Sicherheit in der Cloud – Chancen und Risiken

Dr. Tim Sattler

tim.sattler<at>hamburg.de

OWASP

Stammtisch Hamburg
14.04.2011

The OWASP Foundation

http://www.owasp.org

Zur Person

- Dr. Tim Sattler
  - Studium der Physik
  - seit 2000: Vollzeit in Informationssicherheit
  - seit 2008: IT Security Officer, Bauer Systems KG
  - CISSP, CISM, CISA, CCSK

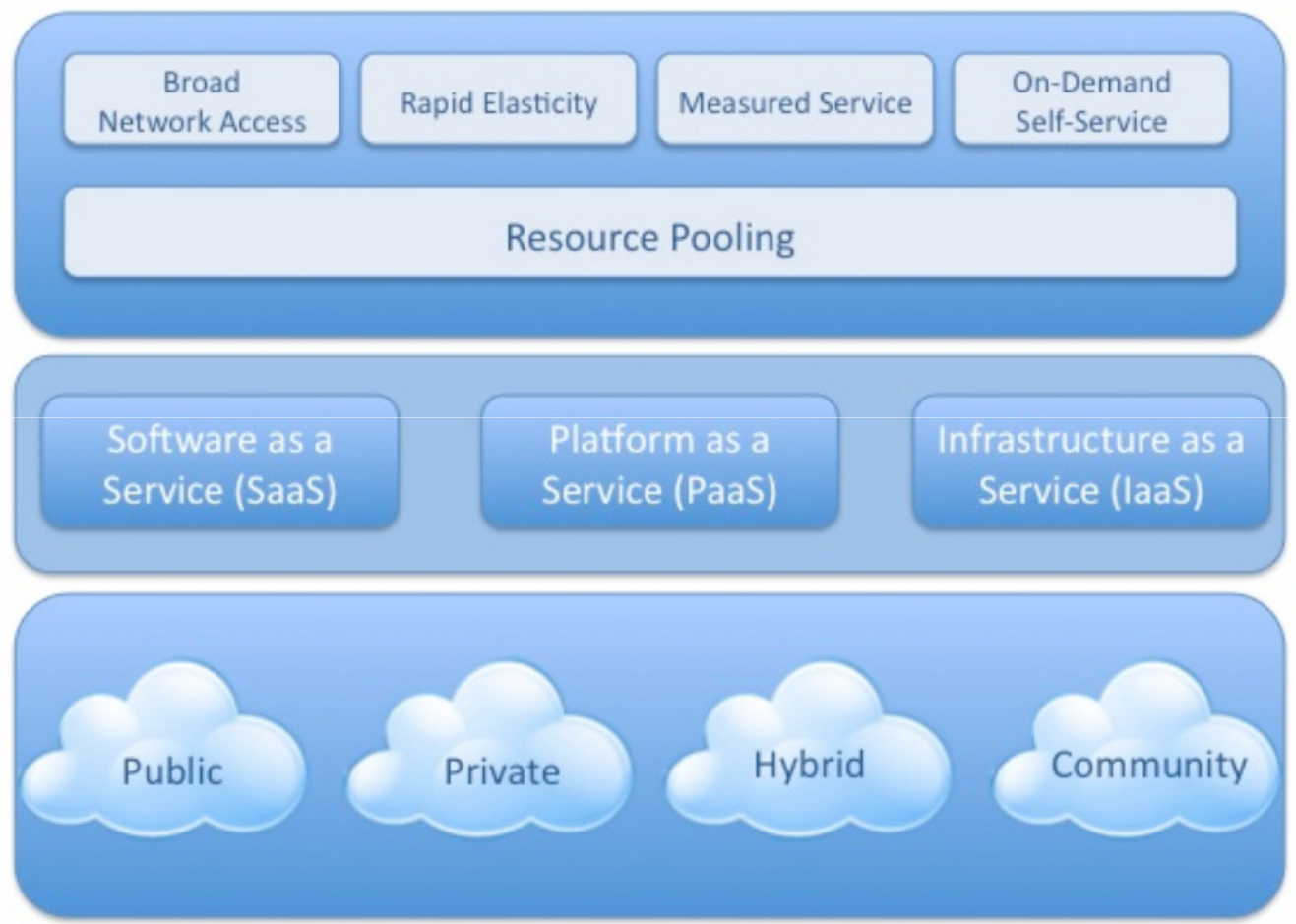
Agenda

- Was ist Cloud Computing?
  - Definition
  - Eigenschaften
  - Servicemodelle
  - Bereitstellungsmodelle
- Sicherheit von Cloud Computing
  - Kernthemen
  - Chancen
  - Risiken
  - Lösungsansätze

Was ist Cloud Computing?

- NIST: “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
- Gartner: “a style of computing where scalable and elastic IT-related capabilities are provided 'as a service' to customers using Internet technologies.”

NIST Cloud Computing Modell



Wesentliche Cloud-Eigenschaften (1)

- On-demand Self-service
  - Selbstbedienung
- Broad Network Access
  - Bereitstellung über Internetprotokolle
  - Heterogene Endgeräte
- Resource Pooling
  - Services teilen sich Ressourcen
  - Ortunabhängigkeit
  - Mandantenfähigkeit

Wesentliche Cloud-Eigenschaften (2)

- Rapid Elasticity
  - Skalierbarkeit
  - Schnelle Reaktion auf Bedarfsänderung
- Measured Service
  - Verfolgung der Nutzungsdaten
  - Unterschiedliche Vergütungsmodelle

Quelle: The NIST Definition of Cloud Computing, Draft SP 800-145
http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Weitere typische Cloud-Eigenschaften

- Nutzung von Skaleneffekten
- Homogenität
- Einsatz von Virtualisierungstechnologien
- Resilient Computing
- Einsatz von Low-Cost-Software
- Geographische Verteilung
- Serviceorientierung
- Fortschrittliche Sicherheitstechnologien

