

Sicherheit in der Wolke: Cloud Computing Security Sicherheitsaspekte und Lösungsansätze

Dominik Birk

Horst Görtz Institut für IT-Sicherheit

Dr. Christoph Wegener
wecon.it-consulting

Stuttgart, 17. November 2010

Zur Person: Dominik Birk



- Mitarbeiter am Horst Görtz Institut für IT-Sicherheit (HGI)
- Forschungsschwerpunkte:
 - Web-2.0 Sicherheit und Cloud Forensics
 - Informationssicherheits-Management
- Freiberuflicher Berater, Autor zahlreicher Fachartikel
- Sprecher auf nationalen und internationalen Konferenzen
- E-Mail: dominik@code-foundation.de Web: www.code-foundation.de

Zur Person: Dr. Christoph Wegener



- Mitarbeiter am 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, CBP, GDDcert
- Fachautor/-lektor/-gutachter
- Verschiedene Lehrtätigkeiten

- E-Mail: wegener@wecon.net

Web: www.wecon.net

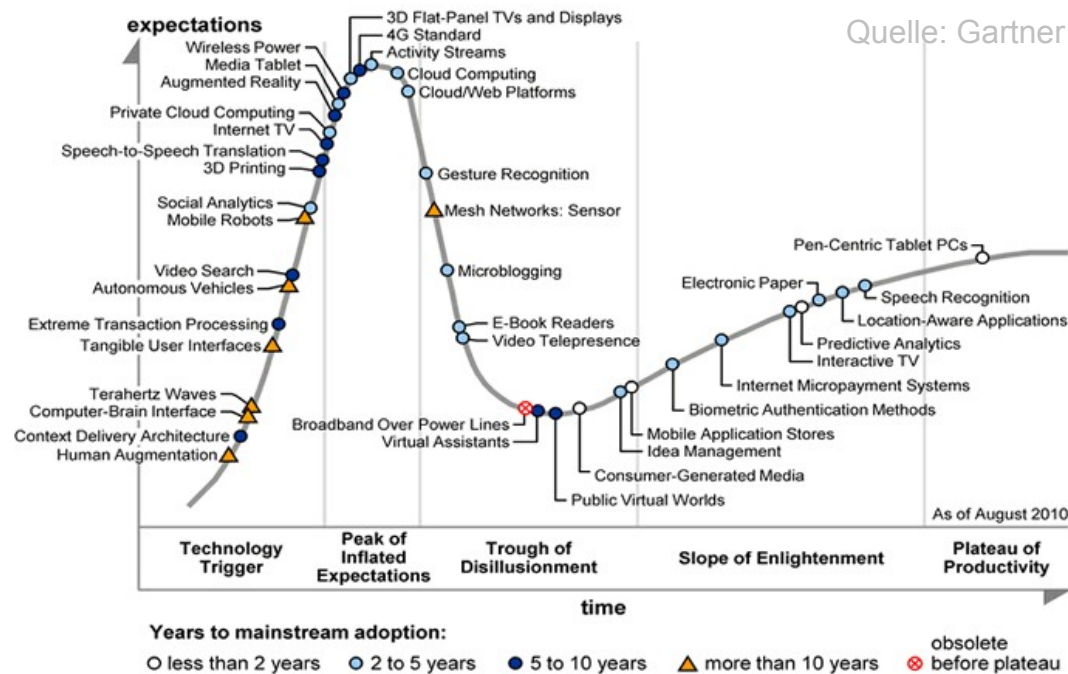
Was werde ich heute vorstellen?

- Motivation und Definitionen
 - Warum sollten Sie sich mit Cloud-Sicherheit beschäftigen?
 - Cloud-Architekturen: Public, Private, Hybrid und Community
 - XaaS im Überblick: Infrastructure, Platform und Software
- Sicherheit für die Cloud
 - "Technische" Aspekte
 - Compliance Fragestellungen
 - Forensik in der Cloud
- Abschließendes Fazit
 - Cloud-Nutzung ja, aber richtig!
 - Goldene Regeln für die Cloud
 - Interessante Links und Literatur

Motivation oder "Warum das Ganze?"

Warum das Thema Sie interessieren sollte

- Cloud Computing ist ein enorm wachsender Markt
 - Immer noch auf der Spitze des "Gartner Hype Cycle"



- Cloud Computing wird zu einer Standardtechnologie
 - Es ist momentan nicht die Frage ob, sondern wann!

Warum ist die Cloud interessant?

