Anforderungen an Datenschutz und Sicherheit von Cloud-Dienstleistungen

Forum Kommune21 auf der DiKOM Süd
4. Mai 2011, Frankfurt

Marit Hansen
Stellvertretende Landesbeauftragte für Datenschutz
Schleswig-Holstein

Überblick

- **Cloud Computing –**
  geringere Kosten und sogar mehr Sicherheit?
- **Sicherheit bei Cloud Computing:**
  Risiken und ihre Behandlung
- **Für personenbezogene Daten: der Blick ins Gesetz**
- **Fazit**

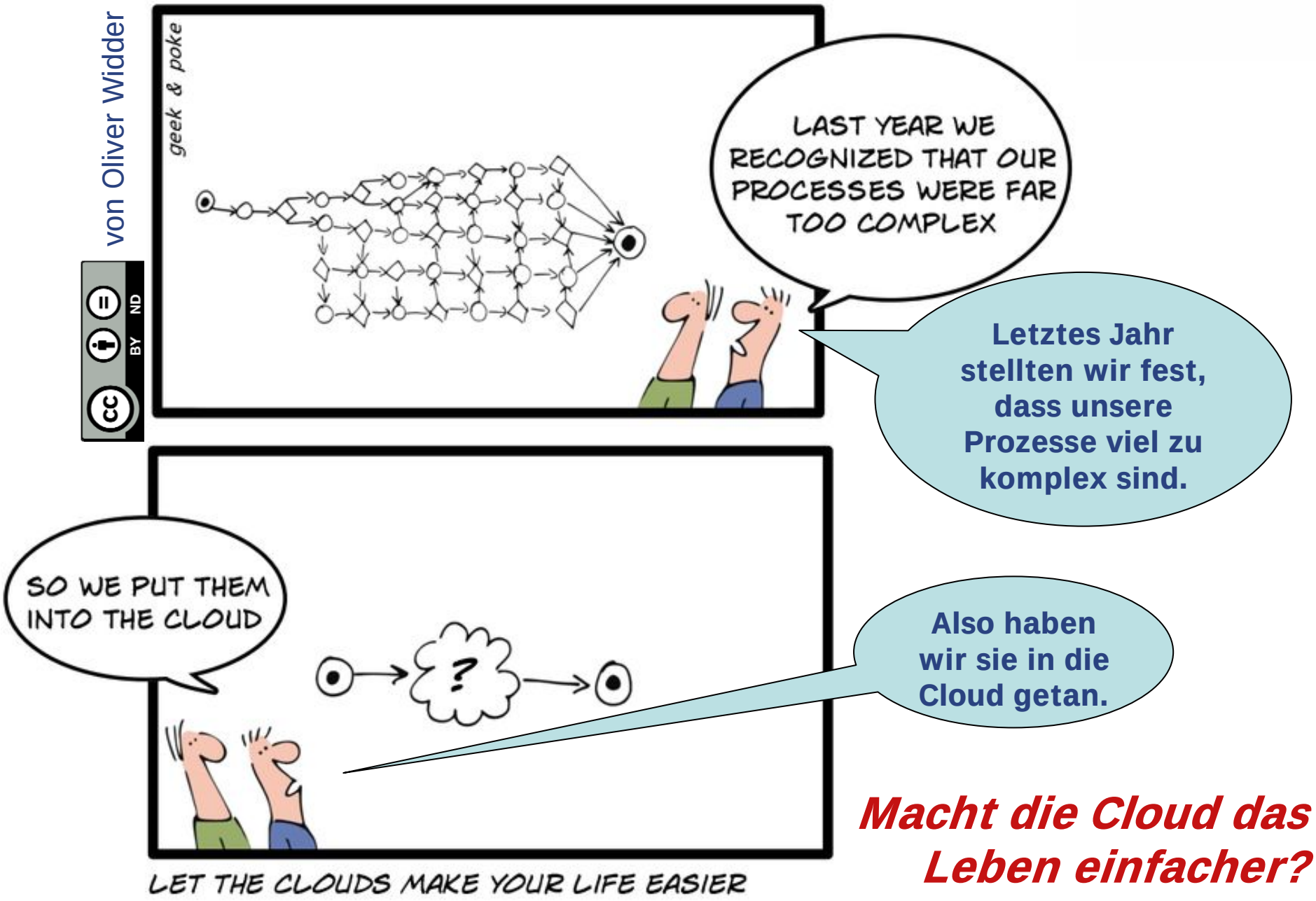
Grundlegende Design-Prinzipien von Cloud Computing