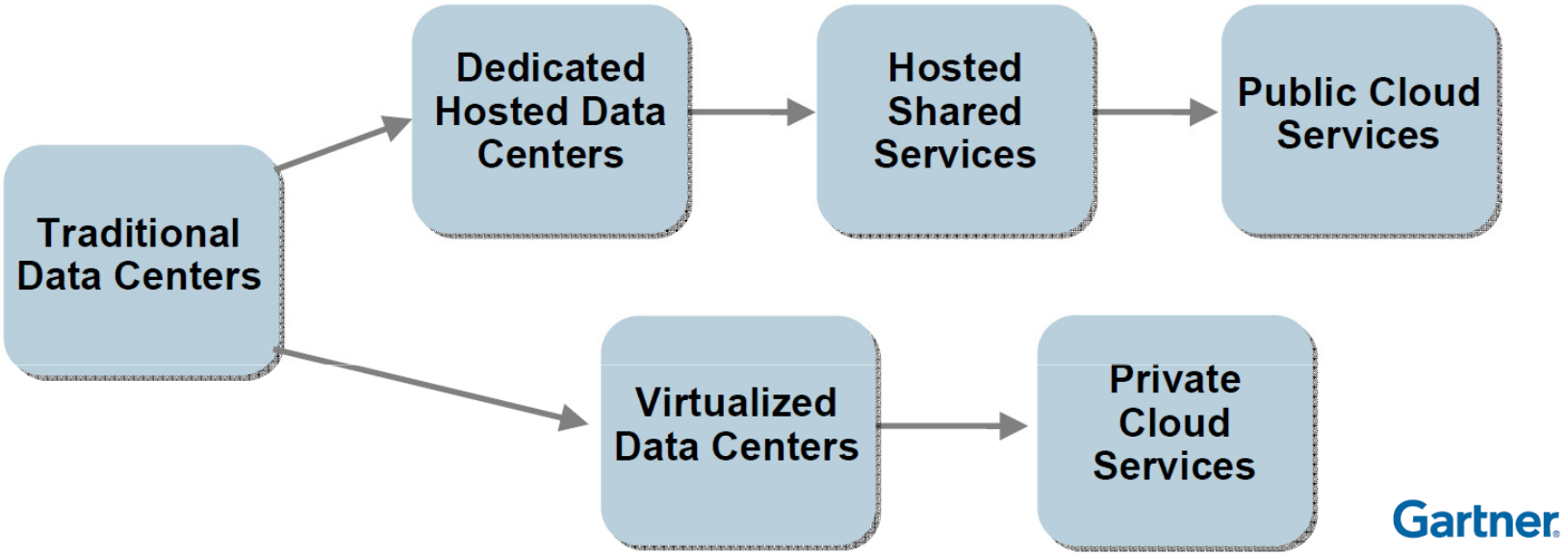
Cloud-Servicemodelle

- Software-as-a-Service (SaaS)
  - Cloud-Provider stellt Anwendung bereit
  - Daten kommen vom Cloud-Kunden
- Platform-as-a-Service (PaaS)
  - Cloud-Provider stellt Entwicklungs- und Runtime-Umgebung bereit
  - Anwendung und Daten kommen vom Cloud-Kunden
- Infrastructure-as-a-Service (IaaS)
  - Cloud-Provider stellt Rechenleistung, Storage oder andere grundlegende IT-Ressourcen bereit