Vorteile des Cloud Computing

- 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

Definition der Cloud-Typen

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

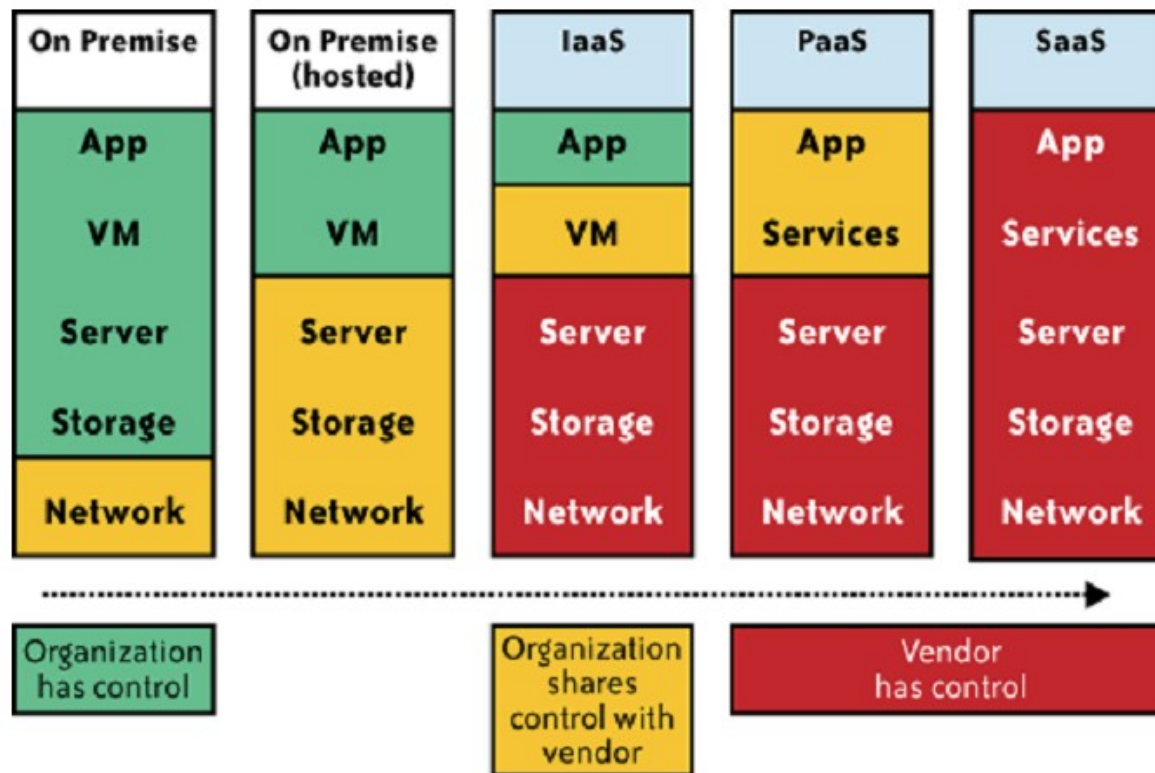
Service ist alles

XaaS im Überblick

- "Infrastructure as a Service" (IaaS)
 - Keine Kontrolle über "Hardware"
 - Volle Kontrolle über Betriebssystem und Anwendungen
- "Platform as a Service" (PaaS)
 - Keine Kontrolle über Betriebssystem
 - Volle Kontrolle über die Anwendungen
- "Software as a Service" (SaaS)
 - Keine Kontrolle über Betriebssystem und Anwendungen
 - "Kontrolle" über die Daten
- Diese Ansätze haben zum Teil völlig unterschiedliche Auswirkungen auf die Informationssicherheit!

Cloud Computing und Governance

- Wer hat die Kontrolle über Ihre Ressourcen?



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

Sicherheit in der Wolke

Alles wie immer?

- Verschiedene Sicherheitsfragestellungen
 - Vertrauen gegenüber dem Cloud Service Provider (CSP)
 - (Physischer) Speicherort der Daten
 - Zugriffskontrolle durch die Plattform
 - Datenverarbeitung durch die Anwendung
- "Typische" Schutzziele
 - Vertraulichkeit: "Kein unbefugter Zugriff"
 - Verfügbarkeit: "Daten in angemessener Zeit verfügbar"
 - Integrität: "Datenveränderungen werden bemerkt"
- Aber: In der Cloud ist auch vieles anders!

Transparente Cloud Konzepte? Dunkle Wolken am Himmel

- Warum ist die Cloud so dunkel?
 - Anbieter wollen nicht, dass ihre Infrastruktur 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
- Und verhindert auch "eigene" Audits
 - Problem bei vielen Fragestellungen im Bereich Informationssicherheit und Datenschutz

