Gesellschaft für Informatik

IT in der Cloud aus Sicht eines Anwenderunternehmens

DB Systel GmbH

Stefan Hirschberg

I.LVE 1(1)

26.02.2016

Agenda

1. **Wolkenbildung**
2. Heiter bis wolkig
3. Wolkenkuckucksheim

Ausgangssituation: steigender Bedarf an mehr Flexibilität und Innovation bei marktgerechten Preisen

Stetiger Kostendruck stellt die heutige IT vor teilweise unlösbare Aufgaben, derzeit manuelle Tätigkeiten müssen zukünftig automatisiert oder durch eine höhere Standardisierung vereinfach und dadurch kosteneffizienter werden

Kostendruck

Heutige Anforderungen an die IT setzen voraus, dass jederzeit und überall, auf Knopfdruck, IT-Ressourcen und IT- Services zur Verfügung stehen, schnell erweitert und flexibel abgeschaltet werden können.

Flexibilität

Cloud Lösungen

- Flexibilität durch vordefinierte und durch den Kunden konfigurierbare Services
- Hoher Automatisierungsgrad möglich durch starke Standardisierung und vollständige Virtualisierung
- Möglichkeit der Pay per Use Verrechnung

Integration in die DB

Die DB Systel vereint in der **DB Enterprise Cloud** diesen Nutzen und bildet eine nachhaltige Integration in den DB Konzern

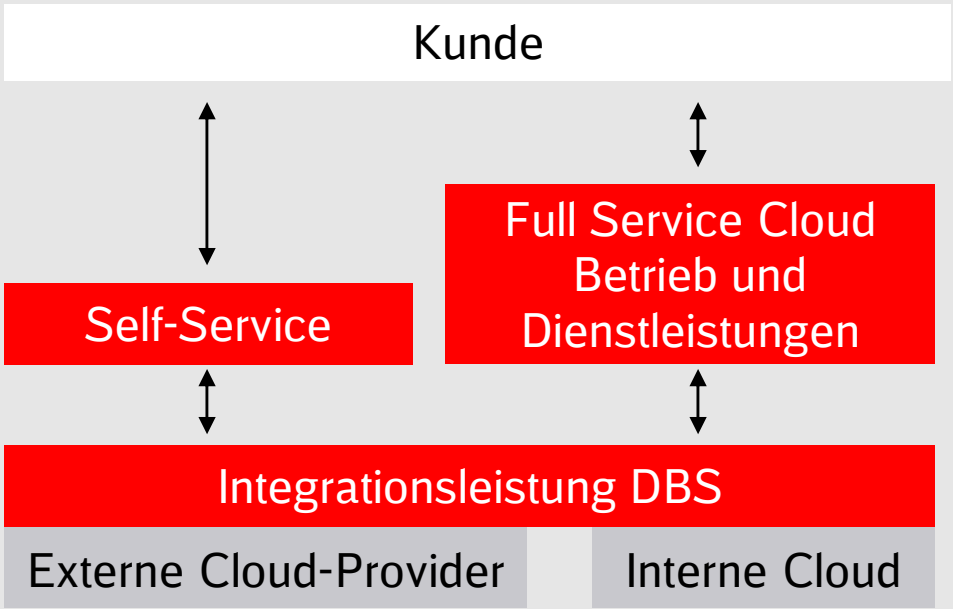
Vorgehensweise der Marktanalyse (PoC)