Cloud Computing:

- Ein oder mehrere Anbieter bieten die **bedarfsgerechte Nutzung** von Informationstechnik (Infrastruktur, Plattform oder Software) über ein Netz an – häufig geringere Kosten als bei eigener Realisierung

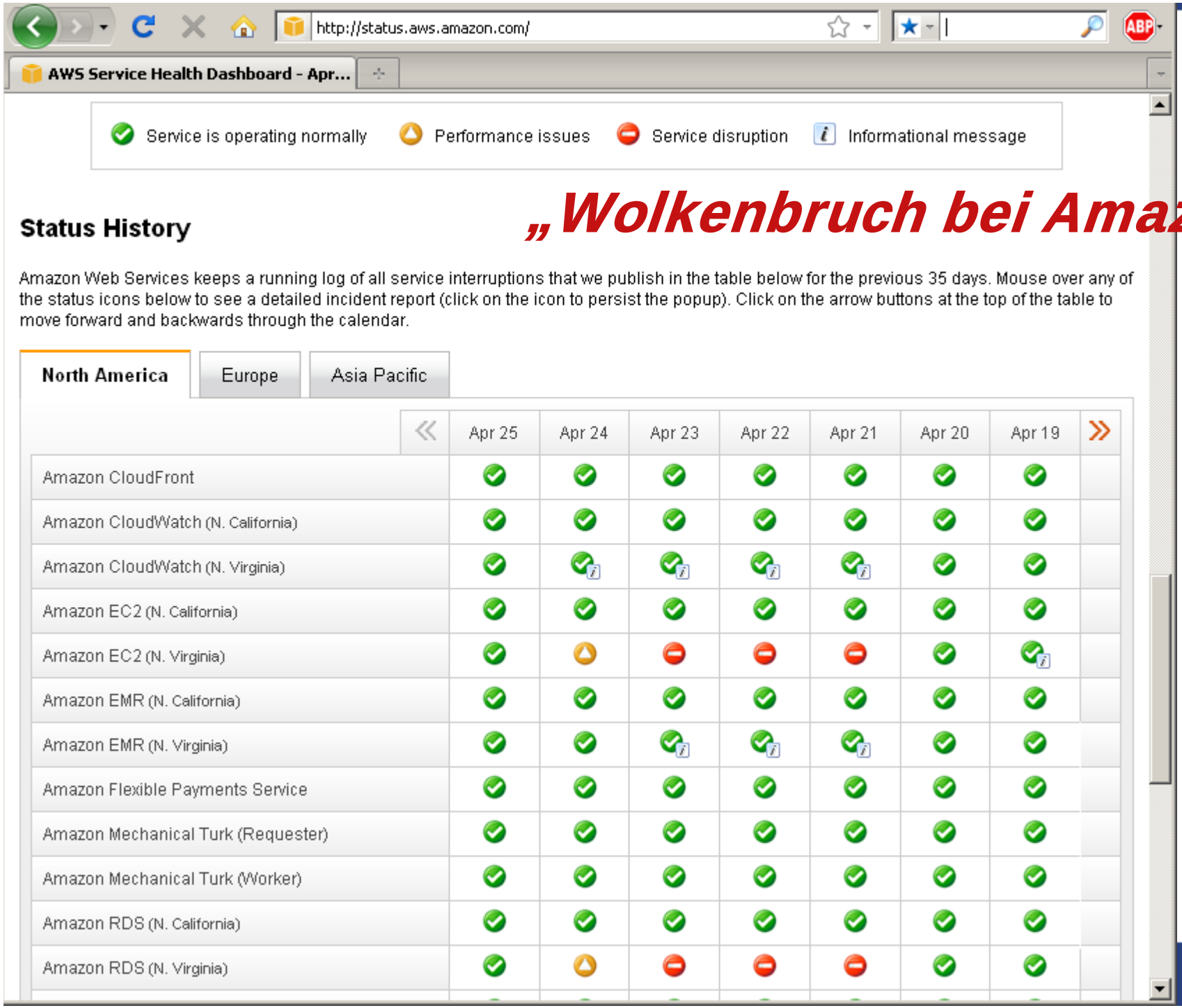
- **Elastizität**: dynamische Anpassung an Ressourcenbedarf – dafür dynamische Zuordnung der Ressourcen

- Abstraktion von realer, physikalischer Infrastruktur bedeutet **Loslösung von Hardware oder Liegenschaften**



von Oliver Widder

Macht die Cloud das Leben einfacher?



