konzept der Layered Defense
 - ▶ Physische und logische Sicherheit
 - ▶ Zutritts-, Zugangs- und Zugriffsschutz

- ▶ Informieren, welche Sicherheit der eigene Anbieter bietet
 - ▶ Beispiel AWS: <http://aws.amazon.com/security/>

Netzwerksicherheit durch Firewalls

- ▶ Konzept der Perimeter-Sicherheit funktioniert nicht mehr
 - ▶ "Service Container wird zum Perimeter": Konzept "Jericho"
 - ▶ Daten liegen auf der "anderen" Seite
- ▶ Einzelne Rechner müssen strikt separiert sein
 - ▶ Bezüglich der Nutzdaten und des Netzwerks



Quelle des Originals: <http://aws.amazon.com/security>

Virtualisierungssicherheit

- ▶ Cloud Computing basiert auf virtuellen Systemen
 - ▶ Sichere Clouds nur mit sicheren virtuellen Systemen

- ▶ Schichten virtueller Sicherheit
 - ▶ Schicht 0: Sicherheit des Host-Systems
 - ▶ Schicht 1: Sicherheit der Virtualisierungsschicht
 - ▶ Schicht 2: Sicherheit der Gast-Betriebssysteme
 - ▶ Schicht 3: Sicherheit der Applikationen

- ▶ Es gibt keine 100%ige Sicherheit
 - ▶ Auch und erst recht nicht bei virtuellen Systemen
 - ▶ Insgesamt bisher mehr als 130 Schwachstellen (vgl. dazu: <http://cve.mitre.org>)

Datensicherheit durch Verschlüsselung

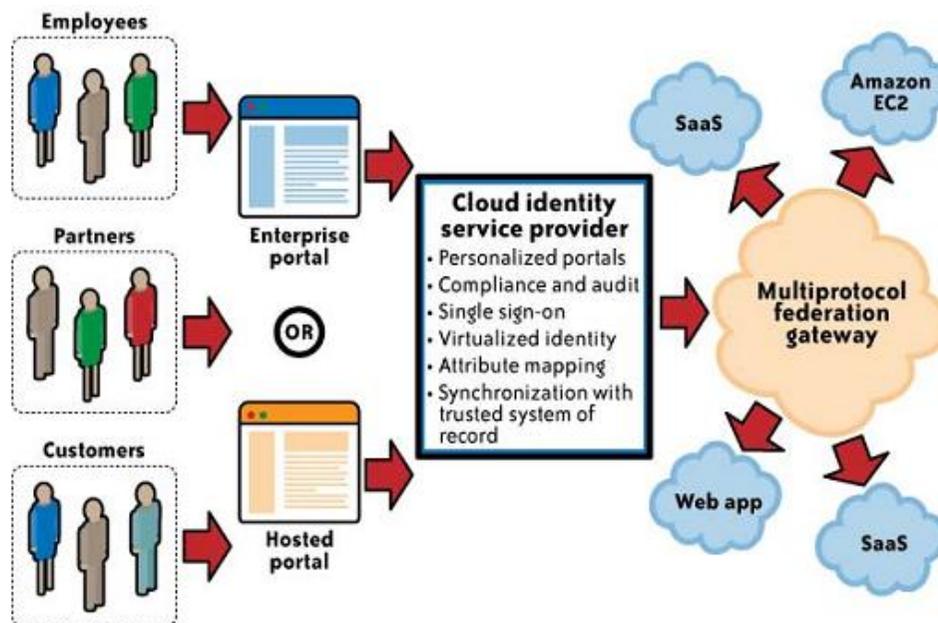
- ▶ Durchgängiges Verschlüsselungskonzept erforderlich
 - ▶ Cloud-Rechner, Netzwerk und Backup
 - ▶ Keine Daten im Machine Image speichern!

- ▶ Zahlreiche Schlüsselprobleme in der Cloud
 - ▶ Trotz Verschlüsselung hat der Cloud-Anbieter Zugriff
 - ▶ Massengenerierung: Genug Entropie vorhanden?
 - ▶ Neue Möglichkeiten für "Brute Force"-Angriffe?
 - ▶ Zugriff auf die Schlüssel?