Evaluierung des Marktes	■ Auf Basis unabhängiger renommierter Rahmenvertragsanalysten (Forrester und Gartner) wurde eine Marktüberblick geschaffen ■ Identifikation der externen Cloud Provider nach Produktstrategien, Businessmodelle, Innovationen, geograph. Strategien, Services, Pricing, Market responsiveness etc.
Deep Dive der Top 4 (Gartner)	■ Auf Basis der Evaluierung des Marktes wurde durch detaillierter Assessments der aktuellen führenden externen Enterprise Cloud-Providern die einzelnen DB Systel spezifischen Capabilities analyisiert
DB Systel Eignungs-kriterien	■ Detaillierten Analysen der Capabilities der AWS, Google, IBM, MS Azure, VM Ware wurden gegen die bestehenden Eignungskriterien (kaufm., fachl., techn.) der DB Systel geprüft und bewertet
Ent-scheidung	■ Auf Basis der Prüfung gegen die Eignungskriterien der DB Systel wurde das Angebot von AWS ausgewählt

Die IT-Kompetenz im DB-Konzern liegt bei der DB Systel. Sie ist Generalunternehmer für Cloudlösungen der DB AG.

- Cloud – Lösung für die flexible Bereitstellung von IT-Ressourcen und komplexen Anwendungen
- Fertigungstiefen von low-SLA Self-Service des Kunden bis high-SLA Full-Service Betrieb durch die DB Systel
- Schutzbedarf von gering bis hoch inkl. Speicherung personenbezogener Daten möglich
- Nutzung von umfangreichen Services für den effizienten/automatisierten Einsatz hochstandardisierter IT-Ressourcen
- Pay per Use Verrechnungsmodell (Self-Service)
- Bedarfsorientierte Nutzung von externen Cloud-Providern und/oder interne IT je nach Anforderung/Fähigkeit der Anwendung

Integration von marktführenden externen Cloud Providern und internen Cloud Lösungen



Agenda

1. Wolkenbildung
2. **Heiter bis wolkig**
3. Wolkenkuckucksheim

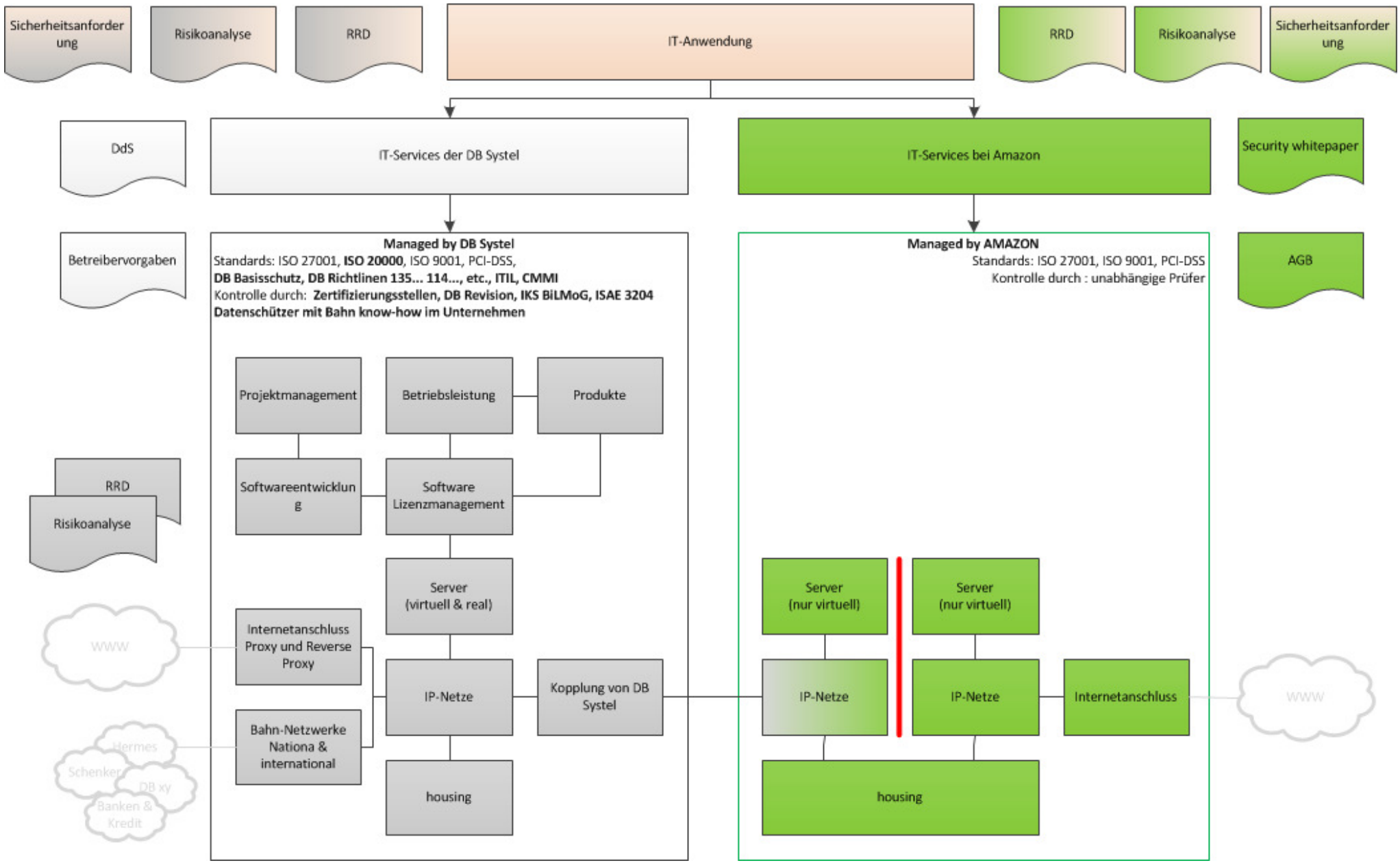
Ein Rollenmodell macht die Verantwortungen deutlich. Hier am Beispiel der unmanaged Services:

DB Mobility Networks Logistics

DB Systel hält bei einer Teilfertigung von Webservices durch Amazon die Sicherheitsanforderungen des Konzerns, ihrer Kunden und ihrer eigenen Sicherheitsstandards ein.

Shared responsibility model	▪ Die Verantwortung wird rollenbasiert geteilt: – **Der Kunde** trägt die Verantwortung für die Sicherheit seiner **Daten**; – **DB Systel** verantwortet die sichere **Integration der Web Services**; – **Amazon Web Services** verantwortet die Sicherheit für **Infrastruktur & IT-Systeme**.
Vertrauens-würdiger Partner	▪ AWS ist ein vertrauenswürdiger Partner/Lieferant für DB Systel bei der Bereitstellung von webbasierten Services. Amazon betreibt ein zertifiziertes, international anerkanntes Informationssicherheits-managementsystem. Es ist kompatibel mit dem Konzern-Basisschutz und den Sicherheitsregelungen und -verfahrensweisen bei DB Systel.
NDA	▪ AWS hat ein NDA (non-disclosure agreement) unterzeichnet und ist vertraglich daran gebunden.
Vertragsgrundlage	▪ Mit dem verbindlichen shared responsibility model als Basis, können DB Systel und ihre Kunden schlank und effizient ihre ITK-Risiken managen.

DB Enterprise Cloud: Architektur der unmanaged services



Das Geschäftsmodell der DB enterprise cloud wirkt auf das InformationsSicherheitsManagementSystem der DB Systel

Erhöhung

Prozess
- Schnittstellen
  - ggf. Medien- und Protokollbrüche
  - evtl. längeren Laufzeiten

Aufwand (regelmäßig)
- Geltungsbereich der Zertifikate abgleichen
- Anwendbarkeitserklärung von best practice Sicherheitsmaßnahmen prüfen
- Lieferantenaudits durchführen
- Kunden (DB) beraten und schulen
  - Anfangs mehr Bedarf
  - Später weniger

