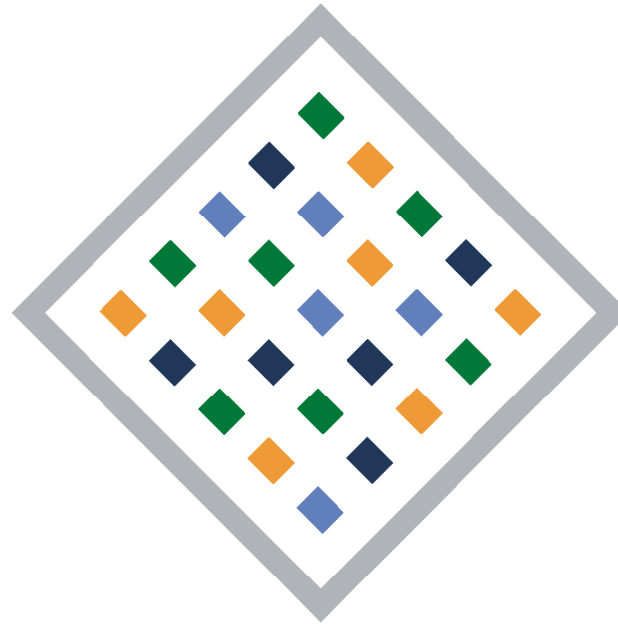


IT-Sicherheitstag 2011

Cloud-Computing und Datenschutz



Gabriel Schulz
Stellvertreter
des Landesbeauftragten für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern



Datenschutzrisiken bei Cloud-Computing

Agenda

- Einführung in das Thema
- Betriebsmodelle und Typen
- Anwendbarkeit von Datenschutzrecht
- Datenschutzrechtliche Verantwortlichkeit
- Forderungen und Empfehlungen





Einführung





Top-Thema der CeBIT 2011

"Work and Life with the Cloud"

- „Cloud Computing wird aktuell so intensiv diskutiert wie kein IT-Thema“
- „Cloud Computing hat Fahrt aufgenommen“
- „Cloud Computing wächst um 16.6 Prozent“
- „Cloud Computing wird die gesamte IT-Welt revolutionieren“

- **Cloud Computing: Ein Datenschutzthema !!**





Das Online-Karriere-Portal Monster als Cloud-Betreiber

Auszug aus den Nutzungsbedingungen

- Alle Inhalte (Designs, Texte, Grafiken, Bilder, Videos, Informationen, Logos, Schaltflächen, Software, Audiodateien und andere Inhalte von Monster) sind **Eigentum von Monster** oder seinen Lizenznehmern.
- Durch das Einreichen, die Veröffentlichung oder die Darstellung von Nutzerinhalten auf oder durch Monster, gewähren Sie Monster das weltweite, nicht exklusive und kostenfreie Recht, diese **Nutzerinhalte** zu reproduzieren, **anzupassen**, zu **verbreiten** und zu **veröffentlichen**.
- Nachdem dieser Nutzerinhalt von der Webseite von Monster entfernt wurde, wird Monster die Nutzung innerhalb eines **wirtschaftlich sinnvollen Zeitraums** einstellen.





Zugriffsbefugnisse gemäß PATRIOT Act

Heise online 30. Juni 2011:

Amazon, Google und Microsoft unterliegen dem
PATRIOT Act:

US-Sicherheits-Behörden dürfen sogar auf
europäische Cloud-Daten zugreifen!



Wie vertrauenswürdig ist Cloud-Computing?





Begriffsdefinition

Cloud Computing:

Von Cloud Computing wird dann gesprochen, wenn eine oder mehrere Dienstleistungen (Infrastruktur, Plattform, Anwendungssoftware) aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Nutzung abrechenbar über ein Netz bereitgestellt werden. *

* Alex D. Essoh (BSI): Cloud Computing und Sicherheit – Geht denn das?