"Technische" Aspekte

Basis der Cloud-Sicherheit

Virtualisierungssicherheit

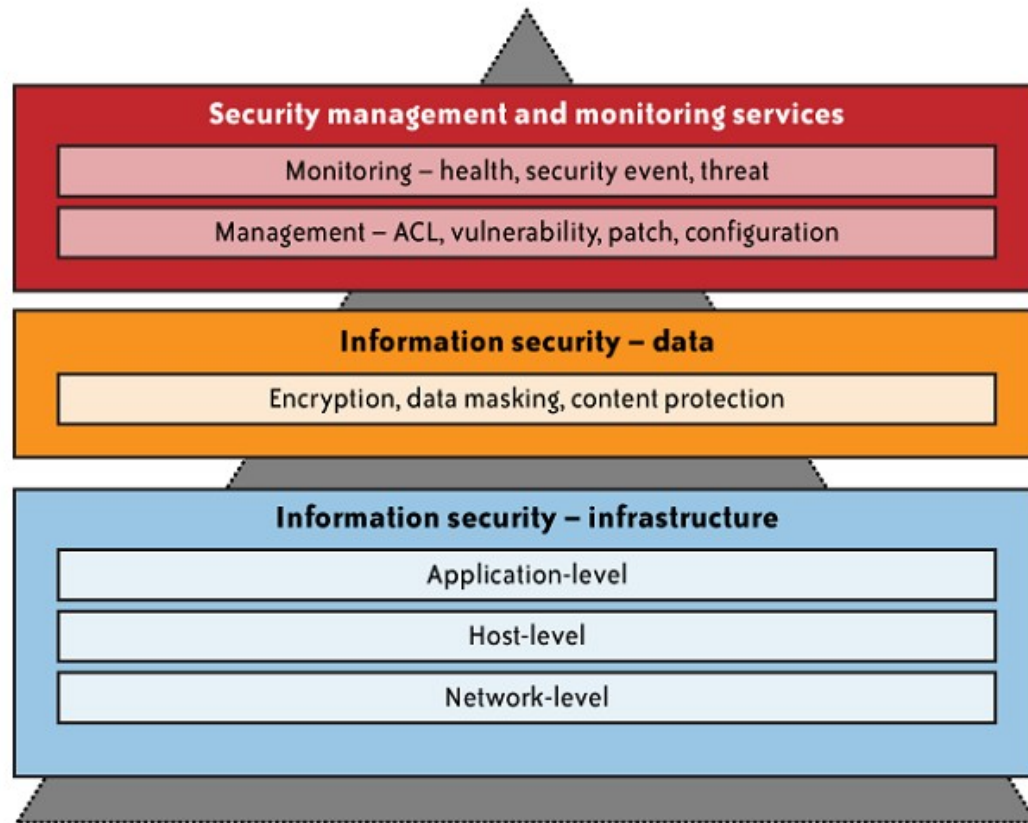
- Cloud Computing basiert auf virtuellen Systemen
 - Sichere Clouds nur mit sicheren virtuellen Systemen
- Schichten virtueller Sicherheit
 - Schicht 0: Sicherheit des Host-Systems
 - Schicht 1: Sicherheit der Virtualisierungsschicht
 - Schicht 2: Sicherheit der Gast-Betriebssysteme
 - Schicht 3: Sicherheit 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>)

Regeln für die Cloud

- Grundlage bildet ein Sicherheitskonzept
 - Besteht überhaupt ein entsprechendes Konzept?
 - Passt das bestehende Konzept zum Cloud Computing?
- Insbesondere ist ein Risikomanagement erforderlich
 - Ist ein solches überhaupt vorhanden?
 - Passt das bestehende Konzept zum Cloud Computing?
- In der Cloud gelten die "üblichen" Regeln
 - "Need to Know"-Prinzip
 - Konzept der "Layered Defense"

Layered Defense in the Cloud

- Sicherheit auf allen Ebenen ist ein wichtiges Konzept



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

Physische Sicherheit

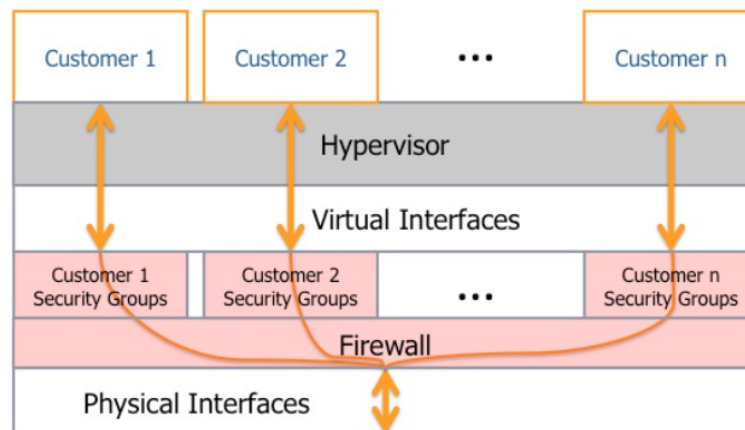
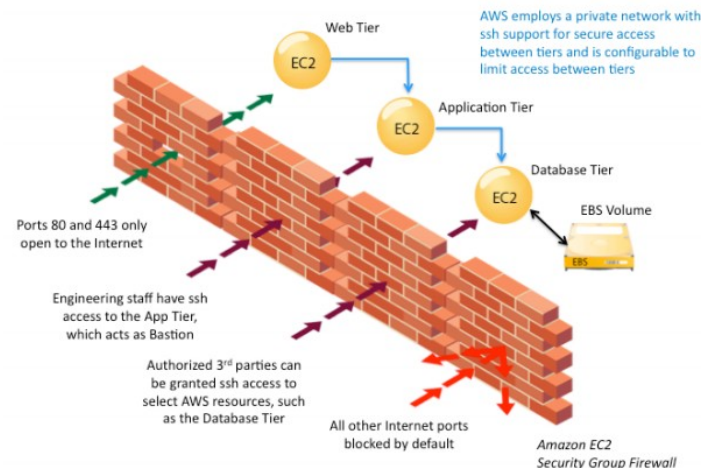
- Physische Sicherheit der Cloud-Rechner und der zugehörigen Netzinfrastruktur ist extrem wichtig
 - Gefahr durch Manipulation der Rechner
 - Gefahr durch Abhören der Kommunikationswege
 - Gilt für IaaS, PaaS und SaaS!
- Physische Sicherheit ist nur "Basisschutz"
 - Kein Schutz vor "logischen" Angriffen
 - 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/>