- ▶ Ansatz "Homomorphe Verschlüsselung"
 - ▶ Daten können auch verschlüsselt bearbeitet werden

Identitätsmanagement für die Cloud

- ▶ Ein sicheres Identitätsmanagement ist eine zwingende Voraussetzung für einen sicheren Cloud-Betrieb!



Quelle des Originals: Tim Mather "Cloud Security and Privacy"

Web Service-Sicherheit

- ▶ "Administration" erfolgt über Web Services
 - ▶ Erfordert spezielle Schnittstellen
 - ▶ Beispiel: Amazon EC2

- ▶ Stichwort: Sicherheit von Web Services
 - ▶ Betrugsmöglichkeiten durch "Signature Wrapping"?
 - ▶ "Rechnen auf Kosten eines Anderen."
 - ▶ Finanzielle und rechtliche Auswirkungen
 - ▶ Verlust der Verfügbarkeit?
 - ▶ Denial-of-Service gegen den Web Service
 - ▶ Verlust der Vertraulichkeit durch "Signature Wrapping"?
 - ▶ "Daten mit den Augen eines Anderen sehen."
 - ▶ Erhebliche Auswirkungen möglich

Compliance in der Cloud

Compliance

- ▶ Vielzahl von Compliance-Anforderungen
 - ▶ Lokale Datenschutzgesetzgebung
 - ▶ Zahlreiche Regularien (HIPAA, PCI DSS, SOX,...)

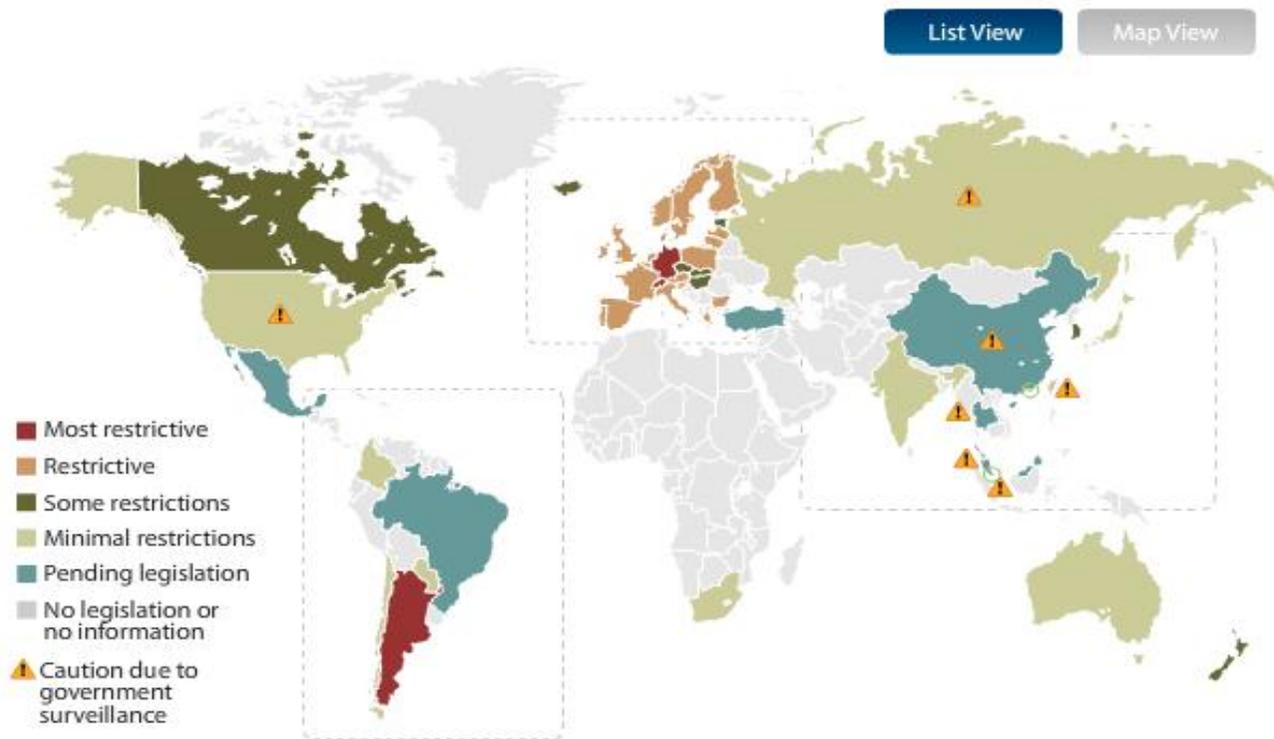
- ▶ Beispiel "Payment Card Industry Data Security Standard"
 - ▶ Explizite Firewall und Virenschutz notwendig
 - ▶ Verschlüsselte Kommunikation erforderlich
 - ▶ Mit PCI DSS 2.0 wird Virtualisierung möglich