Betriebsmodelle Cloud Computing

Privat Cloud

- Dienste innerhalb einer Institution angeboten
- Cloud-Anbieter und -Anwender sind identisch

Public Cloud

- für jedermann verfügbar
- am freien Markt angeboten
- beliebige Zahl von Anwendern

Hybrid Cloud

- Mischung aus Public- und Privat Cloud
- sinnvoll zur Lastverteilung

Community Cloud

- mehrere Cloud-Anbieter bieten Cloud-Services einem definierten Kundenkreis an





Typen des Cloud Computing

IaaS

Infrastruktur
as a Service

Anwender nutzen
virtualisierte
Komponenten und
nutzen eigene
Betriebssysteme
und Programme

PaaS

Platform
as a Service

Anwender nutzen
eigene Programme
auf der vom
Dienstleister
bereitgestellten
Infrastruktur

SaaS

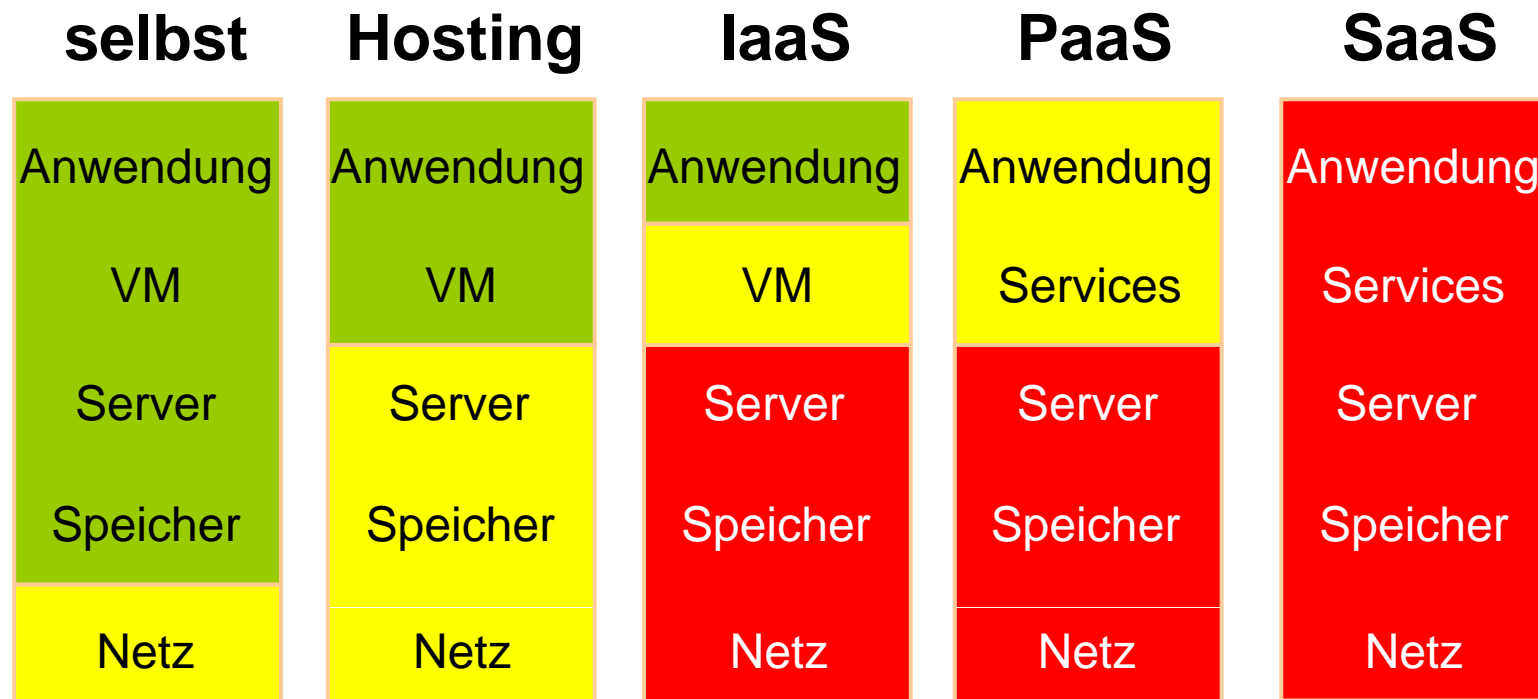
Software
as a Service

Anwender nutzen
vom Dienstleister
bereitgestellte
Programme meist
über Web-Browser
(Thin Clients)