„Wolkenbruch bei Amazon“

Discussion Forums

Life of our patients is at stake - I am desperately asking you to contact

Reply

Posted by: [redacted]
Posted on: Apr 22, 2011 11:20 PM

This question is **answered**. Helpful answers available: **2**. Correct answers available: **1**.

Sorry, I could not get through in any other way

We are a monitoring company and are monitoring hundreds of cardiac patients at home.
We were unable to see their ECG signals since 21st of April

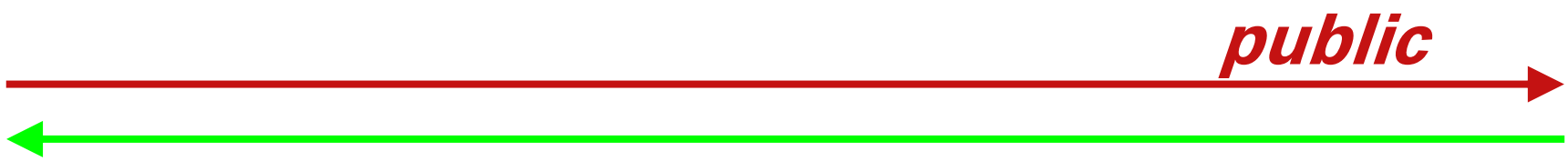
Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

i-bb5c0fd0
i-8e6163e5
i-6589720f

Or please let me know how can I contact you more ditectly.
Thank you

Sicherheit bei Cloud Computing: Risiken und ihre Behandlung

Wie „public“ ist die Cloud?



Private Cloud

Public Cloud

„Öffentlicher Dienst“-Cloud in Deutschland?

Hybrid Cloud

Community Cloud

Cloud Computing: Verlust der Ortsgebundenheit

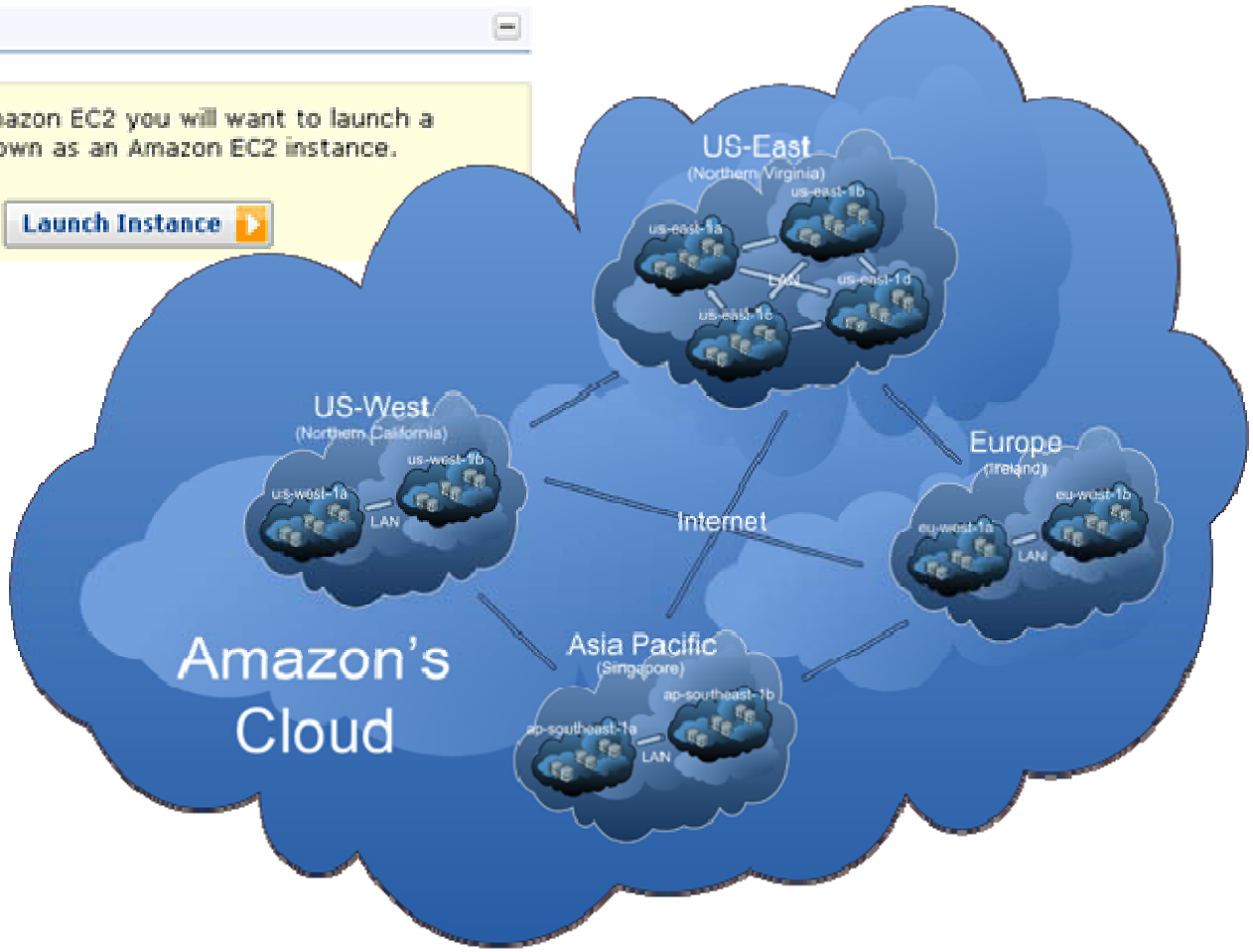
Problem:

- Technisch sind territoriale Grenzen unerheblich
- Aber: (Datenschutz-)Recht ist ortsgebunden
- Einschätzung „ausreichendes Datenschutzniveau“ abhängig vom Ort

Risikobehandlung:

- Für jede Datenverarbeitung Ort oder zumindest anwendbares Datenschutzrecht feststellbar machen
- Vgl. Partitionierung der Amazon-Cloud: **Regionalgarantie**

Beispiel Regionalgarantie

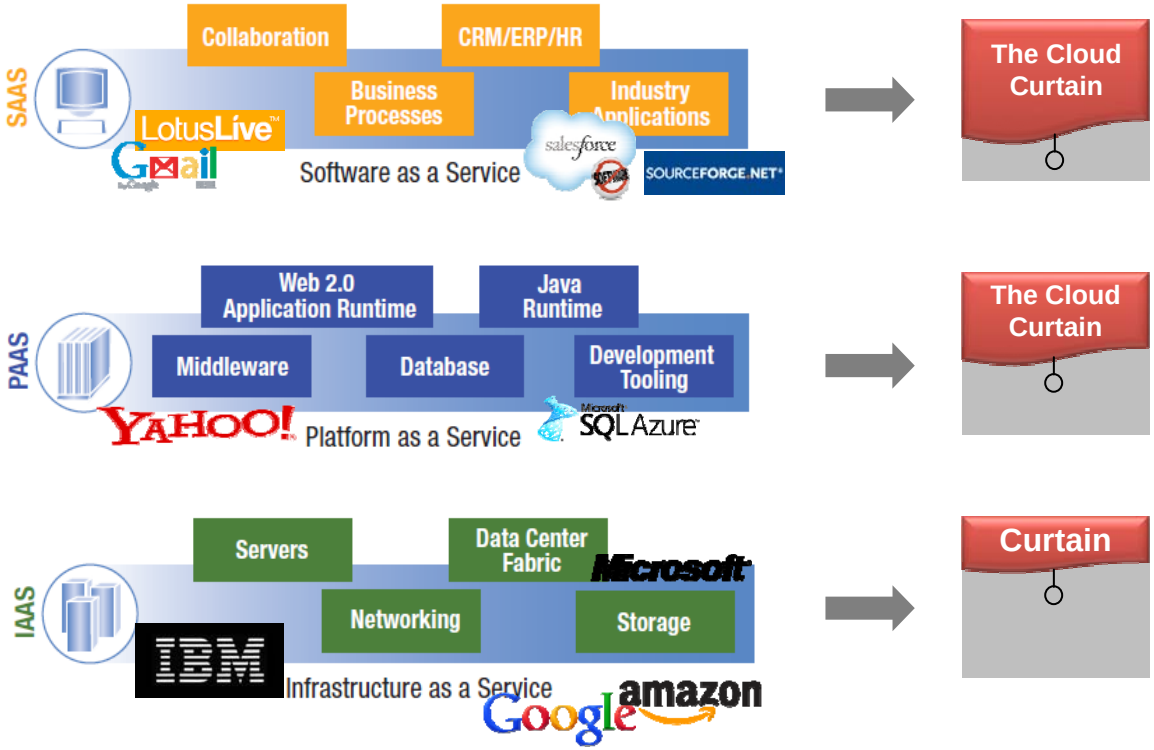


http://www.automatedqa.com/techpapers/testcomplete/cloud-testing-using-different-regions/