Schutz durch Verschlüsselung

- Durchgängiges Verschlüsselungskonzept erforderlich
 - Cloud-Rechner, Netzwerk und Backup
- Keine Daten im Machine Image speichern
 - Trotz Verschlüsselung hat der Cloud-Anbieter Zugriff
- Zahlreiche Schlüsselprobleme in der Cloud
 - Massengenerierung: Genug Entropie vorhanden?
 - Neue Möglichkeiten für "Brute Force"-Angriffe?
 - Zugriff auf die Schlüssel?
- Ansatz "Homomorphe Verschlüsselung"
 - Daten können auch verschlüsselt bearbeitet werden

Cloud Computing und Firewalls

- Althergebrachtes Konzept der Perimeter-Sicherheit existiert nicht mehr
 - "Service Container wird zum Perimeter"
- Einzelne Rechner müssen strikt separiert sein
 - Bezüglich der Nutzdaten
 - Bezüglich des Netzwerks

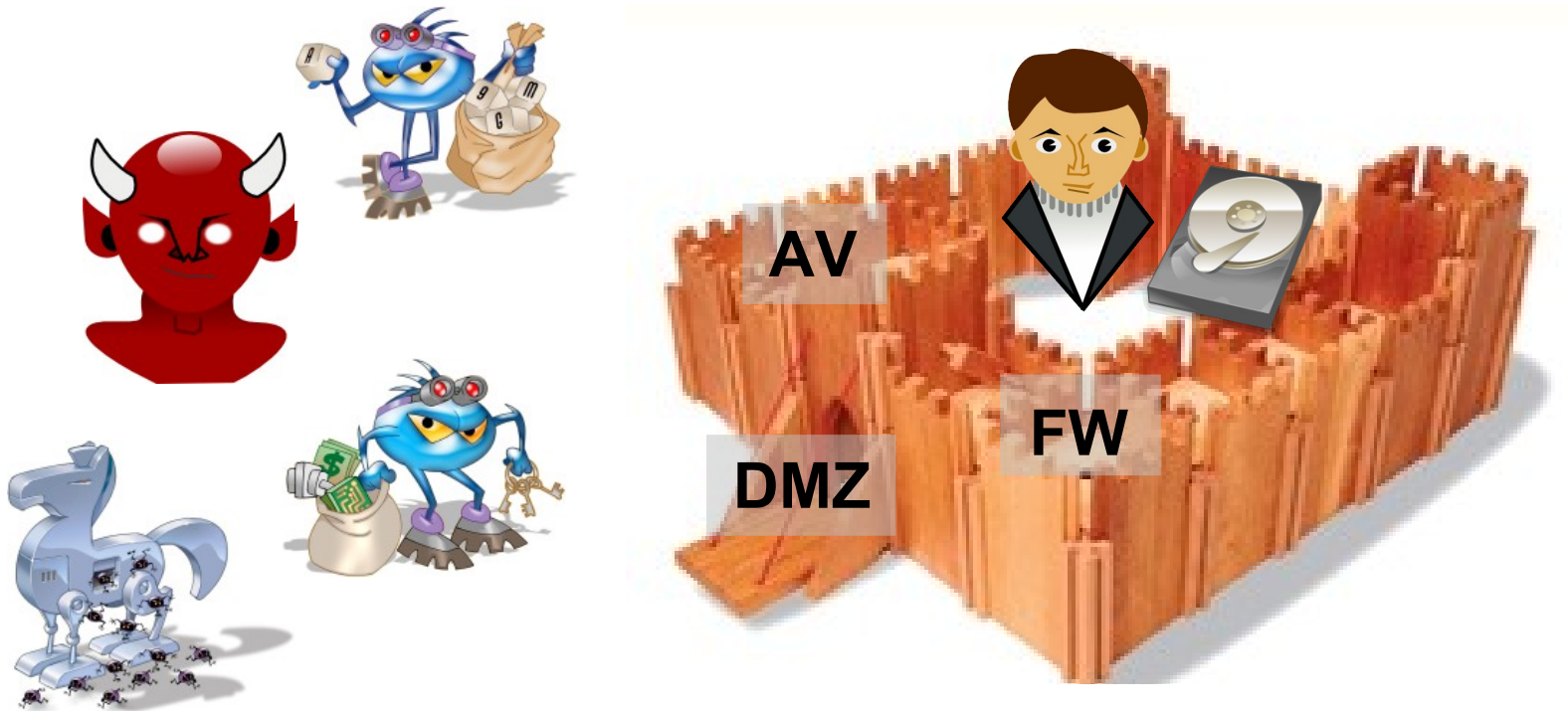


Quelle des Originals: <http://aws.amazon.com/security>

Firewalls im klassischen Fall

Auf einer Ebene mit den Daten

- Klassisch: Nutzer und Daten sind auf derselben Seite
 - Schutzmaßnahmen wie AV, DMZ und FW wirken!