Cloud-Bereitstellungsmodelle

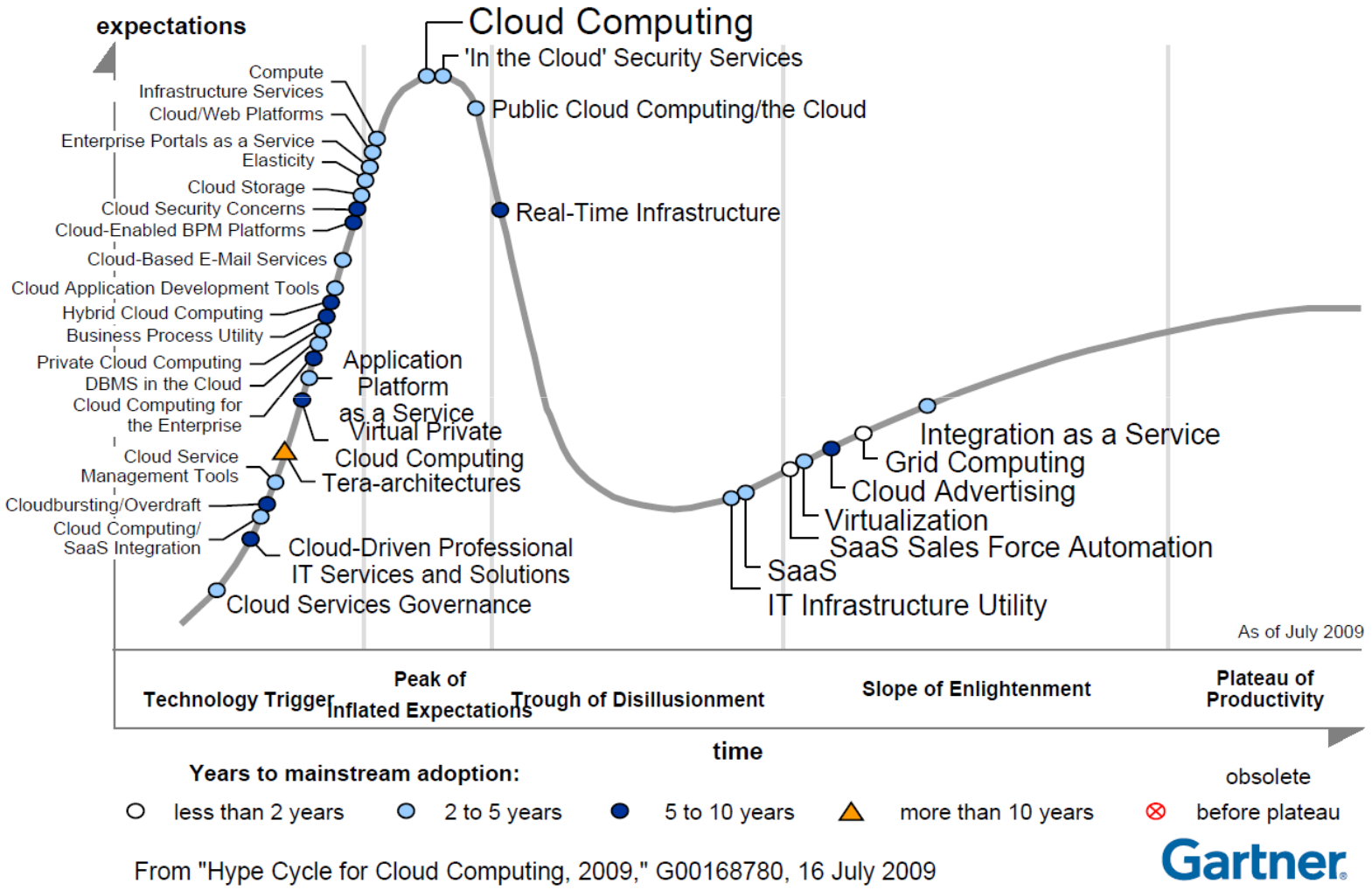
- Private Cloud
  - unternehmenseigene oder gemietete Infrastruktur
  - privat ≠ intern
- Community Cloud (Partner Cloud)
  - gemeinsam genutzte Infrastruktur für spezifische Nutzergruppe
- Public Cloud
  - öffentliches Angebot an eine breite Nutzergruppe
- Hybrid Cloud
  - Kombination von zwei oder mehr Clouds