Fehlende Transparenz

Problem:

- „Cloud-Vorhang“ („Cloud Curtain“): technische Funktion der Cloud-Services wird vor dem Anwender verborgen
- Anwender können dann das Risiko nicht einschätzen



„... eine gewisse Wurstigkeit ...“

Lebenserleichternde Apps

Packen Sie Ihren Krempel in die Wolke!

Von Tom Hillenbrand

...

Nicht nur Watson liest mit: Wer Angst hat, dass andere mitlesen, für den ist die Web-Wolke nichts. Wer Hunderte Megabytes Daten auf diversen Servern auf der ganzen Welt speichert, muss eine gewisse Wurstigkeit an den Tag legen. Denn ganz sicher lesen da welche mit.

Das sollte man sich klarmachen, bevor man seine Daten in die Wolke kippt: "Wenn es etwas gibt, von dem du nicht willst, dass es jemand weiss, solltest du es vielleicht gar

Unbekannte (ggf. legale) Zugriffe Dritter

Problem:

- Zugriff durch Aufsichts- und Ermittlungsbehörden in Drittländern häufig ohne Information der Betroffenen
  - „Innere Sicherheit++“: Polizei, Verfassungsschutz, Finanzbehörden ...
  - Rechteinhaber: Musikindustrie ...
  - Wirtschaftsspionage: Geheimdienste
- „Indecency-Check“: Entfernen/Blockieren von (als anstößig eingestuften) Inhalten

Risikobehandlung:

- Kryptographie: verschlüsselte Datenspeicherung, verschlüsselte Datenübertragung

Rückstandsfreies Löschen nicht garantiert

Problem:

- In vielen Betriebsmodellen:
  sicheres **Löschen** nicht möglich

Risikobehandlung (Ansätze):

- Keine sensitive Daten in eine Public Cloud
- Kryptographie hilft ...

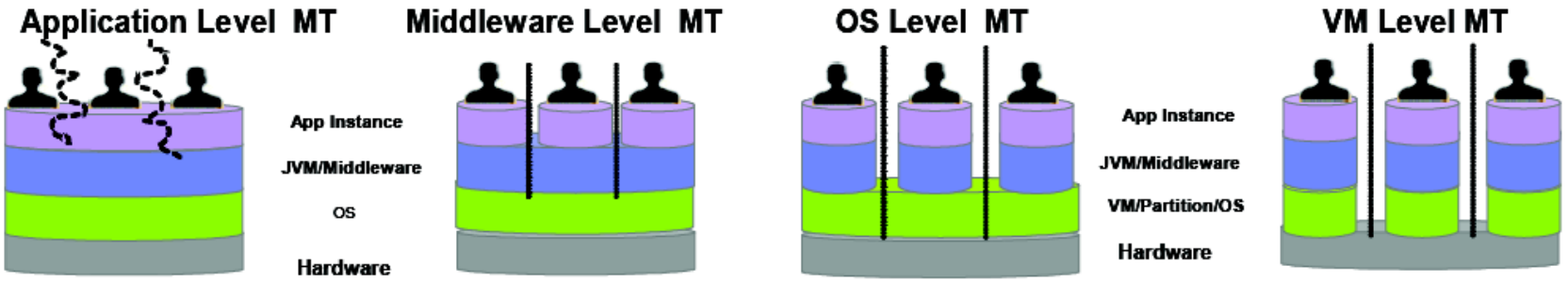
Mangelhafte Datentrennung

Problem:

- Möglicher Datenfluss zwischen eigentlich zu trennenden Anwendern
- Möglicher Einfluss von Sicherheitsproblemen bei einem Anwender auf andere Anwender

Risikobehandlung:

- (Nachvollziehbare!) Produktzertifizierungen

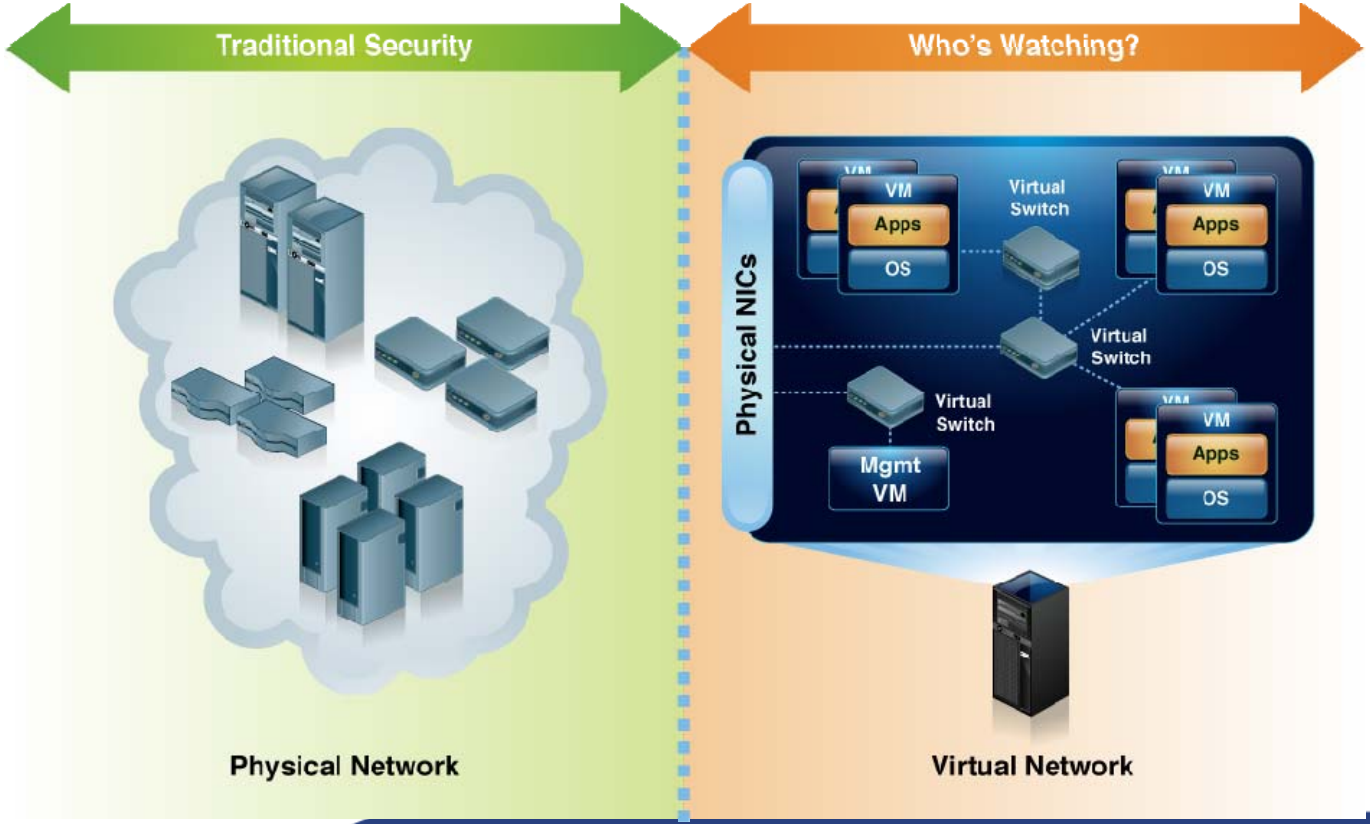


Verschiedene Ebenen der Mandantenfähigkeit

Der Cloud-Anbieter als Angreifer

Problem:

- Missbrauch durch Cloud-Anbieter / -Admins
- Weitgehende Zugriffsrechte der Cloud-Admins



Der Cloud-Anbieter als Angreifer

- Datentransport und -speicherung sind durch Krypto-verfahren mit nutzerseitig erzeugten und kontrollierten Schlüsseln lösbar

Problem: Datenverarbeitung:

- Aktuell nicht technisch ausreichend abzusichern
- Restrisiko bleibt, im Fall einer Risiko-Übernahme entsprechende Dokumentation nötig
- Status: nicht tragbar für Daten, die einem Berufs- oder Amtsgeheimnis unterliegen

Gegenmaßnahmen:

- In Arbeit: Wiederauferstehung von Trusted Computing?
- Feingranulare, temporär beschränkte Zugriffsrechte

Für personenbezogene Daten:

der Blick ins Gesetz

Datenschutzrecht in Deutschland / Europa

- In Deutschland z.B. Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG)
- Auf EU-Ebene harmonisiert
- Territorialprinzip
- **Grundregel:** Verarbeitung personenbezogener Daten nur bei Rechtsgrundlage oder Einwilligung der Betroffenen

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrun
5. die nach Absatz 4 bestehenden Pflic e die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begr
7. die Kontrollrechte des Auftragg Mitwirkungspflichten des Auftra
8. mitzuteilende Verstöße des Auft gegen Vorschriften zum Schutz p getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnis die Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datentr und gespeicherter Daten nach Beendigun Auft

Er kann bei öffentlichen Stellen auch dur Fachaufsicht erfolgen. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig in geeigneter Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,
2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Auftrags-datenverarbeitung

Siehe § 11 BDSG;
ähnlich in LDSG

Wichtig:

Der Auftraggeber bleibt verantwortlich!

Auftrags-DV (§ 11 BDSG)

- **Sorgfältige Auswahl** von (Unter-)Auftragnehmern (AN) durch Auftraggeber (AG)
- **Schriftlicher Auftrag** mit Benennung von
  - Gegenstand,
  - Dauer,
  - Umfang, Art, Zweck, Betroffene,
  - Datenkorrektur,
  - techn.-org. Maßnahmen,
  - Dienstleister, Kontrollen, Weisungen, Vertragsstrafen,
  - abschließender rückstandsfreier Datenlöschung

Auftrags-DV (§ 11 BDSG) – Fortsetzung

- **Erkennbarkeit** des verarbeitenden AN für AG
- **Techn.-org. Maßnahmen**: Benennung der konkreten Instrumente
- **Meldepflichten** des AN bei Sicherheitsverstößen
- Notwendige **Kontrollen** durch AN
- **Auskunfts-/Kontrollrechte** des AG
- Haftungsregeln
- Vorgehen bei Insolvenz oder Übernahme
- **Volle Datenschutzkontrolle** nach § 38 BDSG muss möglich sein

Datenverarbeitung außerhalb EU

- Verarbeitung personenbezogener Daten außerhalb EU/EWR-Raum ist generell **unzulässig**

- **Ausnahmemöglichkeit** bei festgestellter Angemessenheit des DS-Niveaus (§ 4b II 2, 3 BDSG)

- Safe-Harbor-Selbstzertifizierung von US-Unternehmen genügt nicht

- **EU-Standardvertragsklauseln** zur Auftragsdatenverarbeitung (Art. 26 II EU-DSRL)
- Analog **Binding Corporate Rules** (BCRs)

Mangelhafte Kontrolle von Auftrags-DV

Problem:

- Anwender bestimmen einen Großteil der Sicherheitsmaßnahmen nicht mehr selbst
- Nachvollziehbarkeit von Sicherheitsmaßnahmen häufig nicht gegeben
- Fehlendes Kontrollmodell

Risikobehandlung:

- Sicherheitsmaßnahmen und –zusagen vertraglich festlegen
- Zertifizierungen und Audits (ISO 27001, EuroPriSe)

Fazit

Fazit

- Sicherheitsanforderung:
  die Kontrolle über die eigenen Daten behalten
- Dazu die Risiken kennen und bewusst behandeln
- Mechanismen:
  - Vertraglich: Auftragsdatenverarbeitung
  - Technisch: z.B. Verschlüsselung unter der eigenen Kontrolle umsetzen

⇒ Datenschutz- & Sicherheitsanforderungen werden von vielen Angeboten noch nicht erfüllt

Vielen Dank für Ihre Aufmerksamkeit!

Unabhängiges Landeszentrum für Datenschutz
Marit Hansen
Holstenstraße 98
24103 Kiel

Tel.: 0431/988-1214
E-Mail: ULD6@datenschutzzentrum.de

Die Folien sind eine Co-Produktion von Sven Thomsen (ULD), Marit Hansen (ULD) und TClouds/Elmar Husmann (IBM).

TClouds

http://www.tclouds-project.eu/