- ▶ Cloud Computing bringt neue Herausforderungen
 - ▶ Wo sind die Daten wirklich gespeichert?
 - ▶ Welche Kommunikationsbeziehungen gibt es?

- ▶ Nicht vergessen: Zahlreiche Datenschutzaspekte!

Datenschutz in der Cloud ist ein weltweites Problem

Interactive Data Protection Heat Map



Source: US Department of Commerce and country specific legislation

Source: Forrester Research, Inc.

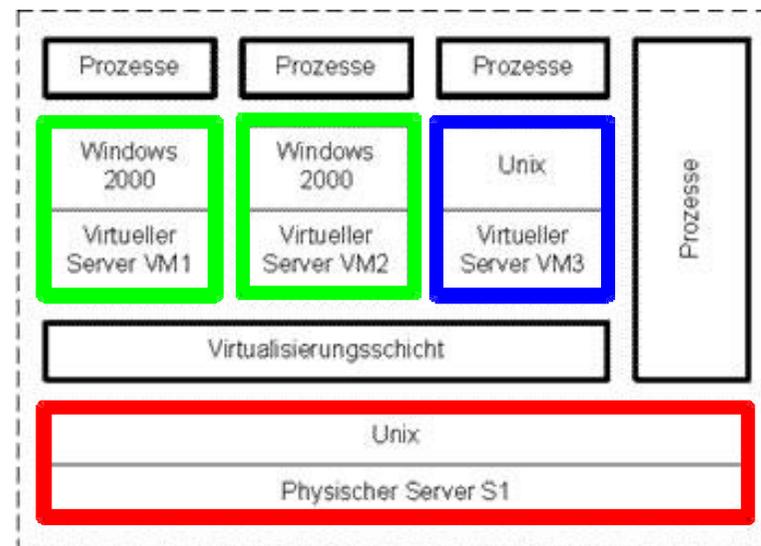
Cloud Computing und BSI IT-Grundschutz

- ▶ Kein dedizierter Baustein zum "Cloud Computing"
 - ▶ Ansatz nach Grundschutz kann aber Hilfestellung geben
 - ▶ Seit Januar 2010 Baustein zum Thema "Virtualisierung"
- ▶ Beispielhaftes Vorgehen
 - ▶ Analysiere die Komponenten des Systems
 - ▶ Betrachte virtuelle Server zunächst wie physische Systeme
 - ▶ Berücksichtige spezielle Anforderungen virtueller Systeme
- ▶ Ohne Kenntnis der Architektur wird die Analyse und Absicherung mittels BSI IT-Grundschutz unmöglich
 - ▶ Transparente Cloud-Architekturen?

Cloud Computing und BSI Grundschutz Vorgehen in der Praxis

- ▶ Konsolidierung der Komponenten
 - ▶ Virtuelle Server VM1 & VM2
 - ▶ Virtueller Server VM3
 - ▶ Physischer Server S1

- ▶ Anwenden der Bausteine
 - ▶ B 3.101 Allgemeiner Server
 - ▶ B 3.102 Server unter Unix
 - ▶ B 3.106 Server unter Windows 2000