“Cloud” ist nicht immer Cloud



- Public Cloud ⊃ Outsourcing
- Private Cloud ⊃ Virtualisierung

Cloud Computing wird Standardtechnologie

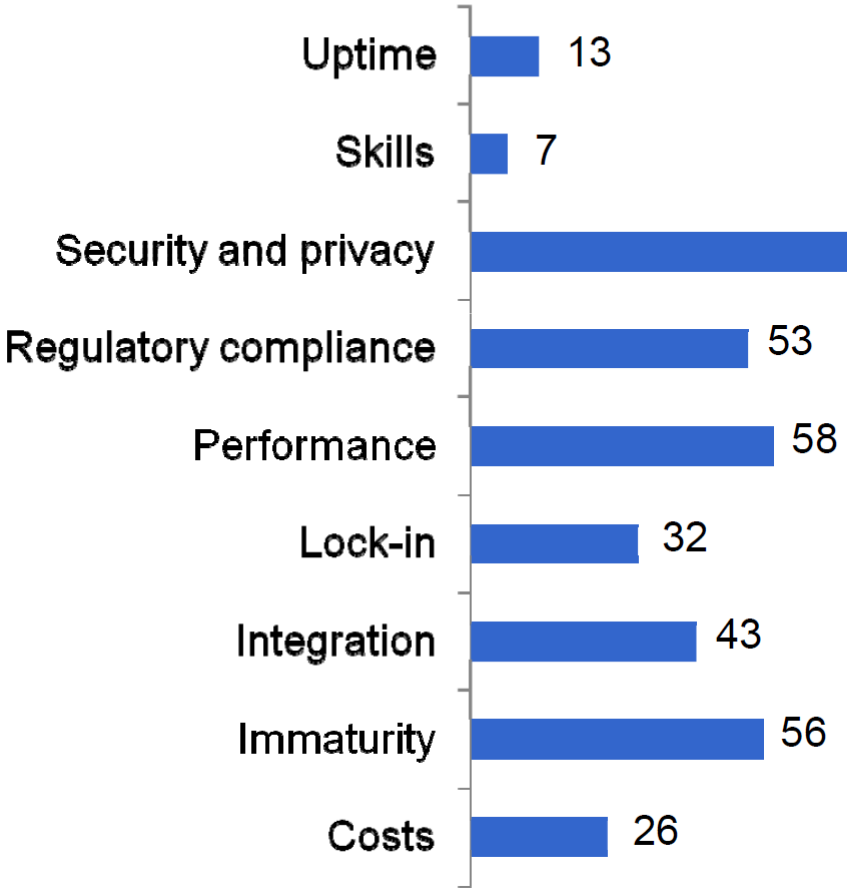


From "Hype Cycle for Cloud Computing, 2009," G00168780, 16 July 2009

Gartner

Sicherheit ist das große Thema

What are your top three concerns (in priority order) with external cloud computing services?



Dec. 2009 Gartner Data Center Conference Poll

n = 94
Weighted scores:
1st priority = 3
2nd priority = 2
3rd priority = 1

Gartner

Cloud Computing in den Schlagzeilen (1)

DIE ZEIT
17.02.2011

Es war die schlimmste Erfahrung seines Berufslebens. »Zwei Tage lang war unsere Firma komplett lahmgelegt«, sagt Bernhard Bahners, Gründer und Prokurist des Internet-Start-ups Radio.de. »Sie können sich gar nicht vorstellen, was hier los war!« Los war Folgendes: Niemand in der ganzen Firma konnte mehr auf irgendein internes Dokument zugreifen; Kunden wunderten sich, dass ihre E-Mails unbeantwortet blieben; 48 Stunden lang war die Firma ohne Daten und Büro-Software. Dabei war an den beiden Standorten von Radio.de in Hamburg und Innsbruck technisch alles in Ordnung, die Computer liefen, die Datenleitungen funktionierten. Der Grund für den Totalausfall im vergangenen Dezember: ein Fehler im Bezahlsystem von Google.