Währungsrisiko
- Fakturierung: **$** -> **€**

Reduktion

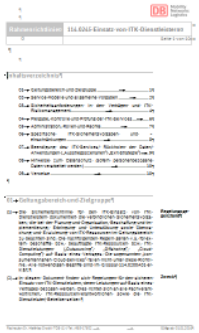
IT-System Risiko
- Weniger Angriffsfläche in der Infrastruktur (Bedrohung geht von der Anwendung aus)
- Auslastungsrisiko (geht zu AWS)

Technische Assets
- Weniger technische Infrastruktur-Audits
- Weniger Inventarverwaltung

Kapilalbindung
- Aus Investitionskosten werden Betriebskosten

Herausforderung für den Konzern: Es wurden die Governance-Vorgaben für die Cloud-Nutzung angepasst bzw. neu erstellt.

- Leitfaden („Gebrauchsanweisung“) für das Produkt „DB enterprise cloud unmanaged“
- Herausgeber: DB Systel und CIO-DB-Konzern
- Klärung von Rollen, Verantwortung und Kompetenzen zur angemessenen und sicheren Nutzung von AWS unmanaged



- Security Policy (DE/EN) zum Einsatz (externer) ITK-Dienstleister („Cloud“) 114.0245 im Rahmen des Frameworks ITK-Sicherheit
- Herausgeber: CIO DB-Konzern
- Erstellung und Beschluss innerhalb des ISB/ ITK-SIMs innerhalb von 8 Wochen, enge Abstimmung mit DB Systel

- „Cloud Computing Rahmenbedingungen“
- Herausgeber: Konzerndatenschutz und Datenschtz DB Systel
- praxisnahe Handlungshilfe für die datenschutzrechtlich zulässige Umsetzung von Cloudlösungen im DB-Konzern

Herausforderung für DB Systel: Bewusstsein beim Kunden erzeugen und die eigene ISMS-Erfahrungen teilen

AWS ist nicht verpflichtet, Konzernformulare zu nutzen und bahninterne Handlungs-anweisungen zu kennen.

Kunden, die jetzt selbst Infrastrukturbetreiber werden, haben den Bedarf die neuen Aufgaben und Tätigkeiten vermittelt und erklärt zu bekommen.

Der Kunde muss nun selbst

- die Sicherheitseigenschaften der (eigenen, virtuellen) Infrastruktur deklarieren;
- die Risiken seiner Infrastruktur analysieren, formal dokumentieren und managen.

Konzerninterne Sicherheitsprozesse und –regelungen gelten nicht bei AWS.

DB Systel begleitet und unterstütz seine Kunden auf ihrem Weg, die Informationssicherheit selbst zu steuern und zu verwalten.

Agenda

1. Wolkenbildung
2. Heiter bis wolkig
3. **Wolkenkuckucksheim**

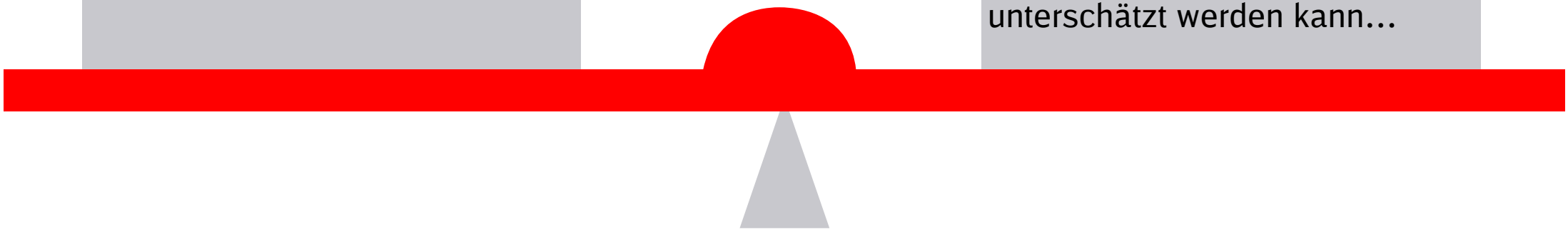
AWS nimmt IT-Security sehr ernst… und beherrscht das Thema

- Zahlreiche einschlägige Zertifizierungen Availability Zones sowie der Rechenzentren
- Regelmäßige Re-Zertifizierung
- Einblick in die Prüfberichte (gegen Unterzeichnung eines NDA)
- Automatisches Logging und Speicherung in AWS Buckets
- Service „Inspector“ in Vorbereitung (Hinterlegung eines maßgeschneiderten Policy-Frameworks; Prüfung auf Regelverstöße alle 15 Min.