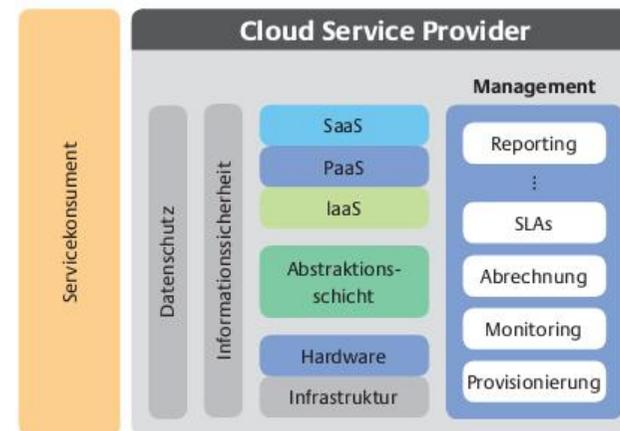


Quelle des Originals: <http://www.bsi.de>

- ▶ Je nach XaaS-Modell kann der Nutzer unterschiedliche Schichten absichern
- ▶ Der Rest fällt in die Verantwortung des CSP!

BSI Eckpunktepapier Mindestanforderungen für CSP

- ▶ Grundlage bildet eine Referenzarchitektur
 - ▶ Provider hat zahlreiche Anforderungen zu erfüllen
- ▶ Dabei müssen unterschiedlichste Bereiche berücksichtigt werden
 - ▶ Technik
 - ▶ Organisation
 - ▶ Personal
- ▶ Je nach Schutzprofil gibt es unterschiedliche Anforderungen
 - ▶ B: Basisanforderungen
 - ▶ C+: hohe Vertraulichkeit
 - ▶ A+: hohe Verfügbarkeit



Sicherheitsprüfung und -nachweis	Private ⇄			Public ⇄		
	B	C+	A+	B	C+	A+
Cloud Service Anbieter müssen den Cloud-Nutzern regelmäßig über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle, die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests berichten	✓			✓		
Regelmäßige Penetrationstests	✓			✓		
Regelmäßige Penetrationstests bei Subunternehmen	✓			✓		
Regelmäßige und unabhängige Sicherheitsrevisionen		✓	✓		✓	✓
Regelmäßige und unabhängige Sicherheitsrevisionen bei Subunternehmern		✓	✓		✓	✓

Quelle des Originals: <http://www.bsi.de>

Ohne Audits keine Transparenz

- ▶ Audits machen die Cloud "nutzbar"
 - ▶ Ohne Audits kein Vertrauen in die Cloud
 - ▶ Eigeninteresse: Transparenz vs. Vertrauen
 - ▶ Erfüllen von Compliance-Anforderungen

- ▶ Je nach Bereich unterschiedliche Anforderungen
 - ▶ HIPAA, ISO 27001, PCI DSS, SAS 70, ...

- ▶ Was sagt ein Audit wirklich aus?
 - ▶ Wer beauftragte das Audit?
 - ▶ Wie vertrauenswürdig ist der Auditor?
 - ▶ Was ist der Umfang des Audits?
 - ▶ Wie detailliert/vollständig ist der Audit-Bericht?

Lizenzfragen in der Cloud

- ▶ Cloud Computing bietet einfaches "Provisioning"
 - ▶ "MI" ermöglicht schnelles, wiederholbares Ausrollen
 - ▶ Birgt aber die Gefahr nicht vorhandener Lizenzen

- ▶ Haben Sie Lizenzen für alle Instanzen?
 - ▶ Wie viele Lizenzen existieren überhaupt?
 - ▶ Auf welcher Grundlage werden Lizenzen berechnet?
 - ▶ Wie löst man die Probleme bei Kurzzeitbetrieb?
 - ▶ Nicht alle Lizenztypen sind "virtualisierbar"!

- ▶ Vorsicht mit "fremden" Machine Images (MI)!