Weil ein Rechnungsbetrag von wenigen Hundert Euro nicht abgebucht werden konnte, hatte der kalifornische Gigant der deutschen Firma kurzerhand den Zugang zu ihrer Büro-Software und den zugehörigen Unterlagen gesperrt. Ohne Vorwarnung. »Am liebsten hätte ich das Geld in einen Umschlag gepackt und persönlich hingetragen«, sagt Bahners. Aber er habe nicht einmal gewusst, wohin. Für mittelständische europäische Kunden ist die Google-Niederlassung in Dublin zuständig, telefonisch erreichbar ist sie jedoch nicht. Und jene Hilferufe, die der entsetzte Bahners per EMail schickte und ins Formular auf der Google-Website eintrug, blieben zunächst unerhört.

Cloud Computing in den Schlagzeilen (2)

Amazon bestreitet politischen Druck wegen Wikileaks

heise online

03.12.2010

Der Online-Einzelhändler Amazon bestreitet, die Enthüllungsplattform Wikileaks auf politischen Druck hin von seinen Servern genommen zu haben. Wikileaks habe gegen die Nutzungsbedingungen verstoßen, teilte Amazon mit. Wikileaks hatte bei der Veröffentlichung der diplomatischen US-Depeschen auf den Amazon Web Service zurückgegriffen, um die hohen Zugriffszahlen auf die Dokumente bewältigen zu können.

Die Geschäftsbedingungen von Amazon Web Services AWS, der Hosting- und Cloud-Sparte von Amazon, sähen vor, dass der Kunde die Rechte an den Inhalten halte und deren Einsatz niemandem Schaden zufüge. "Es ist klar, dass Wikileaks nicht über die Rechte an den vertraulichen Dokumenten verfügt", argumentierte Amazon nun. Auch könne bei der großen Zahl von 250.000 Depeschen nicht gesichert sein, dass durch deren Veröffentlichung nicht Unschuldige wie etwa Menschenrechtler in Gefahr gerieten.