Kontrolle über die Ressourcen



Abnahme der Kontrollmöglichkeit



Nutzer hat Kontrolle

geteilte Kontrolle

Anbieter hat Kontrolle

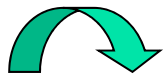
Quelle: Tim Mather „Cloud Security and Privacy“





Vorteile und Chancen

- Flexibilität bei der Buchung, Nutzung und Stilllegung von Ressourcen
- extrem gute Verwaltung der Ressourcen (Skalierbarkeit)
- einfacher Erwerb
- verbrauchsabhängige Bezahlung
- Einsparpotenzial bei Anschaffung, Betrieb und Wartung von IT-Systemen
- Verfügbarkeit von Geschäftsanwendungen unabhängig vom geographischen Standort



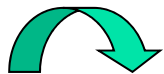
im Wesentlichen wirtschaftliche Aspekte





Nachteile und Risiken

- keine eindeutige Rechtslage
- oftmals unklare Vertragslage
- keine eindeutigen Haftungsregelungen
- ggf. unzulässige Übermittlung von Daten außerhalb der EU
- unternehmensweite IT-Compliance nicht realisierbar
- Sicherheit und Verfügbarkeit von Cloud-Systemen schwer bewertbar
- Betriebs- und Sicherheitskonzepte werden nicht offengelegt
- Standort der Rechenzentren und Speicherort der Daten ist unbekannt
- keine ortsbezogene Datenverarbeitung
- Anbieter von Cloud-Systemen sind an Transparenz nicht interessiert
- Flexibilität und Skalierbarkeit bedingen eine gewisse Intransparenz



zahlreiche rechtlichen Fragestellungen





Betroffene Rechtsbereiche

- Haftung, Gewährleistung
- Urheberrecht
- Steuer- und Handelsrecht (Stichwort Revisionsfähigkeit)
- Verbraucherrecht, AGB-Recht
- Strafprozessrecht
- Sicherheitsrecht
- IT-Vertragsrecht
- **Datenschutzrecht**





Datenschutzrecht





Verfassung Mecklenburg-Vorpommern

Artikel 6 Absatz 1

Jeder hat das Recht auf Schutz seiner personenbezogenen Daten.

Dieses Recht findet seine Grenzen in den Rechten Dritter und in den überwiegenden Interessen der Allgemeinheit.





Personenbezogene Daten

§ 3 Abs. 1 DSGVO M-V

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

§ 3 Abs. 1 BDSG

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).



Cloud Computing ist nur dann datenschutzrelevant, wenn personenbezogene Daten verarbeitet werden.





Wer ist verantwortlich?





Verantwortung für die Datenverarbeitung in der Cloud

Das europäische und deutsche Datenschutzrecht knüpft die **rechtliche Verantwortlichkeit** für die Datenverarbeitung personenbezogener Daten an die **inhaltliche Verantwortlichkeit** über die Entscheidung des Umgangs mit den Daten.