Forensik in der Cloud

Forensik in der Cloud Teuflische Bedingungen

CSPs wollen und werden die Cloud nicht transparent(er) machen

Ohne Vertrauen und Kontrolle über die Umgebung keine Digitale Forensik



Vertrauen und Kontrolle benötigen
Transparenz

Im Falle eines Falles Cloud Computing und Forensik

- ▶ Vorteile durch Forensik mit der Cloud
 - ▶ Systeme können auf den Ernstfall vorbereitet werden
 - ▶ 1:1-Bit-Kopien sind sehr schnell machbar
 - ▶ Ausfallzeiten können verkürzt werden
 - ▶ Prüfsummen sind zum Teil integriert (z.B. EC2)

- ▶ Nachteile bei Forensik an der Cloud
 - ▶ Wo liegen eigentlich physisch die zu analysierenden Daten?
 - ▶ Wie kann die Integrität der Daten sichergestellt werden?

- ▶ Problem bleibt der nicht vorhandene physische Zugriff
 - ▶ Was bedeutet dies für rechtliche Auseinandersetzungen?
 - ▶ (Konfigurierbare) definierte Schnittstellen?

Cloud Computing Beweissicherung in der Cloud

- ▶ Möglichkeiten zur Beweissicherung existieren
 - ▶ Snapshots (aka 1:1-Kopien) der virtuellen Maschine
 - ▶ Logfiles bzgl. Netz, System und Applikationen

- ▶ Snapshot-Techniken eröffnen zudem neue Möglichkeiten
 - ▶ Vollständiges Abbild inkl. RAM, "Zuständen", ...
 - ▶ Gesamtheitliche Sicht auf das System
 - ▶ Wiederholbare, vereinfachte Analysemöglichkeiten

- ▶ Fraglich aber, welche Beweiskraft diese Daten haben
 - ▶ Könnte der CSP die Daten verändert haben?
 - ▶ Ist die Snapshot-Technologie "sauber"?
 - ▶ Technische Dokumentation kann helfen!

Service Level Agreements für die Cloud

Verfügbarkeit in der Cloud

- ▶ Je nach XaaS unterschiedliche Aspekte
 - ▶ Verfügbarkeit des Netzes
 - ▶ Verfügbarkeit der physischen Hosts
 - ▶ Verfügbarkeit der virtuellen Maschine
 - ▶ Verfügbarkeit der Applikation

- ▶ Service Level Agreement (SLA) bildet die Grundlage
 - ▶ Aber was sagt das SLA wirklich aus, was ist es wert?

- ▶ Deaktivieren eines MI kann zum Totalverlust führen
 - ▶ MI wird gelöscht, sobald sie nicht mehr in Betrieb ist!
 - ▶ Nutzdaten möglichst außerhalb des MI ablegen
 - ▶ MI regelmäßig sichern

Beispiel aus der Praxis Amazon EC2 nicht verfügbar

Amazon EC2 cloud service experiences power outage... again

Posted by 14 MAY, 2010



Earlier this week, Amazon's EC2 cloud service experienced yet another power outage. This time, a car crashed into a local utility pole and knocked out the power. The generator transfer switch failed. A number of East Coast customers lost service for about an hour.

A very similar incident occurred in 2007 at a RackSpace data center. Regardless of this, Amazon needs to get its act together. Why didn't the server load transfer over to the generators properly?

The cloud computing provider surely won't be signing up very many new customers if these power outages continue. Finally, current EC2 users must be very upset about this and worried about Amazon's long-term reliability.

Quelle: <http://www.internetblog.org.uk>

Service Level Agreements

- ▶ Aus den Nutzungsbedingungen zu AWS
 - ▶ Beispiel Verfügbarkeit: *"[...] we shall have no liability whatsoever for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that you may incur as a result of any Service Suspension [...]"*
 - ▶ Beispiel Security: *"We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet."*

- ▶ Aus dem SLA zu Amazon EC2
 - ▶ Entschädigung, wenn "Annual Uptime Percentage <99.95%"
 - ▶ Nur als Service Credits (=Guthaben auf dem Kundenkonto)
 - ▶ Nur prozentual (=10%) in Bezug auf die Rechnungssumme

Zusammenfassung

Pro und Contra Cloud Computing

- ▶ Vorteile des Cloud Computing
 - ▶ Cloud Computing zwingt zu Datensicherheit und Datenschutz
 - ▶ Ermöglicht "On-demand"-Computing, bessere Verfügbarkeit
 - ▶ Schnellere Sicherheitsupdates
 - ▶ Weniger Energieverbrauch, weniger Kosten
 - ▶ Unabhängigkeit von eigenen Ressourcen