Es gebe hunderttausende Kunden, die alle Arten von Daten bei AWS speicherten, über einige davon werde auch kontrovers diskutiert – das sei aber völlig in Ordnung, meint man bei Amazon. Aber wenn Unternehmen oder Personen große Mengen von Daten speicherten, auf die sie rechtmäßig keinen Anspruch erheben könnten, und wenn sie Daten veröffentlichten ohne sicherzustellen, dass dadurch andere nicht in Gefahr gerieten, dann sei das eine Verletzung der Amazon-Nutzungsbestimmungen; diese Leute müssten dann anderswo unterkommen.

Cloud Computing in den Schlagzeilen (3)

Cloud Computing: Flickr verliert 4.000 Fotos eines Nutzers und kann sie nicht mehr finden

T e c Z i l l a
02.02.2011

Dass grenzenloses Vertrauen in sicheres Cloud Computing so leichtsinnig sein kann wie eine Festplatte ohne Backup, musste eben ein Nutzer des Foto-Sharing-Dienstes Flickr erfahren. Als Fotoblogger Mirco Wilhelm aus Zürich eben mal wieder einloggen wollte, wurde er zur Erstellung eines neuen Accounts aufgefordert. Er fragte verwundert bei Flickr nach und musste erfahren, dass sein Account durch eine Verwechslung versehentlich gelöscht wurde.

4.000 Bilder aus fünf Jahren

Eine Wiederherstellung war nicht mehr möglich, so etwas hatten die Systemarchitekten bei Flickr nie vorgesehen. Gelöscht waren damit rund 4.000 Bilder aus den letzten fünf Jahren und all ihre Verlinkungen. Die Fotos hatte Wilhelm offenbar auch anderweitig gesichert und damit die ganz große Katastrophe vermieden. Aber er schätzt den Aufwand, all diese Links und Bildbeschreibungen manuell wiederherzustellen, auf Wochen oder Monate seiner Freizeit. Außen vor bleiben dabei noch die Verlinkungen durch externe Websites, unter anderem bei offiziellen Blogs von Flickr und Yahoo, dem Betreiber des Dienstes.

Cloud Computing in den Schlagzeilen (4)

Security researcher questions design of Dropbox authentication

By *paulmah*
Created *Apr 12 2011 - 6:36am*
Security researcher Derek Newton explored the inner workings of several popular file synchronization tools, and decided to start with Dropbox due to its popularity. In a nutshell, Newton made the startling discovery that authentication in Dropbox was tied to a single hash code stored as a plain text file, created when a computer (or smartphone) is first linked to an account. What proved disturbing though, was that the unchanging hash code continues to work even after a password change; gaining access to a hash code effectively gives an attacker lifetime access to an account--unless the specific device is specifically unauthorized.

In response to the original blog post by Newton, Dropbox commented [1] that "the security battle is already lost" should an attacker gain physical access to a computer in the first place. Noting that Dropbox takes security very seriously, Dropbox said that it did not "agree with the assertion that there is a security flaw," using the use of stolen session cookies to illustrate the comparable risks.

FierceCIO
12.04.2011

Cloud Computing in den Schlagzeilen (5)

Amazon-Cloud regional gestört

ZDNet

18.03.2011

Die Elastic Compute Cloud von Amazon Web Services hat vergangene Nacht mit Störungen gekämpft. Betroffen waren die für die US-Ostküste zuständigen Server. Einige bekannte Online-Dienste, die Amazon-Kunden sind, waren deshalb nicht erreichbar.