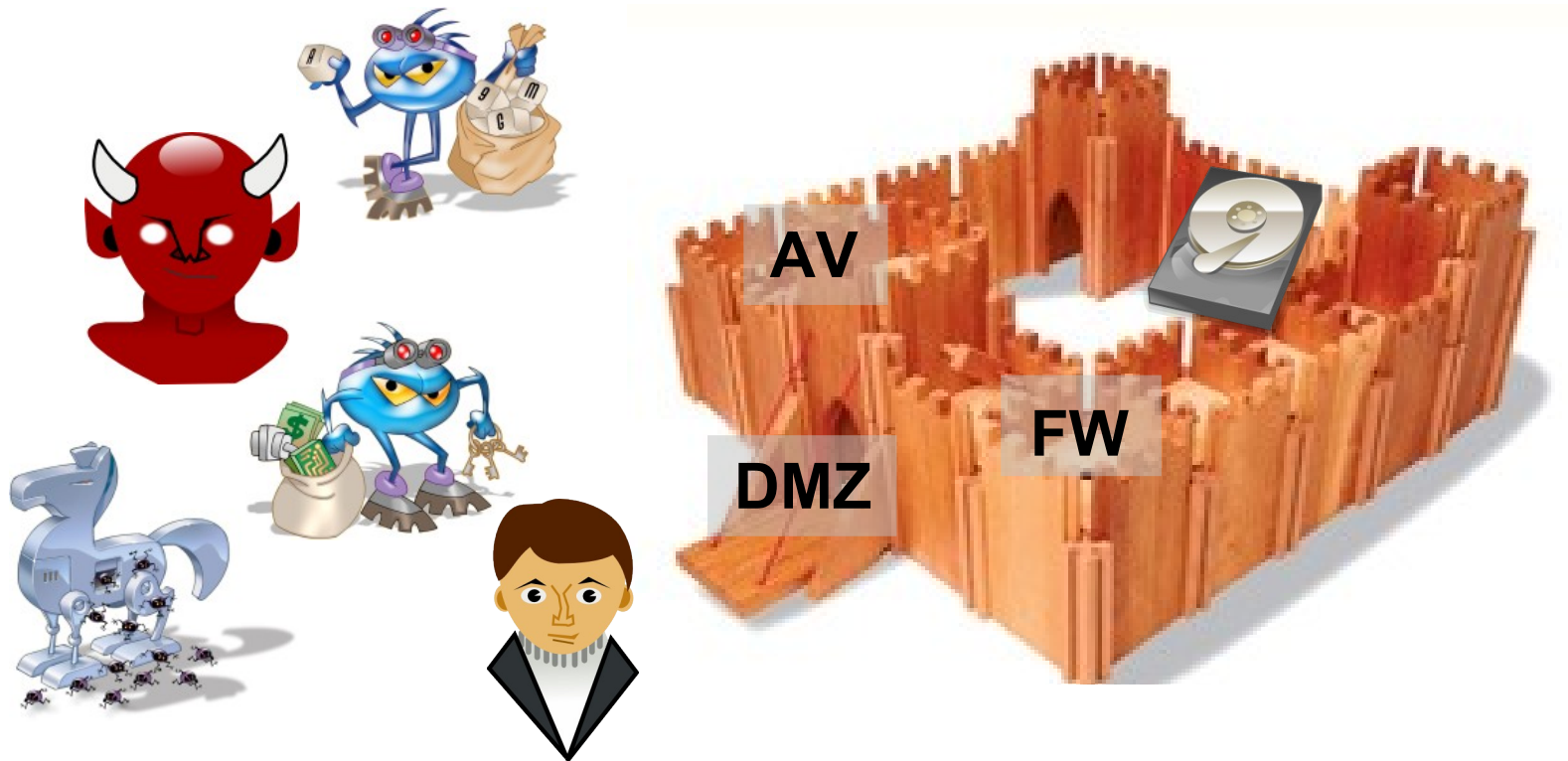


Quelle: <http://www.antispam.br/glossario/> und <http://www.holztiger.de/>

Firewalls bei SaaS

Auf einer Ebene mit dem Angreifer

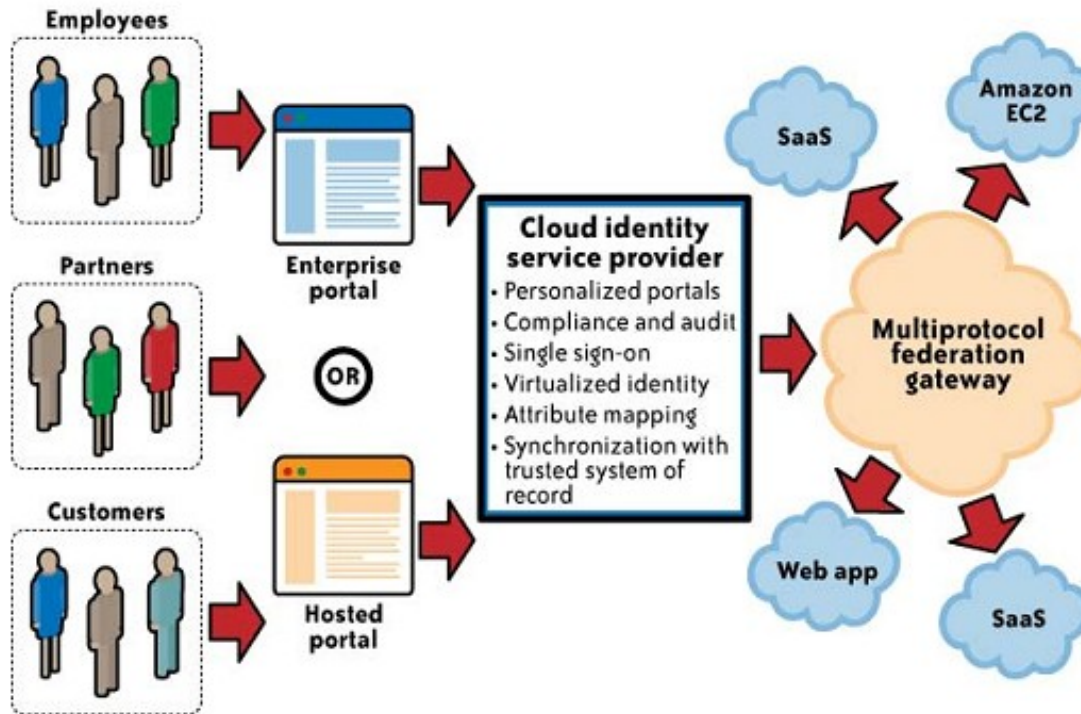
- SaaS: Nutzer und Daten sind auf verschiedenen Seiten
 - Schutzmaßnahmen im eigenen Netz hier nahezu nutzlos!