- ▶ Nachteile des Cloud Computing
 - ▶ Vertrauen in den Cloud-Anbieter
 - ▶ Was passiert, wenn der Cloud-Anbieter verkauft/insolvent ist?
 - ▶ Rechtliche Unsicherheiten (auch wegen Internationalität)
 - ▶ Abhängigkeit von fremden Ressourcen

Fazit und Ausblick

- ▶ Virtualisierungskonzepte und Cloud Computing bieten Chancen
 - ▶ Bessere Verfügbarkeit, Skalierbarkeit, Kosteneffizienz, ...
 - ▶ Höhere "Sicherheit" (möglich)
 - ▶ Unabhängigkeit von eigenen Ressourcen

- ▶ Aber auch nicht zu vernachlässigende Risiken
 - ▶ Verlust der Verfügbarkeit, der Vertraulichkeit, ...
 - ▶ Abhängigkeit von fremden Ressourcen
 - ▶ Vgl. Diskussionen zum Outsourcing

- ▶ "Der frühe Vogel fängt den Wurm!"
 - ▶ Informieren Sie sich rechtzeitig und gründlich
 - ▶ Auch über die relevanten Sicherheitsaspekte! :)

Goldene Regeln für die Cloud

- ▶ Informieren Sie sich weitreichend über die Sicherheit bei Ihrem CSP
 - ▶ Konzepte der Layered Defense beachten
- ▶ Prüfen Sie, inwieweit Ihr CSP auditiert/zertifiziert ist
 - ▶ Beispielsweise ISO 27001, SAS 70, ...
 - ▶ Arbeitet Ihr CSP „datenschutzkonform“?
- ▶ Verschlüsselung ist nicht alles, aber besser als nichts
 - ▶ Beachten Sie aber die Allmacht des CSP
 - ▶ Also keine sensiblen Daten in die Cloud legen!
- ▶ Qualität zahlt sich aus: "You get what you paid for!"

Einige Literaturempfehlungen (1)

- ▶ Cloud Security Alliance (CSA)
<http://www.cloudsecurityalliance.org/>
- ▶ NIST Computer Security Division – Cloud Computing
<http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>
- ▶ Publikationen der ENISA zur Cloud
<http://www.enisa.europa.eu/act/rm/files/deliverables/>
- ▶ Berkeley University: Above the Clouds
<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>
- ▶ Gartner Studie: Seven cloud-computing security risks
<http://www.infoworld.com/print/36853>
- ▶ Amazon Web Service Security (AWS Security)
<http://aws.amazon.com/security>

Einige Literaturempfehlungen (2)

- ▶ Immunity Cloudburst
<http://www.immunityinc.com/documentation/cloudburst-vista.html>
- ▶ Joerg Heidrich und Christoph Wegener: "Sichere Datenwolken", MMR 2010, 803.
- ▶ Dominik Birk und Christoph Wegener: "Über den Wolken: Cloud Computing im Überblick", DuD 2010, 641.
- ▶ Dominik Birk: "Technical Challenges of Forensic Investigations in Cloud Computing Environments", CSC 2011.
- ▶ Google ist Ihr Freund! :)
<http://www.google.de/search?q=cloud+security>

Interessante Bücher (Auswahl)

- ▶ Interessante Bücher zum Thema
 - ▶ George Reese:
"Cloud Application Architectures – Transactional Systems for EC2 and Beyond", O'Reilly Verlag, 1. Auflage 2009
ISBN: 978-0596156367

 - ▶ Tim Mather, Subra Kumaraswamy und Shahed Latif:
"Cloud Security and Privacy – An Enterprise Perspective on Risks and Compliance", O'Reilly Verlag, 1. Auflage 2009
ISBN: 978-0596802769

Danke für Ihre Aufmerksamkeit 😊

- ▶ Haben Sie Fragen?

- ▶ Dr. Christoph Wegener
 - ▶ E-Mail: wegener@wecon.net
 - ▶ Web: www.wecon.net