Mehr zum Thema

- Microsoft-Community Answers kämpft nach Redesign mit Ausfällen
- Mehr als einstündiger Ausfall bei Paypal
- Facebook bestätigt kurzen Ausfall
- Hardwarefehler führt zu Amazon-Ausfall

Zu den betroffenen Diensten zählten Reddit und Heroku. Insbesondere der Nachrichten-Sammeldienst Reddit hat inzwischen öffentlich die Frage gestellt, wie zuverlässig Amazon Web Services eigentlich ist. Der Dienst ist ohnehin schon seit einigen Wochen damit beschäftigt, seine zentrale Datenbank "Cassandra" auf lokale Systeme zu bringen.

Amazon hat zwischendurch ein "Fehlverhalten eines Netzwerkgeräts" gemeldet, die man behoben habe. Für einen folgenden erneuten Ausfall gibt es bisher keine offizielle Erklärung.

Besonders drastisch hat sich ein ehemaliger Programmierer von Reddit, David King, in einem Diskussionsform geäußert. Unter seinem Usernamen ketralnis schreibt er: "Amazons Elastic Block Store ist ein gewaltiger Lacher, was Leistung und Zuverlässigkeit angeht. Amazon muss das sofort beheben - oder Reddit von EC2 weggehen. Leider ist das ein riesiges Projekt und Reddit hat ohnehin viel zu wenige Mitarbeiter."

Cloud Computing Security

- Clouds sind komplexe, hochgradig verteilte und virtualisierte Umgebungen.
- Kernthemen
  - Vertrauen
  - Ressourcenteilung
  - Verschlüsselung
  - Portabilität
  - Compliance
  - Datenschutz
- Cloud Computing birgt sowohl Chancen als auch Risiken

Chancen durch die Cloud (1)

- Skalenvorteile
  - "mehr Sicherheit" für den gleichen Investitionsbetrag
- Sicherheit als Entscheidungskriterium im Markt
  - Cloud-Provider müssen auf Sicherheitsbedenken der Kunden reagieren
- Standardisierte Schnittstellen für Managed Security Services (MSS)
  - Offenerer Markt für Sicherheitslösungen
- Beweissicherung und IT-Forensik
  - Snapshots von laufenden virtuellen Maschinen zur Offline-Analyse möglich

Chancen durch die Cloud (2)

- Skalierbarkeit und Elastizität von Ressourcen
  - Erhöhung der Ausfallsicherheit (z.B. bei DDoS-Angriffen)
- Effektiveres Patchmanagement
  - Homogenität
  - Standardisierte, gehärtete Plattformen
- Vorteile durch Konzentration von Ressourcen
  - Kostenvorteile bei der Absicherung am Perimeter und bei physischen Kontrollen
  - aber: Konzentration birgt natürlich auch Nachteile

Risiken durch die Cloud (1)

- Steuerungs- und Kontrollverlust
  - mangelnde Transparenz
    - kein Einblick in Betriebs- oder Sicherheitskonzepte
    - unklare oder unvollständige Vertragsbedingungen
    - keine Kontrolle über Outsourcing-/Vertragspartner
    - keine Benachrichtigung bei Sicherheitsvorfällen
  - Reaktion auf Auditfeststellungen nicht möglich
  - unvereinbare Sicherheits- und Compliance-Anforderungen von Kunde(n) und Provider
  - eingeschränkte Besitz- und Nutzungsrechte an Daten und Applikationen (“Software Escrow”)
  - Machtungleichgewicht Provider vs. Kunde

Risiken durch die Cloud (2)

- Lock-In
  - Was passiert bei...
    - Vertragsänderungen zu Ungunsten des Kunden?
    - Insolvenz oder Übernahme des Providers (“Bank Run”)?
  - Migration von Daten und Anwendungen möglich?
  - Offene, standardisierte Schnittstellen und Datenformate vorhanden?
  - Lock-In liegt im Interesse des Providers
- Isolationsversagen
  - Kompromittierung des Hypervisors, Guest Hopping, Datenremanenz, Network Sniffing