Quelle: <http://www.antispam.br/glossario/> und <http://www.holztiger.de/>

Identitymanagement für die Cloud

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



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

Problem: 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

Sicheres Cloud Computing

Beispiel: AWS Security

- Zertifikate und Akkreditierungen
 - SAS-70 konform, HIPAA-gesegnet, ...
 - Aber: Was sagt ein Zertifikat wirklich aus?
- Sicherheit der Rechenzentren
 - Geheime Standorte der Rechenzentren
 - Security by Obscurity?
 - Strikte Zugangskontrolle zum Rechenzentrum
 - Begleitung von Besuchern und Dienstleistern
 - Zweifache Zwei-Faktor-Authentifizierung des Personals
 - Sicherheitsüberprüfung der Mitarbeiter
- Ergänzende Maßnahmen
 - Sicherheitsmechanismen der API
 - Strikte Separierung der virtuellen Systeme

Compliance Fragestellungen

Cloud Computing und Compliance

- Vielzahl von Compliance-Anforderungen
 - Lokale Datenschutzgesetzgebung
 - Zahlreiche Regularien (HIPAA, PCI DSS, SOX,...)
- Beispiel "Payment Card Industry Data Security Standard"
 - Explizite Firewall notwendig
 - Expliziter Virenschutz notwendig
 - Verschlüsselte Kommunikation erforderlich
- Cloud Computing bringt neue Herausforderungen
 - Wo sind die Daten wirklich gespeichert?
 - Konzept zum Umgang mit sensiblen Daten?

Cloud Computing und Datenschutz

- "Verarbeitung" von personenbezogenen Daten:
Übermittlung vs. Auftragsdatenverarbeitung
- Übermittlung
 - Beispiel: SaaS (als Funktionsübertragung)
 - Richtlinie 95/46/EG: Keine Übermittlung an Stellen außerhalb der EU, wenn kein angemessenes Datenschutzniveau gegeben (äquivalente Regelung in §4b Abs. 2 BDSG)
 - "Safe Harbor"-Regelung ermöglicht Übermittlung in die USA
 - "Safe Harbor" und Cloud-Anbieter?
- Auftragsdatenverarbeitung
 - Beispiel: IaaS
 - Anforderungen nach §11 BDSG sind zu beachten
 - Wie lassen sich diese Anforderungen überprüfen?

Cloud Computing und Datenschutz Lösungsansätze

- Speicherung nur auf Cloud-Bereichen innerhalb der EU
 - Kann man das wirklich kontrollieren?
- Speicherung bei "Safe Harbor"-konformen Anbietern
 - Infos unter: <https://www.export.gov/safehrbr/list.aspx>
- Umsetzung mittels "Hybridkonzept"
 - Teil der Applikation läuft in der Cloud-Umgebung
 - Datenschutz-relevante Bereiche liegen außerhalb
- Umsetzung der datenschutzrechtlichen Regelungen
 - Einwilligung des Betroffenen einholen
 - Wird dies von den Nutzern akzeptiert werden?
 - Anforderungen zur Auftragsdatenverarbeitung erfüllen
 - Wie lässt sich dies im internationalen Umfeld umsetzen?

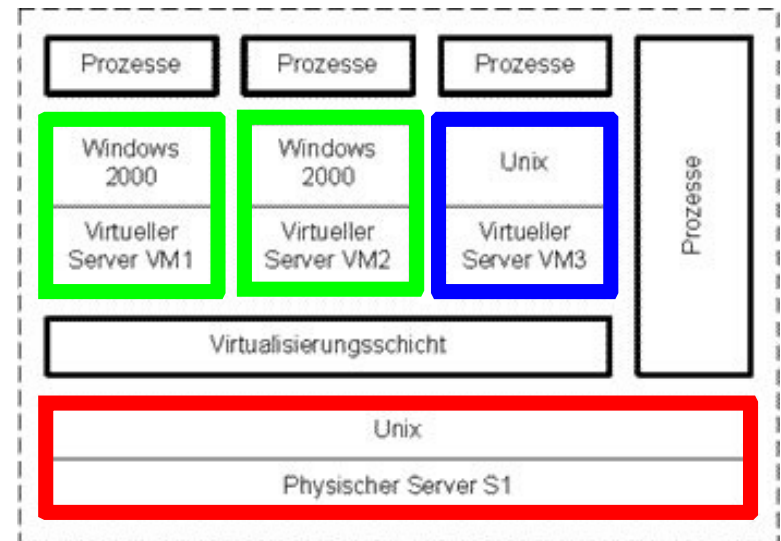
Cloud Computing und BSI IT-Grundschutz

- 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?