Die Cloud kann aus Sicht der Datensicherheit ein Segen sein – es lassen sich (operative) Risiken auslagern.

Durch den Rückbau dezentraler „Serverzentren“ und deren Migration in die Cloud wird sich die Sicherheit und die Sichtbarkeit (z.B. für CIOs) erhöhen. Die Cloud bietet für den Besteller Chancen, durch „selber-machen“ seine IT agiler, direkter und kostengünstiger zu gestalten.

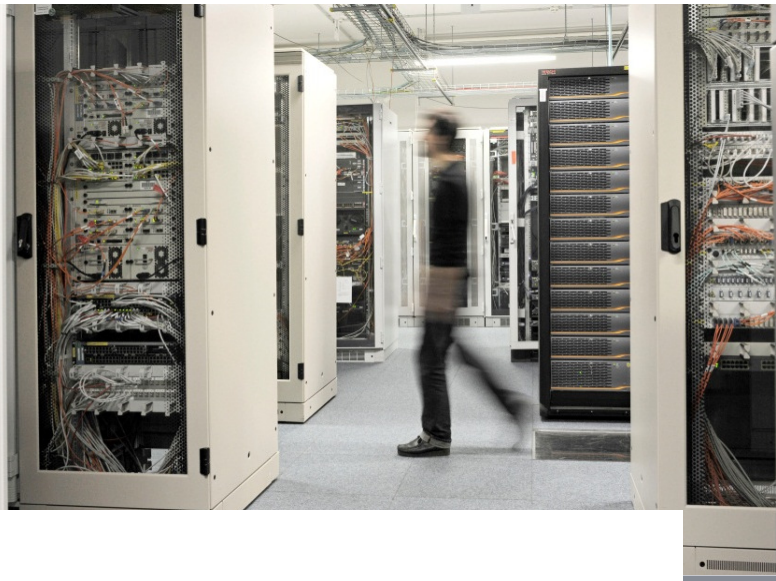
Die Agilität findet im engen Portfolio seine Grenzen, das direkte Wirken ist eingeschränkt und nur virtuell über Services möglich und eine angemessene Informationssicherheit will kontinuierlich überdacht, geplant, gesteuert, umgesetzt und kontrolliert sein. „Selber-machen“ erzeugt Aufwand, der unterschätzt werden kann…



Die Cloud kann aus Sicht des Datenschutz ein Fluch sein – nationale Gesetze wirken nicht (überall) in der Cloud.

- Grundlage des Enterprise Agreement war ein ADV-Vertrag sowie das Safe-Harbor-Abkommen.
- Mit der Entscheidung des EuGH vom 06.10.15 wurde das Abkommen für ungültig erklärt (Az: C-362/14)
- Grundlage derzeit sind b.a.w. die Standardvertragsklauseln der EU.
- Die Cloud-Services von AWS werden vertragsgemäß ausschließlich in der AZ Frankfurt erbracht.

Fotos: Max Lautenschläger, DB Systel (l.)



Vielen Dank für Ihre Aufmerksamkeit!

Stefan Hirschberg

IT Security Management
I.LVE 1(1)

Tel. 069 265-18125

stefan.hirschberg@deutschebahn.com

DB Systel GmbH
Jürgen-Ponto-Platz 1
60329 Frankfurt am Main
www.dbsystel.de