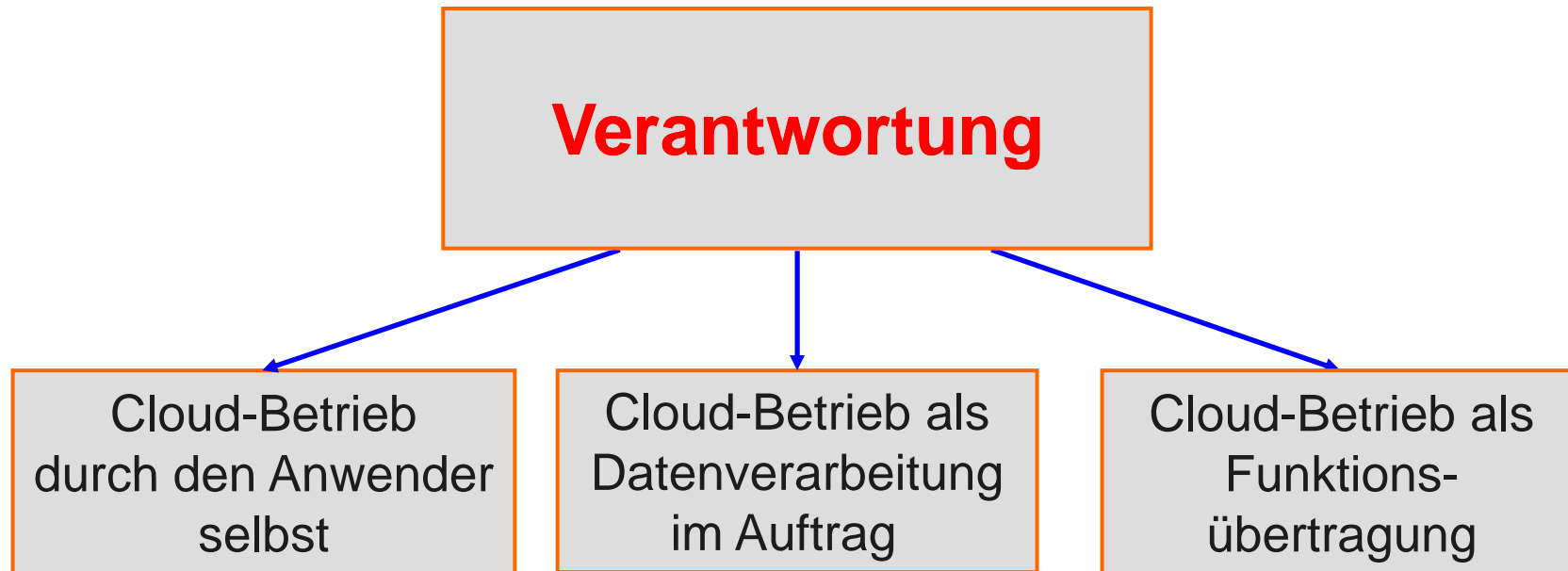
Wer ist verantwortliche Stelle* ?

- *) § 3 Abs. 7 BDSG: Verantwortliche Stelle ist jede Person, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere vornehmen lässt.
- *) Art. 2d EU-DS-RL: Verantwortlich ist, wer über Zwecke und Mittel der Datenverarbeitung entscheidet.





Verantwortung für die Datenverarbeitung in der Cloud





Verantwortung für die Datenverarbeitung in der Cloud

(Cloud-)Betrieb durch den Anwender selbst

- alleinige Verantwortung beim Cloud-Anwender, der gleichzeitig Cloud-Anbieter ist
- Adressat von
 - Verfügungen der Aufsichtsbehörde
 - Betroffenenansprüchen (Auskunft, Löschung usw.)
 - Schadensersatzansprüchen
 - Bußgeldsanktionenist allein der Cloud-Anwender (Privat Cloud)



Datenschutzrechtlich unproblematisch





Verantwortung für die Datenverarbeitung in der Cloud

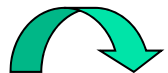
Cloud-Betrieb als Datenverarbeitung im Auftrag

Zulässigkeitsvoraussetzung:

- Auftragnehmer müssen Personen oder Stellen
 - im Inland oder
 - in einem Mitgliedsstaat der Europäischen Union (EU) oder
 - in einem Mitgliedsstaat des Europäischen Wirtschaftsraums (EWR) sein (vgl. § 3 Abs. 8 BDSG)

Auftragnehmer:

- Bestimmungen des § 11 BDSG (Datenverarbeitung im Auftrag) gelten



Datenschutzrechtlich schwierig





Verantwortung für die Datenverarbeitung in der Cloud

Cloud-Betrieb als Datenverarbeitung im Auftrag

Grundsatz:

- der Auftraggeber bleibt für die Einhaltung der Datenschutzvorschriften verantwortlich

Pflichten Auftraggeber:

- der Auftragnehmer muss unter Berücksichtigung der Eignung für die Gewährleistung der technischen und organisatorischen Maßnahmen ausgewählt werden
- der Auftrag ist schriftlich zu erteilen

Pflichten Auftragnehmer:

- Daten dürfen nur nach Weisung des Auftragnehmers verarbeitet werden
- der Auftraggeber ist auf datenschutzwidrige Weisungen hinzuweisen





Verantwortung für die Datenverarbeitung in der Cloud

Im Auftrag ist detailliert festzulegen (vgl. § 11 Abs. 2 BDSG):

- Gegenstand und Dauer des Auftrags
- Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung von Daten
- Kreis der Betroffenen
- Technische und organisatorische Maßnahmen nach § 9 BDSG
- Berichtigung, Sperrung und Löschung von Daten
- Pflichten des Auftragnehmers und dessen Kontrollen
- Unterauftragsverhältnisse
- Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers
- Mitzuteilende Verstöße des Auftragnehmers gegen Datenschutzvorschriften
- Umfang der Weisungsbefugnisse des Auftraggebers
- Rückgabe von Datenträgern bzw. Löschung von Daten nach Auftragsbeendigung





Verantwortung für die Datenverarbeitung in der Cloud

Kontroll- und Dokumentationspflicht nach BDSG:

Der Auftraggeber hat sich **vor Beginn der Datenverarbeitung und sodann regelmäßig** von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Das Ergebnis ist schriftlich zu dokumentieren.





Verantwortung für die Datenverarbeitung in der Cloud

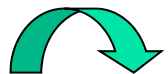
Cloud-Betrieb als Funktionsübertragung

DV im Auftrag nicht zulässig, wenn:

- Auftragnehmer **Dritter** im Sinne des BDSG ist (§ 3 Abs. 8 S. 2), insbesondere
 - jede Stelle außerhalb der Europäischen Union (EU) oder
 - außerhalb des Europäischen Wirtschaftsraums (EWR)

Folge:

- Bestimmungen des § 11 BDSG sind nicht anwendbar
- Rechtliche Voraussetzungen für eine **Datenübermittlung** müssen gegeben sein (bspw. §§ 4b, 4c BDSG) – Stichwort „angemessenes Datenschutzniveau“



Datenschutzrechtlich kaum lösbar





Verantwortung für die Datenverarbeitung in der Cloud

Zulässigkeit der Datenübermittlung (in die Cloud)

Vertrag (§ 28 Abs. 1 Nr. 1 BDSG):

- Übermittlung muss zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich sein (Vertrag kann sich auf Cloud-Verarbeitung erstrecken)
aber:
 - Wer hat schon solche Verträge mit Betroffenen?

Erforderlichkeit (§ 28 Abs. 1 Nr. 2 BDSG):

- Übermittlung muss zur Wahrung berechtigter Interessen des Cloud-Nutzers **erforderlich** sein und Interessen des Betroffenen dürfen nicht überwiegen
aber:
 - Wann ist die Verarbeitung außerhalb der EU / des EWR erforderlich?
 - Wie können die Interessen der Betroffenen gesichert werden?





Zwischenfazit





Cloud-Betrieb für die öffentliche Verwaltung

- derzeit wohl nur in der Privat Cloud zulässig

Cloud-Betrieb als Datenverarbeitung im Auftrag

- rechtlich grundsätzlich zulässig
- Kreis der möglichen Auftragnehmer ist jedoch stark eingeschränkt
- Pflichten des Auftraggebers praktisch kaum wahrnehmbar
- grenzüberschreitende Kontrollen sind schon im EU-Raum faktisch unrealistisch

Cloud-Betrieb als Funktionsübertragung (Übermittlung)

- außerhalb der EU und des EWR-Raums sehr problematisch
- rechtlich allenfalls denkbar durch Vertrag mit Betroffenenem
- Schutz der Betroffenenrechte praktisch nicht realisierbar
- grenzüberschreitende Kontrollen sind hier erst recht unrealistisch





Forderungen und Empfehlungen

DATENSCHUTZ UND



INFORMATIONSFREIHEIT



Forderungen und Empfehlungen

Schutzziele gemäß § 21 Abs. 2 DSGVO M-V

Vertraulichkeit

Kenntnisnahme
der Daten nur
durch Befugte

Verfügbarkeit

Daten müssen
in angemessener
Zeit zur
Verfügung stehen

Integrität

Daten müssen
unversehrt,
vollständig und
aktuell sein

Transparenz

Verarbeitung
von Daten
muss vollständig
nachvollziehbar
sein





Forderungen und Empfehlungen

§ 9 BDSG: technische und organisatorische Maßnahmen

- Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG einzuhalten
- erforderlich sind Maßnahmen, wenn ihr Aufwand im angemessenen Verhältnis zum Schutzzweck stehen
- Details hierzu in der Anlage zu § 9 BDSG





Forderungen und Empfehlungen

Informationssicherheit beim Cloud-Nutzer

- Management von Risiken, die mit der Auslagerung von Geschäftsprozessen einhergehen (Risiken identifizieren und behandeln)
- Etablierung eines Informationssicherheitsmanagement-Systems nach BSI-Standard 100-1
- eigenes Sicherheitskonzept gemäß BSI-Standards 100-2 und 100-3
- Abstimmung des Sicherheitskonzeptes mit dem des Cloud-Anbieters
- Risikoanalyse insbesondere in Bezug auf
 - Webservice-Sicherheitsstandards
 - Sicherheit von Web-Anwendungen
 - Authentifizierungsverfahren
 - Verschlüsselung bei der Übertragung und ggf. Speicherung
 - Malware





Forderungen und Empfehlungen

Informationssicherheit beim Cloud-Anbieter

- vollständige Transparenz der Cloud gegenüber dem Cloud-Nutzer
- Etablierung eines Informationssicherheitsmanagement-Systems nach BSI-Standard 100-1
- Sicherheitskonzept gemäß BSI-Standards 100-2 und 100-3
- Abstimmung des Sicherheitskonzeptes mit dem des Cloud-Nutzers
- Ereignismanagement (z. B. gemäß BSI-Baustein 1.8 - Behandlung von Sicherheitsvorfällen)
- Datenschutzstandards durch Erarbeitung von Protection Profiles
- transparente Auditierung (Zertifizierung nach Common Criteria, ISO 27001, FISMA-Zertifikat, SAS-70-Typ II-Zertifikat, Gütesiegel der künftigen Stiftung Datenschutz dem. § 9a BDSG oder des ULD S-H)





Forderungen und Empfehlungen

Informationssicherheit beim Cloud-Anbieter

- Sicherheit auf allen Schichten des virtuellen Systems
 - Schicht 1: Host-System
 - Schicht 2: Virtualisierungsschicht
 - Schicht 3: Gast-Betriebssystem
 - Schicht 4: Anwendung





Forderungen und Empfehlungen

Klare Regelung der Zugriffsrechte

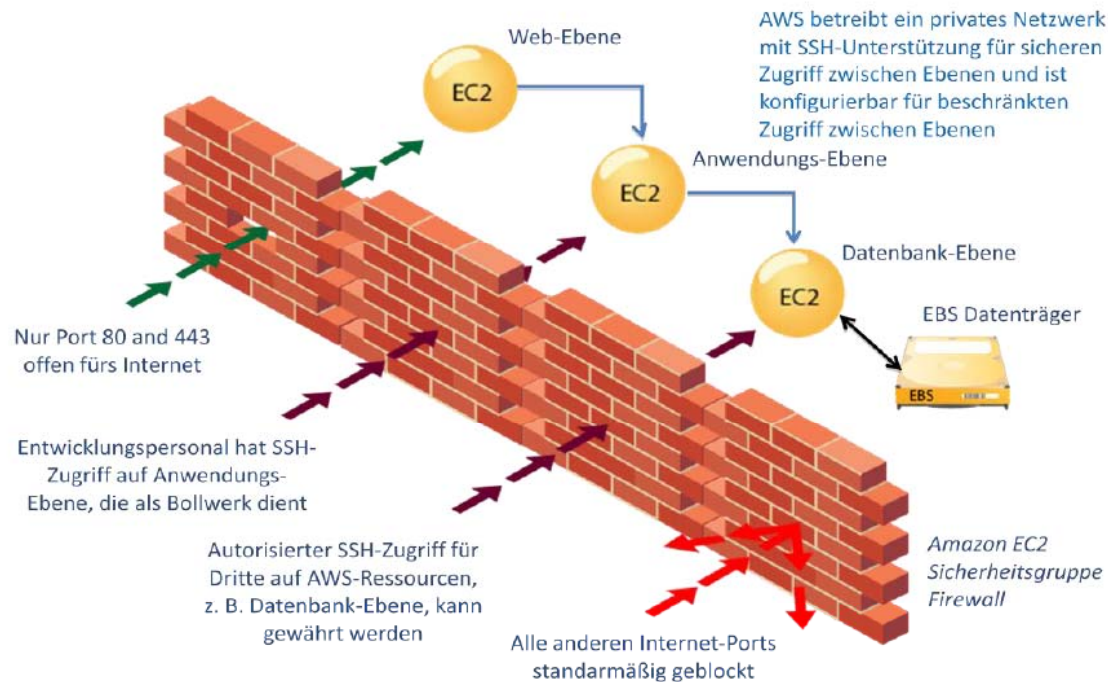
- Abschottung der einzelnen Auftragsverhältnisse (Cloud-Nutzer-Bereiche)
- differenziertes Zugriffsrechte-System insbesondere beim Einsatz von Virtualisierungstechniken
 - welcher Nutzer verwaltet welche virtuelle Maschine
 - welche Dateiberechtigungen werden in virtuellen Maschinen eingerichtet
 - welche Rechte sind für das Gastbetriebssystem erforderlich





Forderungen und Empfehlungen

Regelung der Zugriffsrechte: z. B. Amazon EC2



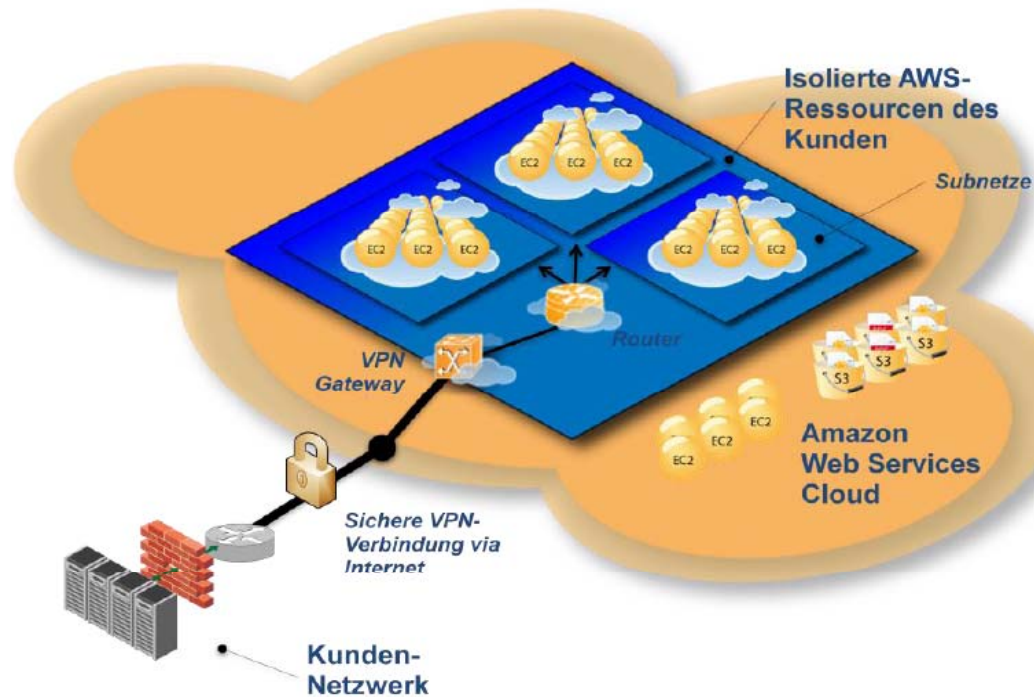
Quelle: Sicherheitsprozesse bei Amazon Web-Services Elastic Compute Cloud - EC2 (<http://aws.amazon.com/sicherheit>)





Forderungen und Empfehlungen

Abschottung der Nutzerbereiche: z. B. Amazon EC2



Quelle: Sicherheitsprozesse
bei Amazon Web-Services
Elastic Compute Cloud - EC2
(<http://aws.amazon.com/sicherheit>)





Forderungen und Empfehlungen

Außereuropäische Clouds

- Datenübermittlung außerhalb des EU/EWR-Raums unzulässig, es sei denn, ein angemessenes Datenschutzniveau existiert (§ 4b Abs. 2, 3 BDSG)
- gilt bspw. für die Schweiz, Kanada oder Argentinien
- bei Datentransfer an Drittstaaten können die Standardvertragsklauseln nach der Richtlinie 95/46/EG vom 05.02.2010 greifen (Cloud-Anwender ist dann verantwortliche Stelle und Datenexporteur, der Cloud-Anbieter ist Datenimporteur); der Cloud-Anwender muss trotzdem die Anforderungen nach § 11 Abs. 2 BDSG erfüllen und entsprechend vertraglich abbilden
- Safe-Harbour-Selbstzertifizierungen in den USA reichen allein nicht aus
- Nachweis der Vertrauenswürdigkeit mit einem SAS-70-Typ II-Zertifikat (wie z.B. Amazon EC2) genügen den Anforderungen nur teilweise
- möglich sind verbindliche Unternehmensregelungen (Binding Corporate Rules), die ein angemessenes Schutzniveau per Vertrag garantieren und die durch Datenschutz-Aufsichtsbehörden genehmigt werden müssen (§ 4c BDSG)





Ausblick





Was erfordert datenschutzgerechtes Cloud-Computing?

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität
- transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen einschließlich der Sicherheitskonzeption
- abgestimmte Sicherheitsmaßnahmen zwischen Cloud-Anbietern und Cloud-Anwendern
- Protection Profiles für Cloud Computing
- spezielle Auditierungsverfahren und aktuelle Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird
- weiterentwickelte Standardvertragsklauseln speziell für Cloud Computing





Weiterführende Literatur

- Orientierungshilfe „Cloud Computing“ (verfügbar ab Oktober 2011)
Konferenz der Datenschutzbeauftragten des Bundes und der Länder
- Cloud Computing und Datenschutz - Dr. Thilo Weichert (ULD S-H)
<https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html>
- BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter
<https://www.bsi.de>
- Cloud-Computing für die öffentliche Verwaltung
ISPRAT-Studie 11/2010 des Fraunhofer Instituts für Offene Kommunikationssysteme
http://www.cloud.fraunhofer.de/publikationen/isprat_cloud.jsp
- Materielien der ENISA zum Thema Cloud Computing
<http://www.enisa.europa.eu/act/rm/files/deliverables>
- Sichere Datenwolken – Jörg Heidrich / Christoph Wegener
MMR 12/2010, s. 803 ff.
- Amazon Webservice Security – AWS-Security
<http://aws.amazon.com/security>







Der Landesbeauftragte für Daten-
schutz und Informationsfreiheit M-V
Johannes-Stelling-Str. 21
19053 Schwerin
Telefon: 0385-59494-0
Telefax: 0385-59494-58
E-Mail: datenschutz@mvnet.de
Internet: www.datenschutz-mv.de