BSI IT-Grundschutz

Beispielsystem mit Virtualisierung

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



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

BSI IT-Grundschutz Baustein "Virtualisierung"

- Erste Vorstellung auf dem 1. IT-Grundschutz-Tag 2010
 - Zurzeit noch finale Abstimmung
- Ausgewählte Maßnahmen
 - M 1.v1 (A): Planung der virtuellen Infrastruktur
 - M 3.v1 (B): Schulung der Administratoren virtueller Umgebungen
 - M 4.v3 (A): Sichere Konfiguration virtueller IT-Systeme
 - M 5.v2 (B): Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen
 - M 4.v7 (A): Sicherer Betrieb von virtuellen Infrastrukturen
 - M 2.v5 (B): Überwachung der Funktion und Konfiguration virtueller Infrastrukturen
 - M 6.v1 (C): Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten

Cloud Computing

Relevanz von Audits

- 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?
 - Ist das untersuchte System noch aktuell?
 - Wie detailliert/vollständig ist der Audit-Bericht?

Cloud Computing Lizenzfragen

- 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"!
- Lässt sich eine vorhanden EA-Lizenz "verclouden"?
 - AWS bietet dafür ein zeitlich begrenztes(!) Modell an:
"Bring Your Own EA Windows Server License to EC2!"
- Vorsicht mit "fremden" Machine Images (MI)!

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

SLAs für das Cloud Computing

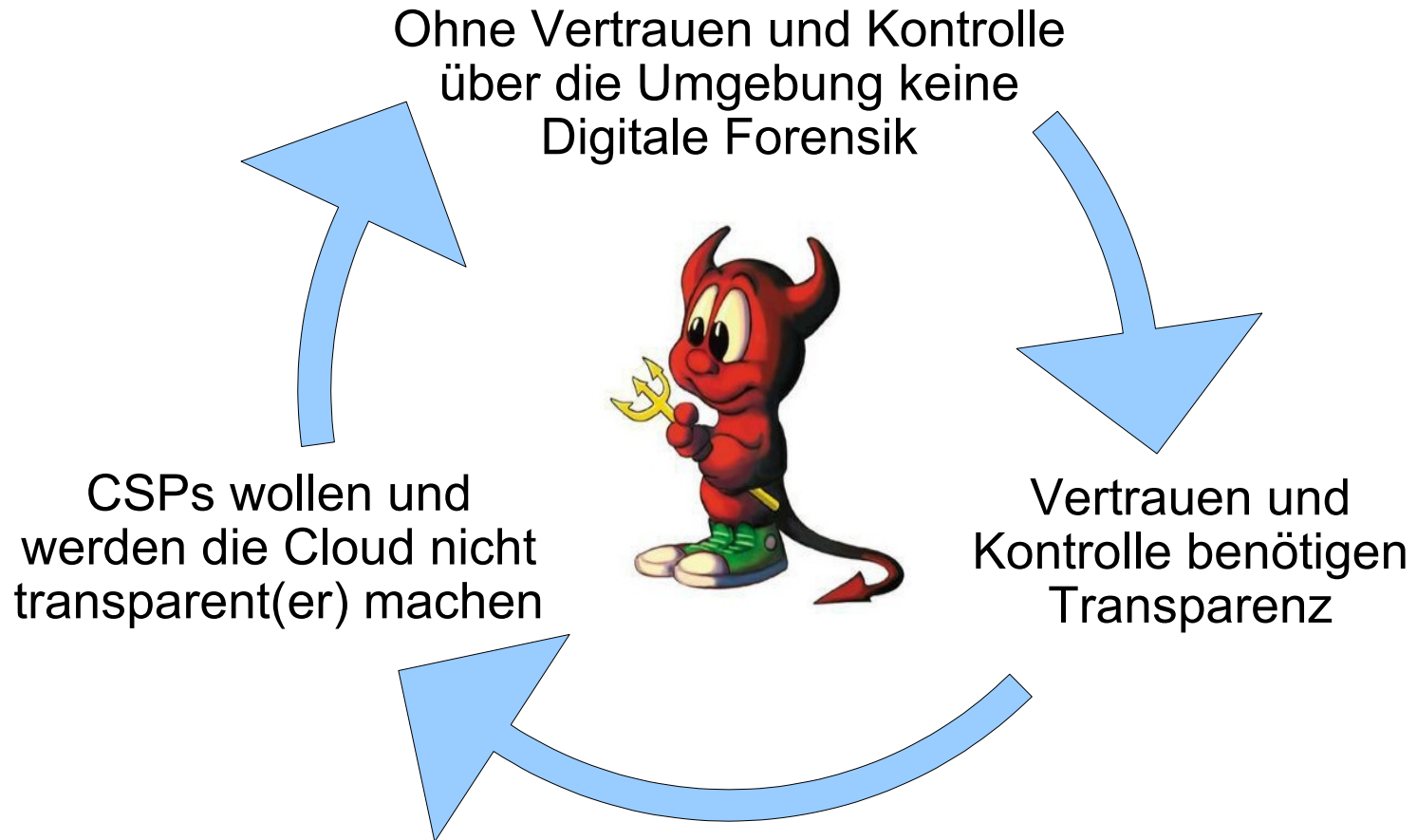
Leistung garantiert?

- 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

Forensik in der Cloud

Forensik in der Cloud

Teuflische Bedingungen



XaaS und Forensik

Welche Daten sind verfügbar?

- Forensik bei IaaS
 - Volle Kontrolle über die Virtuelle Maschine
 - Aber nicht über das Host-System
 - Was passiert, wenn die VM gekappt wird?
- Forensik bei PaaS
 - Kontrolle über die Anwendungen
 - Aber keinerlei Einfluss auf Korrektheit der Logdaten (da keinerlei Kontrolle über das Betriebssystem!)
- Forensik bei SaaS
 - Eigentlich sind Hopfen und Malz verloren! :(
 - Kleiner Rettungsanker: High-level Logs verfügbar?

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?
 - Geheime Rechenzentren?
 - Reaktionszeit im Falle eines Falles?
 - Wie kann die Integrität der Daten sichergestellt werden?
 - Physischer Zugang zum Datenträger?
- Problem bleibt der nicht vorhandene physische Zugriff
 - Was bedeutet dies für rechtliche Auseinandersetzungen?

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-Technik eröffnet 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!

Zusammenfassung und Fazit

Goldene Regeln für die Cloud

- Informieren Sie sich möglichst weitreichend über die Sicherheit bei Ihrem CSP
 - Bei IaaS Abschottungsmöglichkeiten nutzen
 - Zudem Konzepte der Layered Defense beachten
- Prüfen Sie, inwieweit Ihr CSP auditiert/zertifiziert ist
 - Beispielsweise ISO 27001, SAS 70, ...
 - Ist Ihr CSP dem "Safe Harbor Act" beigetreten?
- Nutzen Sie -wenn immer möglich- Verschlüsselung
 - 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!"

"Chancen" des Cloud Computing

- Cloud Computing zwingt zu strikten Maßnahmen bezüglich Datensicherheit und Datenschutz
 - "Konzept der grünen Wiese" möglich
 - Erhebliches Potenzial, vieles besser machen zu können
- Bessere Verfügbarkeit
 - Bezahlbare Verteilung der Rechenzentren
- Schnellere Sicherheitsupdates
 - Homogene Systeme
- Weniger Energieverbrauch, weniger Kosten
 - "On-demand"-Computing
- Unabhängigkeit von eigenen Ressourcen

"Restrisiken" des Cloud Computing

- Vertrauen in den Cloud-Anbieter
 - Zugriff auf die Hardware
 - Zugriff auf das Netzwerk
 - Zugriff auf die Machine Images
- Was passiert, wenn der Cloud-Anbieter
 - verkauft wird?
 - insolvent ist?
- Rechtliche Unsicherheiten
 - Vertragsgestaltung
 - Datenschutzaspekte
- Abhängigkeit von fremden Ressourcen

Fazit und Ausblick

- Virtualisierungskonzepte und Cloud Computing bieten erhebliche Chancen
 - Bessere Verfügbarkeit, Skalierbarkeit, ...
 - 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! :)

Informationen "Cloud Computing"

Einige nützliche Links (1)

- Amazon Web Service Security (AWS Security)
<http://aws.amazon.com/security>
- Cloud Security Alliance (CSA)
<http://www.cloudsecurityalliance.org/>
- NIST Computer Security Division – Cloud Computing
<http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>
- 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>

Informationen "Virtualisierung"

Einige nützliche Links (2)

- Tipps zur Härtung von VMware ESX Servern
http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf
- ESX Security Implementation Guide des DoD
http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf
- Risk Assessment zu VMware ESX Server 3.5i
<http://viops.vmware.com/home/docs/DOC-1032>
- Tipps zur Realisierung virtualisierter DMZs
http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf

Informationen "Virtualisierung"

Einige nützliche Links (3)

- "SubVirt"-Rootkit von King
<http://www.eecs.umich.edu/Rio/papers/king06.pdf>
- "Blue Pill"-Rootkit von Rutkowska
<http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html>
- "Hardware Virtualisation Rootkits" von Zovi
http://www.theta44.org/software/HVM_Rootkits_ddz_bh-usa-06.pdf
- Immunity Cloudburst
<http://www.immunityinc.com/documentation/cloudburst-vista.html>
- Google ist Ihr Freund! :)
<http://www.google.de/search?q=cloud+security>

Informationen "Cloud Computing"

Interessante Literatur

- 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 :)

- Dominik Birk

Kontakt per E-Mail: dominik@code-foundation.de

Mehr Infos im Web: www.code-foundation.de



- Dr. Christoph Wegener

Kontakt per E-Mail: wegener@wecon.net

Mehr Infos im Web: www.wecon.net