Risiken durch die Cloud (3)

- Compliance-Risiken
  - Regulatorien sind nicht oder noch nicht vollständig an Cloud Computing angepasst (z.B. PCI-DSS)
  - Provider kann Compliance nicht nachweisen
  - Provider erlaubt keine Überprüfung (Audit) oder Zertifizierung
- Kompromittierung der Management-Schnittstelle
  - häufig webbasiert, damit anfällig für typische Schwachstellen in Webapplikationen (z.B. OWASP Top 10) und Webservices

Risiken durch die Cloud (4)

- Datenschutz-Risiken
  - Auftragsdatenverarbeitung nur in EU/EWR möglich
  - Sonst Funktionsübertragung (§§ 4b, 4c, 28 Abs. 1 BDSG)
    - keine „Erforderlichkeit" der Verarbeitung außerhalb EU/EWR
    - „Schutzwürdiges Interesse" überwiegt außerhalb EU/EWR
  - Anforderungen nach § 11 BDSG in jedem Fall notwendig, aber nicht hinreichend
    - Wie lassen sich die Anforderungen kontrollieren?
  - „Legaler Zugriff" durch innerstaatliche Behörden oder Dritte nach nationalem Recht des Providers

Risiken durch die Cloud (5)

- Rechtliche Risiken
  - Änderungen des Gesetzgebers / der Rechtsprechung
  - Unterschiedliche Rechtsordnungen
  - Fehlende Rechtsschutzstandards
  - Durchsuchung / Beschlagnahme
  - Lizenzrisiken
- Unsicheres oder unvollständiges Löschen von Daten
  - Sicheres Löschen vs. Pooling und Elastizität

Risiken durch die Cloud (6)

- Malicious Insider beim Provider
  - Ausnutzen der Provider-Privilegien
- Erschöpfung der Ressourcen des Providers
  - Fehlerhafte Modellierung des Bedarfs
  - Unzureichende Investitionen
  - Keine Regelungen für Zuordnung knapper Ressourcen
- Schäden durch Aktivitäten anderer Mandanten
  - Finanzieller Schaden
  - Reputationsverlust

Risiken durch die Cloud (7)

- Economic Denial of Service (EDoS)
  - Verbrauch von Ressourcen zum Schaden des Kunden

Lösungsansätze (1)

- Provider-Auswahl unter Verwendung von Fragenkatalogen / Check-Listen
  - ENISA Information Assurance Requirements
  - BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter
- Mindeststandards für Public-Cloud-Provider
  - Zertifizierung nach SAS 70 Type II / ISO 27001
  - konfigurierbare Sicherheitsmechanismen
  - offene Standards und definierte Schnittstellen (siehe Open Cloud Manifesto)

Lösungsansätze (2)

- Verarbeitung sensitiver Daten in der Cloud nur bei Kontrolle über das Sicherheitsmodell
  - für große Organisationen: Aufbau einer Private Cloud
  - für mittlere Organisationen: Teilnahme an einer Community Cloud
  - Verschlüsselung löst das Problem nicht vollständig
    - Schlüsselmanagement
    - zur Laufzeit müssen Daten entschlüsselt sein

Absicherung nach Schutzbedarf

	Low	Medium	High
Public Cloud	• Security built into cloud is used • SAS 70 sufficient • 27001/FISMA	• Third-party security running in cloud is used • Custom/industry security assessment	• Security is performed outside the cloud • No trust of the cloud
Private Cloud	• Security built into VM is used • Accept vendor security claims	• Third-party security running on VM is used • Certification/ accreditation of system	• Security is performed outside the VM • Security product certification

Gartner

Publikationen

- Cloud Computing Risk Assessment, ENISA
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance
  - https://cloudsecurityalliance.org/csaguide.pdf
- Guidelines on Security and Privacy in Public Cloud Computing, Draft SP 800-144, NIST
  - http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
- Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter, BSI
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf