Band 13 / 2014

Cloud-Sicherheit

Leitfaden für Behörden und Klein- und Mittelbetriebe

Johannes Göllner, Stefan Fenz und Gerald Quirchmayr (Hrsg.)

Schriftenreihe der
Landesverteidigungsakademie

www.bundesheer.at

SCHUTZ UND HILFE

KIRAS
Sicherheitsforschung

Cloud-Sicherheit: Leitfaden für Behörden und KMUs

Impressum:

Cloud-Sicherheit: Leitfaden für Behörden und KMUs

Eine Studie der Technischen Universität Wien, der Universität Wien und SophiSystems GmbH in Kooperation mit dem Bundesministerium für Landesverteidigung und Sport und der Bundessparte Information und Consulting (BSIC) der Wirtschaftskammer Österreich. Finanziert im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie.

Dr. Stefan Fenz

Mag. Johannes Heurix

Dr. Thomas Neubauer

Prof. Dr. A Min Tjoa

DI Johannes Göllner, MSc

DI Christian Meurers

Prof. DDr. Gerald Quirchmayr

Mag. Wolfram Hitz

Dr. Alexander Schatten

Prof. Dr. Erich Neuhold

MANAGEMENT SUMMARY

Cloud-Computing ist nicht länger ein sich entwickelnder Trend, sondern bereits fester Bestandteil der unternehmerischen und behördlichen IKT-Infrastruktur Österreichs. Die Ausprägungen reichen dabei von aktiv durch die Organisationen vorangetriebenen Cloud-Migrationen bis zur unkontrollierten Datenverwaltung auf Filesharing-Diensten wie Dropbox oder Verwendung Cloud-basierter E-Mail-Dienste wie GMail von Google.

Ein Großteil der in dieser Arbeit analysierten Cloud-Computing-Dienste befindet sich entweder ausserhalb des EU-Raums (meist in den USA) oder wird innerhalb der EU mit aus den USA stammenden Produkten betrieben. Jüngste Entwicklungen wie der NSA-Überwachungsskandal, die laschen Anforderungen an US-Unternehmen, welche dem Safe-Harbor-Abkommen unterliegen und der Zwang von US-Unternehmen unter dem „Patriot Act“ mit amerikanischen Behörden zu kooperieren, haben gezeigt, dass die Datenhaltung bei Anbietern, welche diesen Gegebenheiten unterliegen, höchst kritisch zu betrachten ist.

Auf Basis österreichischer und europäischer Datenschutzgesetze kann die Empfehlung gegeben werden, (i) sensible Daten gar nicht oder nur unter besonderen Sicherheitsvorkehrungen an Dritte innerhalb des EU-Raums auszulagern, (ii) personenbezogene Daten unter Berücksichtigung des österreichischen Datenschutzgesetzes nur an zertifizierte Anbieter im EU-Raum auszulagern und (iii) sonstige Daten nur dann an globale Anbieter auszulagern, wenn die Daten keine wirtschaftliche oder sonstige Bedeutung für die jeweilige Behörde oder das Unternehmen haben.

Prinzipiell sollte die Public Cloud als unsichere, z.T. sogar feindliche Umgebung betrachtet werden und Anwender müssen sich bewusst sein, die Kontrolle über die abgegebenen Daten verloren zu haben, sobald sie diese in Public Clouds transferieren. Aus diesem Grund empfehlen wir Vertragsinhalte hinsichtlich der Einhaltung gesetzlicher Bestimmungen genau zu prüfen (z.B. Datenschutzgesetz) und technische Maßnahmen zur Vermeidung von Ausspähungen zu implementieren (z.B. Verschlüsselung der hochgeladenen Daten).

Zur Verminderung der bestehenden US- und asiatischen Technologie-Dominanz und den damit verbundenen Problemen muss eine Stärkung der europäischen Cloud-Industrie erfolgen. Diese Stärkung kann über folgende Maßnahmen erreicht werden: (i) Bewusstseinsbildung innerhalb der Kundengruppen hinsichtlich der Problematik, um mehr Nachfrage nach europäischen Angeboten zu generieren, (ii) Schaffung von anerkannten Zertifikaten für Cloud-Computing-Anbieter, um dem Kunden die Auswahl zu erleichtern, und (iii) verstärkte Kooperation unter europäischen Cloud-Computing-Anbietern, um beispielsweise bewusstseinsbildende Maßnahmen gemeinsam zu leisten.

Inhalt

1 EINLEITUNG

Cloud-Computing hat sich in den vergangenen Jahren zu einem fixen Bestandteil österreichischer IT-Infrastrukturen entwickelt. Sowohl kleine als auch große Unternehmen nutzen Cloud-Computing, um Kosten- und Effizienzvorteile innerhalb ihrer IT-Landschaft zu realisieren. Laut Erhebungen der International Data Corporation (IDC) – als Anbieter von IT Market Intelligence Data – werden sich die Cloud-Computing-Umsätze allein in Westeuropa von 3,3 Milliarden Euro (2010) auf 15 Milliarden Euro in 2015 vervielfachen[1] [1]. Die Cloud-Infrastruktur von Amazon bewältigt bereits jetzt ca. 1% des in Nordamerika anfallenden Internetverkehrs und liefert ungefähr ein Drittel der täglichen Seitenaufrufe an Internetnutzer aus (große Angebote wie u.a. Reddit, Zynga, MySpace, Netflix, Dropbox, IBM, ESA und Newsweek werden teilweise über die Amazon-Cloud ausgeliefert)[2] [2]. Die hohe Anzahl von Cloud-Computing-Anbietern sowie potenzielle Sicherheitsrisiken und datenschutzrechtliche Anforderungen erschweren bei Unternehmen und Behörden die Auswahl geeigneter Anbieter.

1.1 Ziele der Studie

Diese Arbeit entwickelt zielgruppengerechte Handlungsempfehlungen für kleinere und mittlere Behörden und KMUs zur Auswahl des optimalen Cloud-Computing-Nutzungsmodells, welches ein ausgewogenes Maß an Datensicherheit, Datenschutz, Compliance (Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien) und Verfügbarkeit gewährleistet. Folgende damit verbundene Unterziele werden bearbeitet:

- **Kapitel 3: Zusammenfassung** der für österreichische Unternehmen und Behörden **relevanten Literatur** bzgl. rechtlicher und technischer Cloud-Computing-Aspekte (v.a. existierende internationale Leitfäden wie z.B. NIST SP 800-144, NIST SP 800-146 und EuroCloud).
- **Kapitel 4 und 5: Rechtlicher und technischer Evaluierungsbericht** ausgewählter Cloud-Service-Anbieter vor dem Hintergrund der kommenden EU-Datenschutzverordnung.
- **Kapitel 6: Analysebericht bzgl. Cloud-basierter Datenmissbrauchsszenarien** inkl. möglicher technischer, finanzieller und rechtlicher Konsequenzen.
- **Kapitel 7: Zielgruppengerechter Leitfaden** für österreichische Behörden und KMUs, der auf einfache Weise zeigt, wie bei der Nutzung von Cloud-Computing zu verfahren ist.
- **Kapitel 8: Zielgruppengerechte Handlungsempfehlungen** (Behörden und KMUs) für die Auswahl des optimalen Nutzungsmodells in Bezug auf Datensicherheit, Datenschutz, Compliance und Verfügbarkeit.

Diese Arbeit hebt sich in folgender Weise von existierenden, verwandten Arbeiten ab:

- Zusammenfassung der für österreichische KMUs und kleine Behörden relevanten rechtlichen Bestimmungen (inkl. Safe-Harbour-Abkommen)

[1] IDC Cloud Research, abrufbar unter: http://www.idc.com/prodserv/idc_cloud.jsp (letzter Zugriff: 24.03.2014)

[2] How big is Amazon's cloud?, abrufbar unter: http://blog.deepfield.net/2012/04/18/how-big-is-amazons-cloud/ (letzter Zugriff: 24.03.2014)

- Unterscheidung der Anforderungen von EPUs und KMUs
- Evaluierung konkreter Cloud-Service-Anbieter, welche relevante Dienste für EPUs, KMUs und kleine Behörden anbieten
- zielgruppengerechte Leitfäden und Handlungsempfehlungen basierend auf Schutzbedarfskategorien (sensibel, personenbezogen, unternehmenskritisch)

1.2 Studienaufbau

In Kapitel 2 werden die notwendigen Begriffsabgrenzungen vorgenommen und der Fokus der vorliegenden Studie definiert. Folgende Fragen werden beantwortet: Was ist Cloud-Computing? Welche Ausprägungen und Servicemodelle existieren? Welche Zielgruppen werden durch die Studie aufgrund welcher Faktoren adressiert?

Kapitel 3 widmet sich vergleichbaren Arbeiten im österreichischen, deutschen und internationalen Raum. Ziel ist es, möglichst viele bereits gewonnene Erkenntnisse in die vorliegende Studie einzuarbeiten, um den Fokus der eigentlichen Forschungsarbeit auf die Zielgruppen der österreichischen KMUs und Behörden legen zu können.

In Kapitel 4 werden die technischen und rechtlichen Grundlagen und Rahmenbedingungen von Cloud-Computing beschrieben. Sowohl wissenschaftliche Konzepte und Lösungsansätze als auch Best Practices fließen in die Beschreibung ein. Die rechtlichen Grundlagen werden basierend auf geltendem und in näherer Zukunft zu erwartendem österreichischen und europäischen Recht (EU Datenschutzverordnung) beschrieben.

Basierend auf Kapitel 4 erfolgen in Kapitel 5 eine strukturierte Analyse der österreichischen Gesetzeslage sowie der EU-Datenschutzverordnung und die Ableitung von rechtlichen und technischen Anforderungen an Cloud-Computing im EU-Raum. In einem zweiten Schritt werden bestehende Cloud-Service-Anbieter identifiziert; gemeinsam mit den Bedarfsträgern wird ein Teil dieser Anbieter für die rechtliche und technische Analyse ausgewählt. In einem letzten Schritt werden die Anforderungen der österreichischen Gesetzgebung und der EU-Datenschutzverordnung den rechtlichen und technischen Analyseergebnissen gegenübergestellt und eventuelle Lücken identifiziert.

In Kapitel 6 werden in einem ersten Schritt mögliche Datenmissbrauchsszenarien im Zusammenhang mit der Nutzung von Cloud-Diensten definiert und abgegrenzt. Mögliche rechtliche, technische, soziale und finanzielle Folgen werden darauf aufbauend abgeschätzt und Strategien zur Risikominimierung definiert.

In Kapitel 7 werden zielgruppenspezifische Leitfäden zur sicheren Cloud Nutzung in Behörden und KMUs beschrieben. Abgeleitet von den vorangegangenen Kapiteln werden rechtliche Mindestanforderungen, Schutzbedarfskategorien und Nutzungsmodelle definiert sowie Entscheidungsbäume und Checklisten zur einfachen, praktischen Umsetzung erstellt.

Kapitel 8 schließt die Studie mit konkreten Schlussfolgerungen und Handlungsempfehlungen für österreichische KMUs und Behörden ab.

2 DEFINITIONEN UND ABGRENZUNGEN

In diesem Kapitel wird der Begriff Cloud-Computing definiert, die notwendigen Abgrenzungen im Kontext dieser Studie vorgenommen sowie eine beispielhafte Auflistung von verfügbaren Diensten und Anbietern gegeben. Der Fokus der Studie in Bezug auf die Zielgruppen und verfügbare Cloud-Computing-Dienste/-Anbieter wird in Abschnitt 2.4 festgelegt.

2.1 Cloud-Computing

Der Begriff „Cloud-Computing“ ist im Jahr 2014 omnipräsent und ermöglichte die Entstehung neuer Industriezweige und Web-Angebote. Die Idee des heutigen Cloud-Computings ist allerdings keine neue. Bereits 1961 kam am Massachusetts Institute of Technology (MIT) die Idee auf[3] [3], Computerleistung über ein vorhandenes Netzwerk als Dienst anzubieten (ähnlich den Elektrizitätsnetzen). Heute ist diese Idee Wirklichkeit geworden und Cloud-Computing ersetzt zunehmend dezentrale Applikationslandschaften mit zentralen, jederzeit und überall abrufbaren Diensten, welche auf einer Fülle von Endgeräten ausführbar sind.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik definiert Cloud-Computing *als* Plichten des Cloud-Anbieters (Auszug §11) als das *an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur, Plattformen und Software.*[4] [4]

Das National Institute of Standards and Technology (NIST) definiert in der Special Publication 800-145[5] [5], Cloud-Computing durch das notwendige Vorhandensein von fünf Eigenschaften („Essential Characteristics“), drei verschiedenen Servicemodellen („Service Models“) und vier unterschiedlichen Betriebsmodellen („Deployment Models“):

[3] McCarthy, J., “Centennial Keynote Address,” Massachusetts Institute of Technology (MIT), USA, 1961.

[4] Cloud Computing Grundlagen, abrufbar unter: https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html (letzter Zugriff: 24.03.2014)

[5] Mell, P., Grance, T., “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, 2011.

Eigenschaften

- **Zugang zu Breitbandnetzen**

Auf Cloud-Dienste kann unter Verwendung von Breitbandzugängen und unter Einsatz von Standardtechnologie über Mobiltelefone, Laptops, PCs etc. zugegriffen werden.

- **Hohe und schnelle Elastizität (Skalierbarkeit)**

Notwendige Ressourcen (z.B. Rechenleistung oder Speicherplatz) werden dem Cloud-Nutzer automatisch und bedarfsgerecht zur Verfügung gestellt.

- **Messbare Dienste (verbrauchsorientiertes Bezahlmodell)**

Eingebaute Kontroll- und Messfunktionen ermöglichen die Optimierung des Ressourcenverbrauchs und gewährleisten dem Cloud-Anbieter und -Nutzer Transparenz bei den in Anspruch genommenen Diensten.

- **On Demand Selfservice (Ressourcenmanagement durch den Kunden)**

Dienste und Ressourcen können vom Cloud-Nutzer selbstständig und ohne Interaktion mit einem menschlichen Nutzer angefordert werden.

- **Resource Pooling**

Die Ressourcen des Cloud-Anbieters werden dem Nutzer dynamisch, ortsunabhängig und gebündelt zur Verfügung gestellt. Dem Cloud-Nutzer ist es somit nicht eindeutig möglich, den geografischen Ursprung der angebotenen Dienste zu eruieren.

Service-Modelle

- **Software as a Service (SaaS)**

Dem Kunden werden auf der Cloud-Infrastruktur laufende Applikationen angeboten. Auf die Applikationen kann über eine breite Palette von Geräten wie Smartphones, Thin Clients, Web-Browser (z.B. Webmail) oder programmatische Schnittstellen zugegriffen werden. Der Kunde kann dabei nicht die der Applikation zugrunde liegende Infrastruktur wie Netzwerke, Server, Betriebssysteme, Speicher oder generelle Applikationseinstellungen verwalten. Beispiele für SaaS-Angebote sind: salesforce.com, Google Apps oder Microsoft Office 365.

- **Platform as a Service (PaaS)**

Im Gegensatz zu SaaS kann der Kunde bei PaaS selbst entwickelte oder gekaufte Applikationen auf der angebotenen Cloud-Infrastruktur betreiben. Der Cloud-Anbieter stellt dazu eine Plattform inklusive Programmiersprachen, Bibliotheken, Diensten und Werkzeugen zur Verfügung. Der Kunde kann die darunterliegende Infrastruktur wie Netzwerk, Server, Betriebssystem und Speicher nicht selbstständig verwalten, hat aber die Kontrolle über die von ihm installierte Applikation (im Gegensatz zu SaaS). Beispiele für PaaS-Angebote sind: Google Apps Engine, Windows Azure und IBM Smart Business Development.

- **Infrastructure as a Service (IaaS)**

Bei IaaS stellt der Cloud-Anbieter dem Kunden Rechenleistung, Speicher, Netzwerke und andere fundamentale Rechenkapazitäten zur Verfügung; der Kunde ist in der Lage, darauf aufbauend beliebige Software inklusive Betriebssystemen zu installieren. Der Kunde kann die zugrunde liegende Cloud-Infrastruktur nicht verwalten, hat jedoch die Kontrolle über die verwendeten Betriebssysteme, Speicher und Applikationen. Beispiele für IaaS sind: Amazon EC2 und S3, Windows Azure Virtual Machines, Google Compute Engine und DynDNS.

Betriebsmodelle

- **Öffentliche Cloud**

Die Cloud-Infrastruktur wird für den allgemeinen, öffentlichen Gebrauch angeboten. Der Cloud-Anbieter kann aus dem wirtschaftlichen, öffentlichen oder akademischen Umfeld stammen. Die Cloud-Infrastruktur befindet sich im Einflussbereich des Anbieters.

- **Private Cloud**

Die Cloud-Infrastruktur wird exklusiv für eine Organisation und ihre Subeinheiten angeboten. Die Infrastruktur kann von der Organisation selbst oder einem Dienstleister besessen, verwaltet und betrieben werden.

- **Community Cloud**

Die Cloud-Infrastruktur wird exklusiv für eine Gemeinschaft von durch diverse Interessen verbundenen Organisationen angeboten (z.B. ähnliche Sicherheitsanforderungen oder Compliance-Verpflichtungen). Die Infrastruktur kann von den Organisationen selbst oder einem Dienstleister verwaltet und betrieben werden.

- **Hybride Cloud**

Die Cloud-Infrastruktur setzt sich aus zumindest zwei unabhängig voneinander betriebenen Betriebsmodellen zusammen, welche über standardisierte oder proprietäre Technologie zwecks Daten- und Applikationsaustausch verbunden sind (z.B. Load Balancing zwischen den einzelnen Clouds).

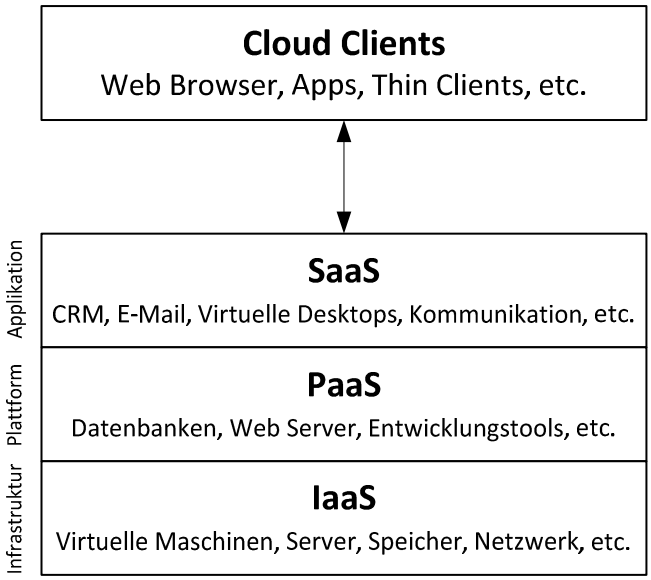

Abbildung 1: Cloud-Servicemodelle

2.2 Fokus der Studie

Der Fokus der vorliegenden Studie liegt auf **kleinen und mittleren Unternehmen und Behörden (inkl. Ein-Personen-Unternehmen)** als Nutzer/Kunden der angebotenen Cloud-Dienste. Innerhalb der angebotenen Cloud-Dienste konzentriert sich die Studie auf **öffentliche (public) Cloud-Dienste** und vernachlässigt aufgrund der Kundenzielgruppe private, hybride und gemeinschaftliche Cloud-Lösungen. Innerhalb der angebotenen öffentlichen Cloud-Dienste fokussiert diese Studie auf jene **Angebote, welche für die Zielgruppe relevante Dienste im Bereich Software as a Service zur Verfügung stellen** (z.B. Webmail- und Office-Lösungen). Der geografische Fokus umfasst **internationale, europäische und österreichische Cloud-Anbieter**.

Definition Ein-Personen-Unternehmen (EPU)

> Als Ein-Personen-Unternehmen gelten Unternehmen ohne unselbständig Beschäftigte (auch ohne geringfügig Beschäftigte) mit Orientierung am Markt, Ausrichtung der Tätigkeit auf Dauer und ohne Mitunternehmertum, d.h. im Wesentlichen nur Einzelunternehmen und GmbH.[6] [6] Für die vorliegende Studie wird diese Definition der Wirtschaftskammer Österreich wie folgt erweitert: Es findet innerhalb des Unternehmens keine IT-gestützte Kommunikation statt (E-Mail, Instant Messaging, geteilte Terminplanung etc.).

[6] Ein-Personen-Unternehmen in Österreich, abrufbar unter: http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=357341&DstID=17 (letzter Zugriff: 24.03.2014)

Definition kleine und mittlere Unternehmen (KMU)

Kleine und mittlere Unternehmen sind von der Europäischen Kommission als Unternehmen bis 249 Mitarbeiter mit weniger als 50 Millionen Euro Umsatz und 43 Millionen Euro Bilanzsumme definiert. [7][7] Bis 9 Mitarbeiter handelt es sich um ein Kleinstunternehmen, von 10 bis 49 Mitarbeiter um ein Kleinunternehmen und von 50 bis 249 Mitarbeiter um ein mittleres Unternehmen. Für die vorliegende Studie werden KMU darüber hinaus als Unternehmen definiert, in welchen eine IT-gestützte Kommunikation innerhalb des Unternehmens stattfindet.

Definition kleine und mittlere Behörde

Als kleine und mittlere Behörde gelten im Kontext dieser Studie Gemeinden mit weniger als 50.000 Einwohnern.

2.2.1 Cloud-Dienste

Im Sinne der oben angeführten Definitionen und Zielgruppen listet Tabelle 1 die in der Studie fokussierten Cloud-Dienste inkl. beispielhaften Produkten und Zielgruppen. Bei den Zielgruppen wird zwischen EPU, KMU bzw. kleinen Behörden und Netzwerken unterschieden. Netzwerke definieren sich als ein loser und informeller Zusammenschluss zwischen EPU, KMU und kleinen Behörden.

Tabelle 1: Cloud-Dienste

Dienst	beispielhafte Produkte	EPU	KMU, kleine Behörden	Netzwerke
E-Mail	Google Mail	X	X	X
Instant Messaging	hosted.IM		X	X
Video- und Audio-Conferencing	BlueJeans	X	X	X
geteilte Kalender	Google Calendar		X	X
geteilter Speicherplatz	Dropbox		X	X
Datensicherung/Datenarchivierung	Wuala, ARQ	X	X	
Textverarbeitung und Tabellenkalkulation	Office365, Google Docs	X	X	X

[7] Klein- und Mittelbetriebe in Österreich: https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/KMU_Definition.html (letzter Zugriff: 24.03.2014)

Abrechnung, Rechnungserstellung	Billomat	X	X	
Projektmanagement	Easy-PM	X	X	X
CRM (Customer Relationship)	Mircosoft Dynamics CRM	X	X	
CMS (Content-Management-Systeme)	Osmek		X	
Zeiterfassungssysteme	TimeTac, Time&Bill	X	X	
Personalgeschäftsprozesse (z.B. Urlaubsantrag)	Utilitas		X	
ERP (Enterprise Resource Planning)	NetSuite ERP		X	
Dokumentenmanagementsysteme (DMS)	Folio Cloud	X	X	
Softwareentwicklungswerkzeuge	GitHub, Amazon Web Services	X	X	
Produktivitätswerkzeuge (To-do-Listen, Notizanwendungen etc.)	Remember the Milk, Evernote	X	X	
virtuelle Server	VMware	X	X	X
Sicherheitsdienstleistungen (E-Mail-Filter, SPAM-Abwehr, Verschlüsselung etc.)	Proofpoint	X	X	

2.2.2 Datenarten

Innerhalb der in Tabelle 1 angeführten Dienste ist im Kontext dieser Studie vor allem die Verarbeitung schutzwürdiger Daten von Interesse. Als schutzwürdig werden folgende Datenarten definiert:

- **sensible Information im Sinne des österreichischen Datenschutzgesetz (DSG)**
  - Gesundheitsbereich (Ärzte, Therapeuten etc.)

- **personenbezogene Information im Sinne des DSG**
  - nahezu alle Branchen (Rechnungen, Angebote, Schriftverkehr etc.)

- **Information mit bestimmten Archivierungspflichten (BAO)**
  - alle Branchen (Buchhaltungsdaten, Rechnungen etc.)

- **sonstige schutzwürdige Information**
    - alle Branchen (Geschäftsgeheimnisse, Konstruktionspläne, Forschungs- und Entwicklungsergebnisse)
    - unternehmensinterne Datenklassifikation (geheim, streng geheim etc.):
        - Vertraulichkeit: hoch, mittel, niedrig (Security Policy BMI, cio.gv.at)
        - Verfügbarkeit: hoch, mittel, niedrig
        - Integrität: hoch, mittel, niedrig

- **Definition sensibler Information im Sinne des DSG:**

Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.

- **Definition personenbezogener Information im Sinne des DSG**

Angaben über Personen, deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen" sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

- **Schutzbedarfsdefinition niedrig**

Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat keine oder kaum Auswirkungen auf das Unternehmen bzw. auf die Behörde.

Beispiele: öffentlich verfügbare Marketingmaterialien (Flyer, Produktbroschüren etc.)

- **Schutzbedarfsdefinition mittel**

Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat empfindliche finanzielle, rechtliche oder rufschädigende Wirkung auf das Unternehmen bzw. auf die Behörde.

Beispiele: personenbezogene Daten, vertrauliche Konstruktionspläne

- **Schutzbedarfsdefinition hoch**

Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat existenzbedrohende finanzielle, rechtliche oder rufschädigende Wirkung auf das Unternehmen bzw. auf die Behörde.

Beispiele: sensible Kundendaten

Sowohl für EPU, KMU als auch kleine Behörden sind die Erfüllung gesetzlicher Bestimmungen (DSG, BAO – Bundesabgabenordnung etc.) und der Schutz sonstiger unternehmenskritischer Daten von höchstem Interesse. In allen der in Abschnitt 2.2.1 genannten Dienste können potenziell sensible, personenbezogene und sonstige schutzwürdige Daten verarbeitet werden (z.B. Notizen bzgl. der religiösen Einstellung eines Mitarbeiters in einer dafür geeigneten Cloud-Anwendung). Aus diesem Grund bezieht diese Studie auch auf den ersten Blick unbedenkliche Cloud-Dienste in die Analyse mit ein und entwickelt zielgruppengerechte Handlungsempfehlungen für kleinere/mittlere Behörden und KMUs zur Auswahl des optimalen Nutzungsmodells für Cloud-Computing, welches ein ausgewogenes Maß an Datensicherheit, Datenschutz, Compliance und Verfügbarkeit gewährleistet.

3 VERWANDTE ARBEITEN

In diesem Kapitel werden Studien, Publikationen und praktische Leitfäden zum Thema Datensicherheit und Datenschutz in der Cloud ausgewertet. Insbesondere werden dabei unter „3.3 International“ folgende bereits existierende Dokumente analysiert: (i) NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (USA), (ii) NIST Special Publication 800-146, DRAFT Cloud Computing Synopsis and Recommendations (USA) und (iii) „Cloud Computing Security Considerations“ des australischen Cyber Security Operations Centre (AU).

3.1 Österreich

3.1.1 ASIT – Österreichisches Informationssicherheitshandbuch – Cloud-Strategie

Abschnitt A3 des österreichischen Informationssicherheitshandbuchs [8] widmet sich den Sicherheitsaspekten von Cloud-Computing und deckt in diesem Kontext folgende Themenfelder ab: (i) Begriffsdefinitionen, (ii) rechtliche Aspekte und deren Auswirkungen, (iii) strukturelle Aspekte, (iv) wirtschaftliche Aspekte, (v) technische Aspekte, (vi) Integration von Cloud-Computing in bestehende Geschäftsprozesse und (vii) Entscheidungsunterstützung bzgl. Cloud-Computing-Integration.

3.1.2 Eurocloud.Austria – Leitfäden Cloud-Computing

Der Verein EuroCloud.Austria publiziert Cloud-Computing-Leitfäden zu den Themen (i) Recht, Datenschutz und Compliance [9], (ii) öffentliche Auftragsvergabe, d.h. wie ist bei der Vergabe von Cloud-Computing-Leistungen zu verfahren, (iii) Lizenzen im Cloudvertrag, d.h. welche relevanten Lizenzbedingungen existieren für Anbieter und Nutzer, (iv) Auswahl und Einführung von Cloud-Services, d.h. welche Dienste können durch Cloud-Services abgedeckt werden und wie gestaltet sich die Einführung und Verwendung im Unternehmen, (v) steuerliche Aspekte aus Sicht des Cloud-Anbieters und Cloud-Nutzers, (vi) Leistungsstörung und Vertragshaftung in der Vertragsabwicklung inkl. straf- und verwaltungsstrafrechtliche Aspekte und (vii) internationale rechtliche Aspekte.

3.1.3 Eurocloud.Austria – Cloud-Verträge – Was Anbieter und Kunden besprechen sollten

Der von EuroCloud.Austria, Wirtschaftskammer Wien, Austrian Standards und Wirtschaftsagentur Wien herausgegebene Katalog „Cloud-Verträge – Was Anbieter und Kunden besprechen sollten“ [10] beinhaltet empfohlene Vertragselemente, die in den Allgemeinen Geschäftsbedingungen oder den Service Level Agreements von Cloud-Service-Unternehmen berücksichtigt werden sollten. Konkret umfasst der Leitfaden Inhalte zu den Themen (i) Vertragsbedingungen, (ii) Leistungserbringung von

Cloud-Services, (iii) Verrechnung, (iv) Sicherheit, (v) Datenschutz, (vi) IT-Sicherheit und (vii) Datensicherung und Datenlöschung.

3.1.4 Wirtschaftskammer Österreich – IT Sicherheitshandbuch

In Kapitel 3 der 5. Auflage des IT-Sicherheitshandbuchs der Wirtschaftskammer Österreich [11] werden die Vorteile, potenzielle Kosteneinsparungen und Risiken (Anbieterabhängigkeit, Verlust der Kontrolle über Daten, Leistungsstörungen, Lizenzfragen, Datenschutz und Schwierigkeiten in der Rechtsdurchsetzung) von Cloud-Computing erläutert. Die Wirtschaftskammer Österreich empfiehlt im Kontext des IT-Sicherheitshandbuchs Unternehmen, sich vor dem Umstieg auf Cloud-Computing mit folgenden Fragen auseinanderzusetzen:

- Welche Datenschutz- und Datensicherheitsstandards hat der Cloud-Anbieter umgesetzt?
- Wie ist die Cloud aufgebaut? Wo werden die Daten gespeichert?
- Wie gewährleistet der Cloud-Anbieter die Verschlüsselung der Daten?
- Wie wird der Zugriffsschutz bzgl. der gespeicherten Daten gewährleistet?
- Welche Verfahren zur Information des Auftraggebers werden bei Datenverlust angewandt?
- Wie sehen die Notfallmaßnahmen bei Service-Ausfall aus?

3.1.5 Bundeskanzleramt Österreich – Cloud-Computing-Positionspapier

Das unter der Leitung des Bundeskanzleramts Österreich erstellte Cloud-Computing-Positionspapier 2011 [12] untersucht die Möglichkeiten des Einsatzes von Cloud-Computing in der österreichischen öffentlichen Verwaltung. Rechtliche, strukturelle, wirtschaftliche und technische Aspekte, Auswirkungen, Chancen und Risiken sowie potenzielle Anwendungen für klassische Rechenzentren werden beschrieben.

3.1.6 EGIZ – E-Government und Cloud-Computing

Dieses Papier konzentriert sich auf die besonderen Anforderungen von E-Government-Applikationen an Cloud-Computing und den damit verbundenen Datenschutz- und IT-Sicherheitsfragen [13]. Die größten Herausforderungen in Cloud-Umgebungen werden bei (i) User-, Access- und Identity-Management, (ii) Datensicherheit im Sinne der Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit durch Verschlüsselung, sicheres Löschen etc., (iii) Auditierung/Zertifizierung von Cloud-Anbietern und (iv) Datenschutz gesehen. Beim Datenschutz werden vor allem die weltweit verteilten Speicherarchitekturen, die dadurch unterschiedlichen Datenschutzgesetzgebungen, potenzielle Off-Shore-Speicherplätze ohne Datenschutzregelungen, Zugriff ausländischer Ermittlungsbehörden (z.B. im Rahmen des Safe-Harbor-Abkommens) als im Einzelfall zu adressierende Herausforderungen identifiziert.

3.1.7 Wirtschaftsagentur Wien – Software as a Service – Verträge richtig abschließen

Herausgegeben vom IT-Cluster der Wirtschaftsagentur Wien setzt sich dieser Leitfaden [14] mit den rechtlichen Aspekten von Software as a Service auseinander und beleuchtet die damit verbundenen Fragestellungen. Folgende Inhalte werden abgedeckt: (i) vertragliche Aspekte inkl. Streit- und Insolvenzfällen, (ii) Datenschutz und -sicherheit aus technischer und organisatorischer Perspektive, (iii) Ausfallsicherheit, (iv) Betriebsverhalten und (v) Hilfsmittel für die Vertragsverhandlung.

3.2 Europa

3.2.1 BSI Sicherheitsempfehlungen für Cloud Computing Anbieter

Die vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeiteten Empfehlungen für sicheres Cloud-Computing [15] richten sich in erster Linie an Cloud-Computing-Anbieter und sollen diesen eine Richtschnur zur sicheren Implementierung ihrer Dienste bieten. Die Empfehlungen erstrecken sich über die Bereiche Sicherheitsmanagement, Sicherheitsarchitektur (Rechenzentrumsicherheit, Server-Sicherheit, Netzsicherheit, Anwendungs- und Plattformsicherheit, Datensicherheit, Verschlüsselung und Schlüsselmanagement), ID- und Rechtemanagement, Kontrollmöglichkeiten für Nutzer, Monitoring und Security Incident Management, Notfallmanagement, Portabilität, Sicherheitsprüfungen, Anforderungen an das Personal, Vertragsgestaltung und Datenschutz. Die Empfehlungen adressieren neben einem Grundschutz auch Maßnahmen für erhöhte Verfügbarkeits- und Vertraulichkeitsanforderungen. Vom BSI wird das Papier als Diskussionsgrundlage zwischen Cloud-Konsument und -Anbieter verstanden und bildet die Basis für die Erweiterung und Konkretisierung der IT–Grundschutz-Bausteine des BSI. Im Rahmen dieser Studie bilden die BSI-Sicherheitsempfehlungen eine der Grundlagen für die in diesem Projekt erarbeiteten Empfehlungen.

3.2.2 Bitkom Cloud Computing – Was Entscheider wissen müssen

In dem vom deutschen Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) herausgegebene Cloud-Computing-Leitfaden [16] werden folgende Aspekte behandelt: (i) wirtschaftliches Potenzial von Cloud-Computing, (ii) Marktentwicklung, (iii) Geschäftsmodelle, (iv) vertragliche Regelungen für Cloud-Computing (Definitionen von Leistungen und Pflichten, Anzahl der Vertragspartner, Rechtswahl, Leistungsbeschreibung und Service Level Agreements, Vertragsänderungen, Gewährleistung und Haftung, Nutzungsrechte, Vergütung, Subunternehmer, Notfall-Management und Vertragsbeendigung), (v) Cloud-Computing und Datenschutz (Relevanz, anwendbares Datenschutzrecht, Auftragsdatenverarbeitung, technisch-organisatorische Maßnahmen und Informationspflichten), (vi) Cloud-Computing und Informationssicherheit (technische und organisatorische Aspekte, Security as a Service) und (vii) Cloud Compliance (Compliance-Management-Systeme, IT-Compliance-Anforderungen und -Risiken).

3.2.3 ULD Datenschutzrechtliche Anforderungen an Cloud-Computing

Das vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein herausgegebene Merkblatt „Datenschutzrechtliche Anforderungen an Cloud-Computing“[8] [17] unterscheidet zwei Hauptgruppen von Cloud-spezifischen Risiken im Kontext der Datenschutzgesetzgebung: (i) jene, welche einen Kontrollverlust über personenbezogene Daten bei der Nutzung von Cloud-Diensten mit sich bringen, und (ii) jene, welche sich auf unzureichende Information über das „Wie“, „Wo“ und „Wer“ der Verarbeitung personenbezogener Daten beziehen. Neben der durch Art. 17 Abs. 3 Richtlinie 95/46/EG verlangten vertraglich zu vereinbarenden Regelung, dass der Auftragnehmer (Cloud-Service-Anbieter) den Weisungen des Auftraggebers (Kunde) Folge zu leisten sowie technische und organisatorische Maßnahmen zu treffen hat, um die personenbezogenen Daten angemessen zu schützen, empfiehlt das ULD-Merkblatt die vertragliche Regelung folgender Punkte:

- detaillierte Angaben zu den Weisungsbefugnissen des Kunden an den Cloud-Service-Anbieter (anwendbare SLAs und relevante Strafen)
- Beschreibung konkreter technischer und organisatorischer Maßnahmen, die der Cloud-Service-Anbieter zu erfüllen hat
- Gegenstand und Laufzeit der Cloud-Nutzung sowie Umfang, Art und Zweck der Verarbeitung personenbezogener Daten
- Regelung für die Rückgabe personenbezogener Daten oder deren Zerstörung nach Vertragsende
- Vereinbarung einer Vertraulichkeitsklausel für Cloud-Service-Anbieter und dessen Mitarbeiter
- Gewährleistung der Betroffenen-Rechte im Hinblick auf Auskunft, Berichtigung und Löschung ihrer Daten
- Verbot von Datenweitergabe an Dritte (Ausnahme: vertraglich vereinbarte Weitergabe an Sub-Auftragnehmer)
- Information des Kunden durch den Cloud-Service-Anbieter im Falle eines Datenschutz-Verstoßes
- Bereitstellung einer Liste der Orte, an welchen die Daten des Kunden gespeichert und verarbeitet werden
- Recht des Kunden, die Einhaltung der Verpflichtungen des Cloud-Service-Providers zu überwachen
- Information des Kunden durch den Cloud-Service-Anbieter im Falle von relevanter Änderungen (z.B. Implementierung neuer Funktionalität)
- Loggen und Auditieren der Verarbeitung von personenbezogenen Daten
- Verpflichtung der Information des Kunden durch den Cloud-Service-Anbieter, falls lokale Strafverfolgungsbehörden Zugriff auf den Datenbestand des Kunden gestatten wird

[8] Datenschutzrechtliche Anforderungen an Cloud-Computing, abrufbar unter: https://www.european-privacy-seal.eu/results/fact-sheets/Cloud%20Computing%20FS-201207-DE.pdf (letzter Zugriff: 24.03.2014)

3.2.4 ENISA Cloud Computing – Benefits, Risks, and Recommendations for Information Security

Der von der European Network and Information Security Agency (ENISA) veröffentlichte Leitfaden [18] beschreibt (i) Security Benefits (standardisierte Interfaces, Skalierbarkeit etc.), (ii) Risiken (organisatorische Risiken, technische Risiken und rechtliche Risiken) und (iii) Schwachstellen von Cloud-Computing. Im Gegensatz zu anderen Leitfäden geht der ENISA-Leitfaden explizit auf die Sicherheitsvorteile von Cloud-Computing ein:

- Sicherheit und die Vorteile skalierbarer Umgebungen (Sicherheitsmaßnahmen werden mit dem Umfang ihrer Implementierung kostengünstiger)
- Sicherheit als Dienstleistung für Kunden durch gemanagte Umgebungen
- standardisierte Schnittstellen und gemanagte Sicherheitsdienste
- Skalierbarkeit der benötigten Ressourcen
- Audit und vereinfachte Beweissicherung durch virtuelle Umgebungen
- zeitnahe Softwareupdates
- Audits und Service Level Agreements erfordern ein besseres Risikomanagement.

ENISA identifizierte folgende Top-Risiken im Zusammenhang mit Cloud-Computing:

- Steuerungsverlust durch verminderte Kontrollmöglichkeiten aufgrund Auslagerung von IT-Services
- „Lock-in"-Effekte durch meist fehlende Möglichkeiten bzgl. Applikations- und Datenportabilität unter verschiedenen Anbietern
- fehlende Isolation der Dienste durch gemeinsame Verwendung von Ressourcen (Speicher, Netzwerke etc.)
- Compliance-Risiken durch fehlende Zertifizierungen der Cloud-Service-Anbieter
- Kompromittierung der meist Web-basierten Management-Schnittstellen
- Verletzung von Datenschutzvorschriften durch Speicherung/Verarbeitung in nicht sicheren Drittstaaten
- unsichere oder unvollständige Löschung von Daten
- Insider-Bedrohungen durch Administratoren des Cloud-Service-Anbieters

3.2.5 ENISA Survey – An SME perspective on Cloud Computing

Die Online-Studie [19] wurde von ENISA im Zeitraum April 2009 bis Juni 2010 durchgeführt und identifizierte auf Basis der 74 erhaltenen Rückmeldungen folgende Gründe, Modelle, Entscheidungsfaktoren etc., deren zwei bis drei häufigsten Antworten hier auszugsweise gelistet werden:

- **Gründe, warum KMU Cloud-Services nutzen:**
    1. Kosteneinsparungen (68%)
    2. Flexibilität und Skalierbarkeit der IT-Ressourcen (64%)
    3. Business Continuity und Disaster Recovery (52%)

- **Das passendsten Modell (private, public etc.):**
    1. Zusammenschluss von Clouds aus verschiedensten Quellen (31%)
    2. Partner Cloud – administriert von einem vertrauten Partner (27%)
    3. Public Cloud – im Eigentum und unter Verwaltung von Externen (24%)

- **Der geeignetste Typ (SaaS, PaaS, IaaS etc.):**
    1. Software as a Service (34%)
    2. Platform as a service (29%)
    3. Infrastructure as a Service (25%)

- **Bereitschaft, Dienste zu mehreren Cloud-Service-Anbietern auszulagern:**
    1. Ja (74%)
    2. Nein (26%)

- **mögliche Disaster-Recovery-Optionen:**
    1. Pläne, welche auf unternehmensinternen Ressourcen beruhen (64%)
    2. komplett ausgelagerte Disaster-Recovery- und Business-Continuity-Dienste (49%)

- **Dienste, welche am wahrscheinlichsten durch Cloud-Service-Anbieter unterstützt werden:**
    1. CRM/Sales Management (53%)
    2. Anwendungsentwicklung (44%)
    3. Projektmanagement (42%)

- **Bedenken in Bezug auf Cloud-Computing-Services:**
    1. Vertraulichkeit von unternehmensinternen Daten
    2. Privacy/Datenschutz
    3. Integrität von Diensten und Daten

3.2.6 ENISA – Critical Cloud Computing – A CIIP perspective on cloud computing services

In dem von ENISA im Dezember 2012 publizierten Bericht [20] wird die Verwendung von Cloud-Computing in kritischen Infrastrukturen untersucht. Folgende übergeordnete Schlussfolgerungen wurden gezogen:

- Cloud-Computing wird durch dessen hohe Durchdringung innerhalb der kritischen Infrastrukturen selbst zur kritischen Infrastruktur.
- Ein wesentlicher Vorteil von Cloud-Computing ist die Risikominimierung bzgl. lokaler Risiken wie Naturkatastrophen, Stromausfällen und Erdbeben (natürlich nur dann, wenn die Cloud-Computing-Rechenzentren geografisch dementsprechend verteilt sind).
- Cloud-Computing hilft durch dessen Ressourcenelastizität DDoS-Attacken besser abzuwehren.

- Einzelne Angriffe auf größere Cloud-Computing-Anbieter können aufgrund der hohen Datenkonzentration signifikante Datenlecks nach sich ziehen.
- IaaS- und PaaS-Anbieter sind kritischer einzustufen als SaaS-Anbieter.
- Verwaltungstechnische und rechtliche Konflikte eines Cloud-Service-Kunden können negative Auswirkungen auf Kunden haben, welche dieselben Ressourcen innerhalb des Cloud-Service-Anbieters verwenden.

Folgende Empfehlungen werden bzgl. der nationalen Governance kritischer Cloud-Computing-Dienste gegeben:

1. **Risikoerfassung**
    a. Nur die wesentlichsten und kritischsten Cloud-Services sollten in einem ersten Schritt adressiert werden. Die Ressourcen, um alle Cloud-Services zu adressieren sind meist nicht verfügbar.
    b. Erfassung und Schaffung von Transparenz hinsichtlich der logischen und physischen Abhängigkeit von Cloud-Computing. Welche Abhängigkeiten bestehen bereits bzw. welche werden in naher Zukunft geschaffen?

2. **Sicherheitsmaßnahmen**
    a. Sicherheitsmaßnahmen müssen bei Bedarf aktualisiert und an die veränderten Gegebenheiten angepasst werden. Die Orientierung an Best Practices und der Austausch mit anderen Betreibern kritischer Infrastrukturen werden unbedingt empfohlen.
    b. Cloud-Computing-Infrastrukturen sind meist geografisch verteilt, um für den Kunden das Risiko lokaler Ausfälle zu minimieren. Zusätzlich zur physischen Redundanz sollten auch logische Redundanzen geschaffen werden, um die Verwundbarkeit bzgl. Angriffen, welche beispielsweise auf spezielle Softwareschwachstellen abzielen, zu minimieren.
    c. Standardisierung ist für den schnellen Wechsel zwischen Cloud-Service-Anbietern für Betreiber kritischer Infrastrukturen von äußerster Wichtigkeit und sollte speziell in der IaaS- und PaaS-Domäne vorangetrieben werden.
    d. Regelmäßige Audits und Tests von internen und externen Auditoren sollen die Implementierung der Sicherheitsmaßnahmen überwachen. Jährliche Tests werden im Kontext der kritischen Infrastrukturen als nicht ausreichend angesehen.

3. **Incident Reporting**
    a. Verpflichtendes Reporting bzgl. zu definierender Sicherheitsvorfälle soll die Sicherheit der Cloud-Services messbarer machen und basierend auf ausreichender Datenlage die Adaptierung von Sicherheitsmaßnahmen ermöglichen.
    b. Nationale Regierungen sollten Anreize für die Meldung von Sicherheitsvorfällen schaffen. Ansonsten besteht die Gefahr, dass Vorfälle aus Angst vor rechtlichen oder rufschädigenden Konsequenzen nicht gemeldet werden.

3.2.7 RAND Europe – The Cloud – Understanding the Security, Privacy and Trust Challenges

Co-finanziert von der Europäischen Kommission, identifizierte RAND Europe Herausforderungen bzgl. Security, Privacy und Trust im Kontext des Cloud-Computings [21]:

- Technologische Herausforderungen: Virtualisierung und potenzielle Hypervisor[9]-Schwachstellen, Interoperabilität unterhalb der Anbieter, übergreifendes Identitätsmanagement, ausreichende Stärke der verwendeten Verschlüsselungsalgorithmen
- Rechtliche und regulatorische Herausforderungen: Berücksichtigung unterschiedlicher Gesetzgebungen bei über mehrere Rechtsräume verteilten Cloud-Systemen, Effektivität von Informationspflichten im Falle eines Datenlecks, effektive Verfolgung von Cyber-Crime innerhalb von Cloud-Umgebungen
- Operationale Herausforderungen: Effektivität von Risk Governance Frameworks, gesetzeskonforme Datenspeicherung außerhalb des EU-/EWR-Raums, Einhaltung der Informationspflichten, Vendor Lock-in, Audit-Komplexität, Transparenz und Messbarkeit der Sicherheit von Cloud-Diensten

In durchgeführten Fallstudien konnten folgende Herausforderungen identifiziert werden:

- unreife bzw. experimentelle Cloud Computing Deployments
- fehlende Risikoanalysen vor Cloud-Migrationen
- Balance zwischen Kostenvorteilen und der Wahrung von Sicherheit und Datenschutz
- Integration von Cloud-Sicherheit in bestehende Sicherheitsprogramme im Unternehmen
- fehlendes Bewusstsein bzgl. der Abhängigkeit von Cloud-Computing-Diensten (bei vollständiger Auslagerung)
- Angepasste Sicherheitsvereinbarungen können nur durch dementsprechende Verhandlungen mit dem Anbieter erreicht werden.

Basierend auf den identifizierten Herausforderungen werden folgende Empfehlungen formuliert:

- Harmonisierung von relevanten rechtlichen und regulatorischen Rahmenwerken (z.B. Datenschutzgesetzgebung)
- Verbesserung der Kundenstellung in Bezug auf die Wahrnehmung und Durchsetzung ihrer vertraglich zugesicherten Rechte (Security Service Level Agreements)
- Erhöhung der Transparenz bzgl. der Umsetzung von Security, Privacy und Trust Maßnahmen
- Verbesserung von Security Event- und Incident Monitoring durch automatisierte Tools

[9] Computerprogramm, welches eine virtuelle Maschine bereitstellt und überwacht (siehe http://de.wikipedia.org/wiki/Hypervisor [22]).

3.3 International

3.3.1 NIST Special Publication 800-144 – Guidelines on Security and Privacy in Public Cloud Computing (US)

Die vom National Institute of Standards and Technology heraus gegebenen „Guidelines on Security and Privacy in Public Cloud Computing“ [23] bieten einen Überblick über die Herausforderungen bzgl. Sicherheit und Datenschutz in Cloud-Computing:

- **Governance**
  Governance impliziert den Überblick und die Kontrolle der Organisation über Policies, Prozeduren und Standards für Anwendungsentwicklung und -betrieb (Design, Implementierung, Tests, Verwendung und Monitoring). Während Cloud-Computing die Auslagerung der Anwendungsentwicklung und des Anwendungsbetriebs kostengünstig erlaubt, verliert die Organisation zunehmend die Kontrolle über die dahinterstehenden Prozesse. Eine unter 900 europäischen und amerikanischen Unternehmen durchgeführte Umfrage zeigt, dass Besorgnis über einen potenziellen Wildwuchs an Cloud-Computing-Anwendungen im Unternehmen besteht[10] [24] (vergleichbar mit nicht autorisierten WLAN Access Points, welche interne Unternehmensnetzwerke an existierenden Firewalls vorbei an die Außenwelt anbinden).

- **Compliance**
  Compliance beschreibt die Verantwortung einer Organisation, gemäß geltender Gesetze, Regulativen, Standards und Normen zu handeln. Die verteilte Struktur von Cloud-Computing erschwert durch die Auslagerung von IT-Dienstleistungen die Überprüfung der Einhaltung von gesetzlichen Bestimmungen (nationale und internationale Datenschutzgesetze, Auskunftspflichten etc.). Der oft unklare physische Ort der in der Cloud gespeicherten Daten macht es zunehmend schwierig, die getroffenen Sicherheitsmaßnahmen auf deren Wirksamkeit zu prüfen. Zusätzlich ergeben sich bei der Speicherung in unterschiedlichen Rechtsräumen juristische Herausforderungen, welche im Extremfall auf sich widersprechenden Anforderungen der Rechtsräume basieren können.

- **Trust**
  Die Auslagerung von IT-Services an Cloud-Computing-Anbieter stellt ein enormes potenzielles Sicherheitsproblem dar. Organisationsinterne Daten werden außerhalb der Organisationsgrenzen verarbeitet/gespeichert und sind somit für Administratoren des Cloud-Computing-Anbieters zugänglich. Neben Administratoren können die Daten auch Subauftragnehmern und im Falle eines technischen Defekts anderen Kunden zugänglich sein. Das Eigentumsrecht der an den Cloud-Computing-Anbieter überlassenen Daten sowie notwendige Risikomanagementmaßnahmen sollten im Vertrag eindeutig zugunsten des Auftraggebers definiert sein.

[10] Larry Ponemon, Security of Cloud Computing Users, Ponemon Institute, May 12, 2010, <URL: http://www.ca.com/files/IndustryResearch/security-cloud-computing-users_235659.pdf>

- **Architektur**
  Um potenzielle Datensicherheitsprobleme möglichst vollständig zu erfassen, muss der Auftraggeber die technische Architektur des angebotenen Cloud-Services verstehen und potenzielle Subauftragnehmer bzw. die verwendete Cloud-Technologie Dritter ebenfalls in seine Risikoanalyse miteinbeziehen.

- **Identitäts- und Zugriffsverwaltung**
  Der Auftraggeber sollte sicherstellen, dass angemessene Mechanismen für Autorisierung, Authentifikation sowie Identitäts- und Zugriffsverwaltungsfunktionen beim Cloud-Service-Anbieter implementiert sind.

- **Isolierung der Software**
  Zum Schutz der organisationsinternen Daten sollte der Cloud-Service-Anbieter Methoden zur logischen Softwareisolation und Virtualisierung implementiert haben.

- **Datensicherheitsmaßnahmen**
  Angemessene Datensicherheitsmaßnahmen müssen über den gesamten Datenlebenszyklus implementiert sein (Speicherung, Übermittlung, Verwendung und Löschung). Risiken betreffend der beim Cloud-Service-Anbieter implementierten Verwaltung kryptografischer Schlüssel müssen erfasst und abgewogen werden.

- **Verfügbarkeit**
  Die Anforderungen der Organisation bezüglich Verfügbarkeit, Datensicherung bzw. Wiederherstellung von Daten sowie Disaster Recovery müssen erfasst und vom Cloud-Service-Anbieter unterstützt werden.

- **Incident Response**
  Die Organisation muss sicherstellen, dass der Cloud-Service-Anbieter angemessene Incident-Response-Prozesse (z.B. im Fall einer unautorisierten Weitergabe von Daten) unterstützt und der Prozess in einer transparenten Art und Weise beschrieben ist.

NIST empfiehlt folgende Vorgangsweise bei der Auswahl geeigneter Cloud-Service-Anbieter:

- **vorbereitende Aktivitäten**
  - Identifikation von sicherheitstechnischen und organisatorischen Anforderungen an den Cloud-Service-Anbieter

  - Analyse der von den Cloud-Service-Anbietern umgesetzten Sicherheitsmaßnahmen und Bestimmung des korrespondierenden Risikos im Falle einer Auslagerung an den jeweiligen Anbieter
  - Evaluierung, ob der Cloud-Service-Anbieter die gesetzten Anforderungen über die angestrebte Vertragslaufzeit erfüllen kann

- **laufende Aktivitäten**
  - Sicherstellung, dass alle sicherheitstechnischen Anforderungen im Vertrag und dem dazugehörigen Service Level Agreement festgelegt sind
  - Rechtlicher Beistand sollte bei der Durchsicht der Vertragsdokumente und bei der Verhandlung der Bedingungen hinzugezogen werden.
  - kontinuierliche Qualitätsüberprüfungen der bezogenen Leistungen und Sicherstellung, dass die vertraglichen Vereinbarungen eingehalten werden

- **abschließende Aktivitäten**
  - Hinweis des Cloud-Service-Anbieters auf die im Vertrag vereinbarte Vorgehensweise bei Kündigung des Vertrags
  - Entzug aller physischen und elektronischen Zugriffsrechte sowie Rückgabe kryptografischer Token vom Cloud-Service-Anbieter an den Auftraggeber
  - Sicherstellung, dass organisationsinterne Information vom Cloud-Service-Anbieter an den Auftraggeber in einer geeigneten und vertraglich vereinbarten Weise zurückgegeben und die Daten auf den Systemen des Anbieters sicher gelöscht werden.

3.3.2 NIST Special Publication 800-146 – Cloud Computing Synopsis and Recommendations (US)

Die NIST Special Publication 800-146 [25] beschreibt die generelle Funktionalität von Cloud-Computing und geht darüber hinaus auf die Spezifika der Umgebungen von Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) ein. Als Herausforderungen des Cloud-Computing werden folgende Punkte identifiziert:

- **Performance:**
  Latenz, Offline-Datensynchronisation, skalierbare Programmierung, Datenspeicherungsverwaltung

- **Zuverlässigkeit:**
  Abhängigkeit von Netzwerken, Ausfälle der Cloud-Service-Anbieter, Verarbeitung sicherheitskritischer Daten

- **wirtschaftliche Zielsetzungen:**
  Risiko für Business Continuity, Entwicklung von Service Agreements, Portabilität, Interoperabilität, Disaster Recovery

- **Compliance:**
  physischer Speicherort der Daten, begrenzte Zugänglichkeit der Rechnerressourcen, geografisch unterschiedliche Gesetzgebungen, Unterstützung forensischer Aktivitäten

- **Informationssicherheit:**
  Risiko der Vertraulichkeitsverletzung, Datenschutz, Systemintegrität, Mehrfachbenutzung von gleichen Ressourcen durch unterschiedliche Benutzer, Browser-Sicherheit, Verwaltung kryptografischer Schlüssel

NIST empfiehlt, folgende Punkte bzgl. Cloud-Computing-Sicherheit zu beachten:

- Minimierung kundenseitiger Schwachstellen in Browsern und spezieller Clientsoftware, welche für den Zugriff auf die Cloud-Dienste verwendet werden.
- Daten, welche beim Cloud-Service-Anbieter gespeichert oder zu diesem übermittelten werden, sollten mit starken Verschlüsselungsmethoden verschlüsselt werden.
- Überprüfung der physischen Sicherheitsmaßnahmen des Cloud-Service-Anbieters (z.B. Backup-Rechenzentren).
- Verwendung starker Authentifizierungsmethoden (Tokens etc.), um die unerlaubte Übernahme von Nutzerkonten zu erschweren.
- Verständnis des Kunden bzgl. der Qualität verwendeter Identitäts- und Zugriffsverwaltungsmethoden

3.3.3 Cloud Computing Security Considerations (AU)

Die „Cloud Computing Security Considerations“ [26] des australischen Verteidigungsministeriums verstehen sich nicht als Sicherheits–Checkliste, sondern als Diskussionsgrundlage, um das Risiko einer Cloud-Migration zu erfassen. Folgende Überlegungen sollten vor der Inanspruchnahme eines Cloud-Dienstes angestellt werden:

- Werden unternehmenskritische/sensible Daten oder Funktionalitäten in die Cloud ausgelagert?
- Sind die Business-Continuity- und Disaster-Recovery-Pläne des Cloud-Service-Anbieters einsehbar?
- Ist ein zusätzlicher organisationsinterner Datensicherungsplan für die in der Cloud gespeicherten Daten vorgesehen?
- Soll ein zweiter Cloud-Service-Anbieter als Backup zum ersten Cloud-Service-Anbieter verwendet werden?
- Ist die Netzanbindung zum Cloud-Service-Anbieter hinsichtlich Verfügbarkeit, Durchsatz, Latenz und Paketverlusten ausreichend dimensioniert?
- Wird im Service Level Agreement eine ausreichende Verfügbarkeit zugesichert und sind Kompensationen für SLA-Verletzungen adäquat?
- Wie wahrt der Cloud-Service-Anbieter die Integrität und Verfügbarkeit der Daten (Backup-Strategie etc.)?
- Wie lange dauert es, irrtümlich gelöschte Dateien aus den Backup-Kopien wiederherzustellen?

- Wie können Daten und Funktionalität im Falle einer Insolvenz oder eines simplen Anbieterwechsels zu einem neuen Anbieter portiert werden („Vendor Lock-in“)?
- Können geltende Datenschutzbestimmungen trotz Auslagerung der Daten eingehalten werden?
- In welchen Staaten werden die Daten gespeichert/verarbeitet und besteht die Möglichkeit des Zugriffes durch Behörden in diesen Staaten?
- Werden die Daten verschlüsselt gespeichert und übertragen?
- Wie wird sichergestellt, dass die Daten sicher gelöscht werden?
- Besteht die Möglichkeit, die Sicherheit der vom Cloud-Service-Anbieter betriebenen Systeme selbst zu überwachen?
- Geht das Eigentum an den Daten auf den Cloud-Service-Anbieter über?
- Implementiert der Cloud-Service-Anbieter angemessene Netzwerksicherheitsmaßnahmen (Firewalls, Traffic Flow Filter, Inhaltsfilter, Antivirus etc.)?
- Gewährt der Anbieter Einblick in die Struktur seines Information-Security-Management-Systems?
- Gewährt der Anbieter Einblick in die konkrete Umsetzung seines Sicherheitskonzepts (Patchzyklen, Konfigurationen etc.) und kann dieses durch Audits oder Penetrationstests getestet werden?
- Wird zur Anmeldung bei den Cloud-Service-Diensten eine starke Authentifizierung verwendet?
- Welche Maßnahmen werden gesetzt, um unsichere Geräte von einer Verbindung zu den in der Cloud gespeicherten Daten abzuhalten?
- Welche Maßnahmen sind zur physischen Sicherheit der IT-Infrastruktur umgesetzt?
- Wie wird sichergestellt, dass organisationsinterne Daten isoliert von anderen Kunden gehalten werden? Ist es möglich, IT-Infrastruktur exklusiv zu nutzen?
- Wird der Kunde als Referenzkunde auf der Website des Cloud-Service-Anbieters präsentiert und somit einem erhöhten Sicherheitsrisiko ausgesetzt?
- Hat der Cloud-Service-Anbieter Kenntnis über die von der Organisation verwendeten kryptografischen Schlüssel?
- Führt der Cloud-Service-Anbieter Hintergrundüberprüfung hinsichtlich seiner Mitarbeiter durch und ist die IT-Infrastruktur ausreichend gegen Insider-Bedrohungen geschützt?
- Gilt für Subauftragnehmer dasselbe Sicherheitsniveau?
- Existieren klare und konkrete Regelungen hinsichtlich Incident Response und den damit verbundenen Reaktionszeiten des Cloud-Service-Anbieters?

3.3.4 CSA Security Guidance for Critical Areas of Focus in Cloud Computing

Der von der Cloud Security Alliance (CSA) veröffentlichte Leitfaden „Security Guidance for Critical Areas of Focus in Cloud Computing“ [27] umfasst 13 Domänen, welche potenzielle Cloud-Computing-Kunden bei der sicheren Umsetzung einer Cloud-Migration unterstützen sollen:

1. **Governance und Enterprise Risk Management**

Erfassung und Bewertung des Risikos, welches durch den Einsatz von Cloud-Computing in die Organisation eingebracht wird (z.B. Umgang mit sensiblen Daten in unterschiedlichen Rechtsräumen)

2. **Legal Issues: Contracts and Electronic Discovery**

   Rechtliche Mindeststandards betreffend Schutz von Informationssystemen, Informationspflichten bei Datenschutzverletzungen, regulative Anforderungen, Datenschutzanforderungen, internationale Gesetze etc.

3. **Compliance and Audit**

   Aufrechterhaltung, Überprüfung und Nachweis der Compliance des Cloud-Computing-Betriebs in Bezug auf interne Richtlinien und öffentliche rechtliche/regulative Anforderungen

4. **Information Management and Data Security**

   Maßnahmen zur Wahrung der Datensicherheit in der Cloud sowie Verantwortlichkeiten bzgl. Vertraulichkeit, Integrität und Verfügbarkeit der in der Cloud gespeicherten Daten werden in dieser Domäne thematisiert.

5. **Portability and Interoperability**

   Mögliche Methoden, um Daten und Dienste von einem Cloud-Service-Anbieter zum nächsten zu transferieren bzw. die Interoperabilität unterhalb der Anbieter sicherzustellen.

6. **Traditional Security, Business Continuity and Disaster Recovery**

   Wie beeinflusst der Einsatz von Cloud-Computing das traditionelle Sicherheitskonzept und den Risikolevel der Organisation?

7. **Data Center Operations**

   Hilfestellungen zur Beurteilung der Qualität von Datenzentrumsarchitekturen und deren Implementierungen.

8. **Incident Response, Notification and Remediation**

   Auswirkungen des Cloud-Computing-Einsatzes auf bisherige organisationsinterne Incident-Response-Prozesse; Leitfäden für geeignete Incident-Response-Mechanismen auf Anbieter und Kundenseite, um reibungslosen Informationsfluss und nachträgliche Forensik zu gewährleisten.

9. **Application Security**

   Gewährleistung von Anwendungssicherheit bei in der Cloud angebotenen bzw. entwickelten Diensten

10. **Encryption and Key Management**
    Identifikation geeigneter Verschlüsselungs- und Schlüsselverwaltungssysteme

11. **Identity and Access Management**
    Beschreibung der Herausforderungen, welche mit einer Erweiterung des Identitäts- und Zugriffsmanagements in die Cloud verbunden sind; Beschreibung Cloud-basierter Identity- und Access-Management-Lösungen.

12. **Virtualization**
    Beschreibung von Risiken bzgl. Hardware- und Softwarevirtualisierung: Mehrbenutzerumgebungen, Isolierung virtueller Maschinen, Hypervisor-Schwachstellen etc.

13. **Security as a Service**
    Beschreibung der Vorteile und Risiken von Cloud-basierten Security-Diensten (Web-Security, E-Mail-Security, Network Security, IDS/IPS etc.).

3.3.5 Gartner – Assessing the Security Risks of Cloud Computing

Gartner identifizierte in der Studie „Assessing the Security Risks of Cloud Computing“[11] [28] sieben Hauptrisiken bei der Verwendung von Cloud-Computing in Unternehmen:

1. Zugriff durch privilegierte Nutzer des Cloud-Service-Anbieters auf ausgelagerte unternehmensinterne Daten
2. fehlende Sicherheitszertifizierung beim Cloud-Service-Anbieter und sich daraus ergebende rechtliche Probleme auf Kundenseite
3. eingeschränkte Kontrolle über den physischen Speicherort der Daten
4. Vermischung von Daten durch die gemeinsame Verwendung von Speicherressourcen
5. eingeschränkte Kontrolle über Wiederherstellungsmechanismen
6. schwierige Rekonstruktion von Vorgängen durch verteilte Speicherung von Log-Dateien
7. Konkurs und/oder Fusion des Cloud-Computing-Anbieters und die damit verbundenen Konsequenzen

3.3.6 CSA – The Notorious Nine: Cloud Computing Top Threats in 2013

Basierend auf einer Umfrage unter Experten aus der Industrie identifizierte die Cloud Security Alliance die neun kritischsten Cloud-Computing-Bedrohungen [29]:

1. **Datenlecks**

[11] Assessing the Security Risks of Cloud Computing, abrufbar unter: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing (letzter Zugriff: 24.03.2014)

Durch fehlerhaft geplante oder betriebene virtuelle Infrastrukturen können organisationseigene Daten von Konkurrenzunternehmen oder anderen Angreifern ausgelesen werden.

2. **Datenverlust**
   Daten werden absichtlich (Angriff) oder unabsichtlich (Naturkatastrophe) unwiederbringlich gelöscht und stehen dem Kunden nicht länger zur Verfügung.
3. **Übernahme des Accounts oder des Datenverkehrs**
   Phishing, Betrug oder die Ausnutzung von Softwareschwachstellen werden verwendet, um Zugriff auf den organisationseigenen Cloud-Computing-Account zu erlangen, um in weiterer Folge Daten auszuspähen, zu manipulieren oder zu löschen. Auch die Verwendung des organisationseigenen Accounts für kriminelle oder rufschädigende Zwecke ist möglich (z.B. Versand von Spam-Mail)[12] [30].

4. **Unsichere APIs**
   Application Programming Interfaces (APIs) werden verwendet, um mit Cloud-Services zu interagieren, sie untereinander zu verbinden und zu verwalten. Authentifizierung, Zugriffskontrolle, Verschlüsselung und Überwachung werden mithilfe von öffentlich zugänglichen APIs realisiert. Unsichere APIs stellen deshalb eine ernstzunehmende Bedrohung für die Sicherheit des Cloud-Services dar.

5. **Denial of Service**
   „Denial of Service"-Angriffe verhindern, dass Cloud-Service-Nutzer Zugriff auf die von ihnen benötigten Dienste und Daten erhalten. Durch die gemeinsame Verwendung von Cloud-Computing-Ressourcen kann die übermäßige Ressourcenkonsumation eines Kunden zu eingeschränkten oder nicht verfügbaren Diensten anderer Kunden führen.

6. **Bösartige Insider**
   Die Auslagerungen kritischer IT-Dienste an Cloud-Service-Anbieter erhöht das Risiko von Angriffen interner Akteure (z.B. Administratoren des Cloud-Service-Anbieters).

7. **Missbrauch von Cloud-Services**
   Der kostengünstige und rasche Zugriff auf enorme Mengen an Rechenleistung kann von Kunden für kriminelle Aktivitäten verwendet werden (z.B. „Denial of Service"-Angriffe oder Entschlüsselung von Passwörtern).

8. **Unzureichende Due Diligence der Cloud-Kunden**
   Potenzielle Kosteneinsparungen veranlassen Organisationen schnell und teils unbedacht dazu, ihre IT-Dienste an Cloud-Service-Anbieter auszulagern. Genau Prüfung und Planung vor Migration in die Cloud wird empfohlen, um spätere Probleme zu vermeiden.

[12] Zeus bot found using Amazon's EC2 as C&C server, abrufbar unter:
http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/ (letzter Zugriff: 24.03.2014)

9. **Probleme aufgrund der geteilten Nutzung von Ressourcen**
   Die gemeinsame Verwendung von IT-Ressourcen (Prozessor, Speicher, Netzwerke, Datenträger, Server etc.) eröffnet zahlreiche Möglichkeiten, die Daten anderer Kunden durch Ausnutzung von fehlerhaften Konfigurationen oder Schwachstellen auszulesen, zu manipulieren oder zu löschen.

3.3.7 CSA – GRC Stack

Der von der Cloud Security Alliance (CSA) entwickelte GRC (Governance, Risk, and Compliance) Stack[13] [31] ermöglicht es Unternehmen, Cloud-Service-Anbietern, Anbietern von Sicherheitslösungen, IT-Auditoren und anderen mit Cloud-Sicherheit befassten Akteuren, private und öffentliche Clouds gegen Industriestandards, Best Practices und Compliance-Anforderungen abzugleichen. Folgende Werkzeuge sind Teil des GRC Stacks:

- **Cloud Audit**
  Gemeinsame Schnittstelle für Kunden und Anbieter zur Automatisierung von Audits, Assertion, Assessment und Assurance in IaaS-, PaaS- und SaaS-Umgebungen.

- **Cloud Controls Matrix (CCM)**
  Maßnahmenkatalog für den sicheren Betrieb von Cloud-Services. Jede im Katalog enthaltene Maßnahme ist mit anerkannten Standards wie HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI DSS, HIPAA und NIST SP 800-53 abgeglichen und erleichtert somit die Kontextfindung in diesen Standards. Darüber hinaus ist jede Maßnahme bzgl. ihres Architekturkontexts (physisch, Netzwerk, rechnen, speichern, Applikation, Daten) und Cloud-Service-Modells (SaaS, PaaS, IaaS) definiert.

- **Consensus Assessments Initiative Questionnaire (CAIQ)**
  Ähnlich der Cloud-Control-Matrix, enthält der CAIQ Fragen bzgl. der Umsetzung von Sicherheitsmaßnahmen und vertraglichen Regelungen zwischen Cloud-Service-Anbietern und Kunden. Folgende Maßnahmengruppen werden abgedeckt: Compliance, Data Governance, Facility Security, Human Resources Security, Information Security, rechtliche Aspekte, Operations Management, Risk Management, Release Management, Resilience und Security Architecture. Jede Maßnahme ist mit den Standards COBIT, HIPAA, ISO 27001, NIST SP 800-53, FedRAMP, PCI DSS, BITS und GAPP abgeglichen.

- **Cloud Trust Protocol (CTP)**
  Das Cloud Trust Protocol unterstützt die Kommunikation zwischen Kunden und Anbieter bzgl. umgesetzter Sicherheitsmaßnahmen und durchgeführter Aktivitäten innerhalb der Cloud. Ziel ist es sicherzustellen, dass nur vereinbarte Aktionen und Maßnahmen vom Anbieter in der Cloud ausgeführt werden.

[13] GRC Stack, abrufbar unter: https://cloudsecurityalliance.org/research/grc-stack/ (letzter Zugriff: 24.03.2014)

3.3.8 The FedRAMP Security Controls Baseline

Das Federal Risk and Authorization Management Program (FedRAMP) [32] ist ein US-Regierungsprogramm, welches einen standardisierten Ansatz für das Security Assessment, die Autorisierung und die laufende Überprüfung von Cloud-Produkten und -Diensten bietet. Die FedRAMP Security Controls Baseline ist vom NIST SP 800-53 Maßnahmenkatalog abgeleitet und wurde innerhalb der einzelnen Maßnahmen um Cloud-spezifische Aspekte erweitert. Die Maßnahmendomänen umfassen Access Control, Awareness and Training, Audit and Accountability, Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Personnel Security, Risk Assessment, System and Service Acquisition, System and Communications Protection und System and Information Integrity.

4 TECHNISCHE UND RECHTLICHE GRUNDLAGEN

In diesem Kapitel werden die technischen und rechtlichen Grundlagen und Rahmenbedingungen von Cloud-Computing beschrieben. Sowohl wissenschaftliche Konzepte, Lösungsansätze als auch Best Practices fließen in die Beschreibung ein. Die rechtlichen Grundlagen werden basierend auf geltendem und in näherer Zukunft zu erwartendem österreichischen und europäischen Recht (EU Datenschutzverordnung) beschrieben.

4.1 Technische Grundlagen

Cloud-Computing basiert auf Architekturen, welche in den letzten 20 Jahren für verteilte Netzwerkapplikationen entwickelt wurden. Zusätzlich zu den standardisierten Netzwerkprotokollen verwendet Cloud-Computing die im letzten Jahrzehnt entwickelten Virtualisierungsmethoden, um Ressourcen wie zum Beispiel Speicher- oder Rechenleistung bedarfsgerecht anbieten zu können. In Erweiterung zu den Beschreibungen in Abschnitt 2.1, zeigt Abbildung 2 das Cloud-Computing Referenzmodell nach Sosinsky[14] [33]. Darin bauen die Servicemodelle Infrastructure as a Service, Platform as a Service und Software as a Service aufeinander auf und bieten dem Kunden Ressourcen unterschiedlicher Abstraktionsebenen (z.B. reine Hardware und spezialisierte Software):

- **Infrastructure as a Service:** Rechenleistung, Speicher, Netzwerke und andere fundamentale Rechenkapazitäten werden dem Kunden auf Basis von Virtualisierungstechnologie zur Verfügung gestellt. Der Hypervisor erlaubt die Verwaltung der virtuellen Ressourcen.
- **Platform as a Service:** Dem Kunden wird Soft- und Hardware zur Entwicklung von Web-Applikationen und -Diensten zur Verfügung gestellt.
- **Software as a Service:** Dem Kunden werden auf der Cloud-Infrastruktur laufende Applikationen zur unmittelbaren Verwendung angeboten.

Grundsätzlich kann die Cloud in zwei unterschiedliche Schichten unterteilt werden: der Client als Frontend und die Cloud als das Backend. Beide Schichten haben sich ergänzende Funktionalität und verwenden eine Mischung unterschiedlicher Standards und proprietärer Protokolle, um die gewünschten Dienste bereitzustellen. Application Programming Interfaces (APIs) erlauben die Kommunikation mit außenstehenden Diensten. Bei Software as a Service wird die eigentliche Funktionalität des Dienstes auf den Servern der Anbieter bereitgestellt. Der Browser des Kunden oder eine Client-Applikation des Anbieters fungieren als Schnittstelle zum Dienst und stellen die folgenden Funktionalitäten bereit: (i) Erfassung der Eingabedaten via lokaler Speichermedien, Tastatur, Maus oder anderer Eingabegeräte, (ii) Darstellung textueller, grafischer und akustischer Ausgabedaten und (iii) Speicherung von Aus-

[14] Sosinsky, Barrie: Cloud Computing Bible (2011)

gabedaten auf lokalen Speichermedien. Um die dabei ausgetauschten Daten vor Einsicht Dritter zu schützen, wird die Verbindung zwischen den Servern des Anbieters und dem Browser des Kunden verschlüsselt. Zur Erstellung der dafür notwendigen Schlüssel authentifiziert sich der Kunde beim Anbieter meist mittels Benutzername und Passwort. In manchen Fällen werden zusätzlich Hardware-Tokens zur Erhöhung der Sicherheit verwendet.

Im Fall von Public-Cloud-Services teilt sich der Kunde fast immer die darunterliegende Hard- und Software mit anderen Kunden. D.h. im Falle von SaaS-Angeboten werden die organisationseigenen Daten gemeinsam mit den Daten anderer Kunden auf denselben Speichermedien, Betriebssystemen, virtuellen Maschinen, Netzwerken und Rechnern verarbeitet. Folgende technische Überlegungen sollten bei der Nutzung von Public-Cloud-Services angestellt werden[15]:

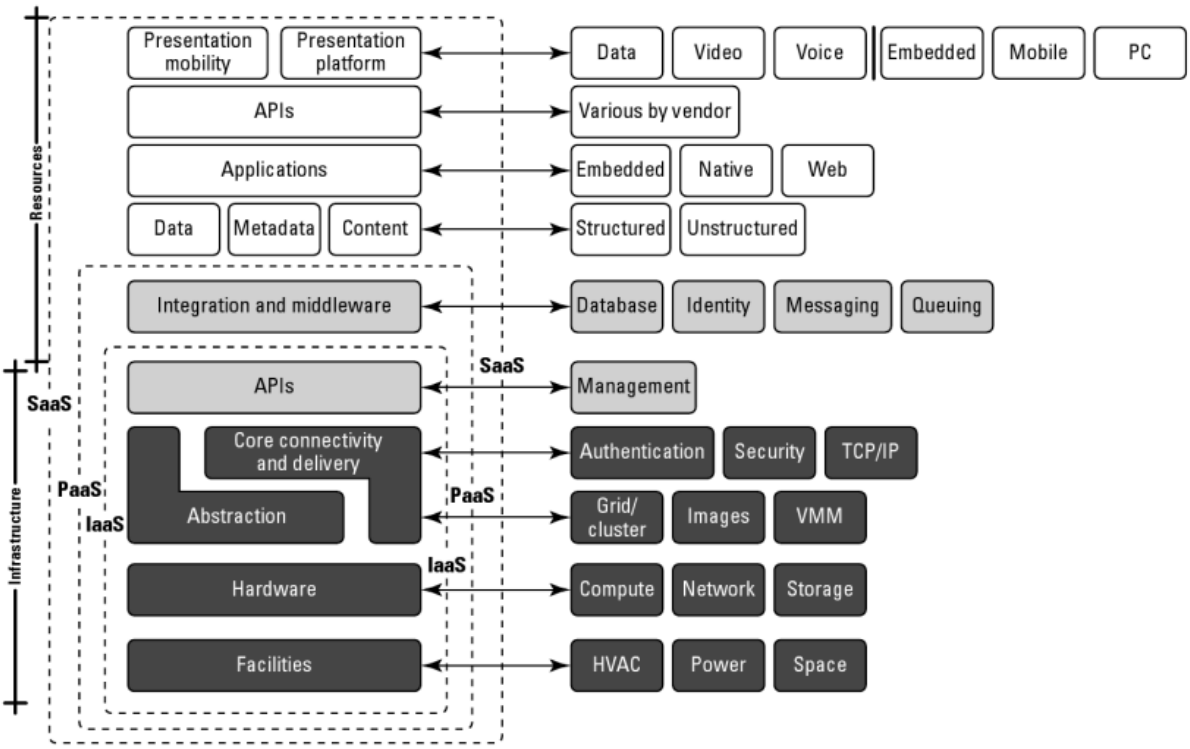

Abbildung 2: Cloud-Computing-Referenzmodell[16]

- **Abhängigkeit von öffentlichen Netzwerken** bzw. der Zuverlässigkeit des Internet-Service-Anbieters zwecks Zugangs zum Cloud-Service

- Der **Ort der Speicherung und Verarbeitung der Daten** ist dem Kunden oftmals nicht bekannt. Um kostengünstige Cloud-Services anbieten zu können, bedienen sich Cloud-Service-Anbieter unterschiedlicher Rechenzentrumsstandorte, welche die Arbeitslast je nach Bedarf und Kostenstruktur an den Standorten abarbeiten. Sollten die Daten einen gewissen geografi-

[15] Diese Überlegungen basieren auf NIST SP 800-146 und dem BKA-Positionspapier.

[16] vgl. Sosinsky (2011)

schen Raum nicht verlassen (z.B. EWR-Raum), so ist dies vertraglich zu vereinbaren. Die technische Überprüfung der Einhaltung gestaltet sich jedoch sehr schwierig.

- Die **gemeinsame Verwendung von Ressourcen** (Soft- und Hardware) mit anderen Kunden oder gar Mitbewerbern stellt ein Sicherheits- und Zuverlässigkeitsrisiko dar. Attacken können somit nicht nur von außen, sondern auch von innen (beispielsweise über die internen Ressourcen des Cloud-Service-Anbieters) ausgeführt werden. Sind die Ressourcen des Cloud-Services nicht ausreichend dimensioniert, kann die übermäßige Ressourceninanspruchnahme eines Kunden die Zuverlässigkeit der Dienste anderer Kunden beeinträchtigen.

- Der Kunde hat nur **limitierte Kontrolle über Datenzugriffe,** welche nicht von ihm selbst durchgeführt werden (beispielsweise von Administratoren des Cloud-Service-Anbieters). Dies gilt auch für vermeintlich gelöschte, aber physisch noch immer vorhandene Kundendaten auf den Systemen des Cloud-Service-Anbieters. Unabhängige externe Audits und eine genaue vertragliche Spezifikation des Rechte- und Zugriffsmanagements können die Sicherheit in diesem Aspekt erhöhen.

- **Unzureichende Standardisierung von Portabilitätsschnittstellen.** Der Wechsel des Cloud-Service-Anbieters ist nach wie vor mit einem hohen Aufwand auf Seiten des Kunden verbunden. Standardisierte Schnittstellen für die Daten- bzw. Funktionsportierung bestehen kaum. Potenzielle Gefahr: Vendor Lock-in.

- Der **Zugriff auf kundenspezifische Metadaten** wie zum Beispiel Logfiles und Zugriffslisten muss vertraglich geregelt werden, um die organisationsinterne Sicherheitspolitik und Compliance umsetzen zu können.

- Zwar gewährleisten Cloud-Services ein effizientes Patch-Management (schnellere Einspielungen bei geringeren Ausfallzeiten), jedoch werden kundenspezifische Anforderungen hinsichtlich der **Verträglichkeit der Patches mit kundenspezifischen Anwendungen** im Normalfall nicht vom Cloud-Service-Anbieter getestet.

Neben den beschriebenen Herausforderungen bieten SaaS-Angebote folgende Vorteile:

- keine aufwändige Softwareinstallation und -verteilung erforderlich
- Effiziente Verwendung von Softwarelizenzen: Lizenzen müssen nicht pro Computer erworben werden, sondern werden zentral auf den Servern des Anbieters verwaltet.
- Zentralisierte Verwaltung und Datenhaltung: Zentral implementierte Sicherheitsmaßnahmen (z.B. zentralisiertes Daten-Backup) senken die Kosten der einzelnen SaaS-Kunden.
- zentral gewartete Plattformen und Infrastruktur (Patch-Management, physische Sicherheit etc.)

4.2 Rechtliche Grundlagen

Welches nationale Recht im Einzelfall zur Anwendung kommt, regelt Art. 4 der Datenschutz-Richtlinie 95/46/EG. Bei Cloud-Diensten kann zwischen zwei Fällen unterschieden werden[17] [34]:

- Ist der Cloud-Kunde in einem EU-/EWR-Mitgliedsstaat niedergelassen, so kommt das Recht des Niederlassungsstaats zur Anwendung
- Ist der Cloud-Kunde außerhalb des EU-/EWR-Raums niedergelassen und beauftragt einen Cloud-Anbieter innerhalb des EU-/EWR-Raums, kommt das Recht des Niederlassungsstaats des Cloud-Anbieters zur Anwendung (datenschutzrechtlicher Auftragnehmer und als „Mittel" im Sinne des Art.4(1)(c) Richtlinie 95/46/EG).

4.2.1 Österreichische Rechtslage

Dieser Abschnitt beschreibt jene Bereiche der österreichischen Gesetze, welche für das Angebot und die Nutzung von Cloud-Computing Relevanz haben. Das österreichische Datenschutzgesetz bildet einen Schwerpunkt dieses Abschnitts.

4.2.1.1 Allgemeines Bürgerliche Gesetzbuch (ABGB)

Das Allgemeine Bürgerliche Gesetzbuch ist ein Bundesgesetz, welches am 1. Jänner 1812 in Kraft getreten und heute noch geltend ist. Es stellt eine der wichtigsten Kodifikationen des österreichischen Zivilrechts dar, was durch § 1 des ABGB dargelegt wird.

§ 1 ABGB: „*Der Inbegriff der Gesetze, wodurch die Privat-Rechte und Pflichten der Einwohner des Staates unter sich bestimmt werden, macht das bürgerliche Recht in demselben aus.*"

Das ABGB unterteilt sich in fünf Teile: (1) Präambel/Promulgationsklausel, (2) Einleitung: Von den bürgerlichen Gesetzen überhaupt, (3) 1. Teil: Von dem Personenrechte, (4) 2. Teil: Von dem Sachenrechte und (5) 4. Teil: Von den gemeinschaftlichen Bestimmungen der Personen- und Sachenrechte.

Im Kontext von Cloud-Computing und Subauftragnehmern ist vor allem § 1313a ABGB von Bedeutung:

„Wer einem andern zu einer Leistung verpflichtet ist, haftet ihm für das Verschulden seines gesetzlichen Vertreters sowie der Personen, deren er sich zur Erfüllung bedient, wie für sein eigenes."

4.2.1.2 Unternehmensgesetzbuch (UGB) und GmbH-Gesetz

Die Verantwortung für Informationssicherheit liegt laut Unternehmensgesetzbuch und GmbH-Gesetz grundsätzlich bei der Unternehmensführung. Zwar können IT-sicherheitsrelevante Aufgaben im Rahmen einer IT-Sicherheitspolicy an Mitarbeiter delegiert werden, das Management ist jedoch für die Einhaltung gesetzlicher Bestimmungen letztverantwortlich.

[17] Datenschutzrechtliche Anforderungen an Cloud-Computing, abrufbar unter: https://www.european-privacy-seal.eu/results/fact-sheets/Cloud%20Computing%20FS-201207-DE.pdf (letzter Zugriff: 24.03.2014)

4.2.1.3 Verbandsverantwortlichkeitsgesetz (Unternehmensstrafrecht)

Verbände im Sinne des Verbandsverantwortlichkeitsgesetzes sind Aktiengesellschaften, GmbHs, Stiftungen, Vereine, Genossenschaften, Personengesellschaften und Erwerbsgesellschaften. Bund, Länder, Gemeinden und anerkannte Religionsgesellschaften werden im Kontext dieses Gesetzes nicht als Verbände eingestuft (§1 VbVG).

Ein Verband ist für eine Straftat verantwortlich, wenn die Tat zu seinen Gunsten begangen worden ist oder durch die Tat Pflichten verletzt worden sind, die den Verband betreffen (beispielsweise Pflichten im Sinne des Datenschutzgesetzes). Der Verband ist sowohl für Straftaten des Entscheidungsträgers (Tat rechtswidrig und schuldhaft begangen), als auch jene der Mitarbeiter (vorsätzlich Handlungen; wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung der Tat wurden durch den Entscheidungsträger nicht implementiert) verantwortlich. Ein Unternehmen ist zu bestrafen, wenn die Tat zum Vorteil des Unternehmens begangen wurde. Aus diesem Grund ist das Unternehmen so zu organisieren, dass bei Straftaten von Mitarbeitern kein Organisationsverschulden eines Entscheidungsträgers vorgeworfen werden kann[18] [35]. Nach § VbVG werden Geschäftsführer, Vorstände, Prokuristen, Vertretungsmächte oder sonstige Personen mit maßgeblichen Einfluss als Entscheidungsträger definiert. Dienstnehmer, Lehrlinge und überlassene Arbeitskräfte werden als Mitarbeiter verstanden.

Beim arbeitsteiligen Zusammenwirken mehrerer Personen gilt der Vertrauensgrundsatz: Wer sich selbst objektiv sorgfaltsgemäß verhält, darf grundsätzlich auch auf das sorgfaltsgemäße Verhalten eines anderen vertrauen, es sei denn, dass dessen sorgfaltswidriges Verhalten eindeutig erkennbar ist oder doch aufgrund konkreter Umstände nahe liegt. Bei hierarchischen Strukturen kann sich auf den Vertrauensgrundsatz nur berufen, wer selbst seinen Auswahl-, Überwachungs- und sonstigen Organisationspflichten ordnungsgemäß nachkommt, sich also seinerseits sorgfaltsgemäß verhält, z.B. eindeutige Anweisungen erteilt hat[19].

Die Verbandsgeldbußen bemessen sich in Tagsätzen und reichen, je nach Schwere der Straftat, von 40-180 Tagsätzen (§4 VbVG). Der Strafrahmen bewegt sich somit bis zu 180 Tagsätze*10.000 € = 1.800.000 €.

4.2.1.4 Datenschutzgesetz

Der Nutzer bleibt auch bei der Nutzung von Cloud-Computing für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (§10 DSG). Auch bei der Test-Verwendung von Cloud-Computing Anwendungen mit Echtdaten muss die datenschutzrechtliche Grundlage vertraglich geregelt werden. Dienstleister (d.h. Cloud-Anbieter) dürfen laut §10 DSG nur dann in Anspruch genommen werden, wenn sich der Nutzer von der sicheren und rechtmäßigen Datenverarbeitung des Cloud-Anbieters überzeugt hat. Nach Vertragsabschluss muss der Nutzer regelmäßig überprüfen, ob organisatorische und technische Schutzmaßnahmen angemessen umgesetzt werden.

[18] Vgl. Göllner, DI Johannes, MSc: Unterlagen zu Vorlesung „Einführung in Risikomanagement“.
[19] ebd.

Plichten des Cloud-Anbieters (Auszug §11 DSG)

Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

- Die Daten sind ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten.

- Alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen sind zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

- Weitere Dienstleister sind nur mit Billigung des Auftraggebers heranzuziehen und deshalb ist der Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.

- Sofern dies nach der Art der Dienstleistung in Frage kommt, sind im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen.

- Nach Beendigung der Dienstleistung sind alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten.

- Dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten. Vor allem §11 Abs. 1 Z 6 DSG verlangt, dass der Nutzer sich gegenüber dem Cloud-Anbieter vertraglich Kontrollrechte einräumen lassen muss. Kontrollen vor Ort bzgl. Datenverarbeitung und Umsetzung der Schutzmaßnahmen durch den Nutzer oder einen befugten Dritten (Auditor) müssen somit möglich sein. Darüber hinaus sollten auch Kontrollen durch Aufsichtsbehörden vertraglich geregelt werden, um eventuellen Auskunfts-, Richtigstellungs- oder Löschungspflichten nachzukommen.

Datensicherheitsmaßnahmen (§14 DSG)

Der Nutzer hat gemäß §14 DSG sicherzustellen, dass beim Cloud-Anbieter ausreichende Datensicherheitsmaßnahmen implementiert wurden. Die Überprüfung muss nicht zwingend vor Ort durchgeführt werden, sondern kann auch durch Vorlage entsprechender Zertifikate erfolgen. Die Datensicherheits-

maßnahmen müssen vertraglich als Leistungspflicht geregelt werden und konkrete, dem Schutzbedarf angepasste Maßnahmen enthalten. Bei standardisierten SaaS-Angeboten ist der Nutzer verpflichtet zu überprüfen, ob das angebotene Sicherheitskonzept den datenschutzrechtlichen Anforderungen entspricht (noch vor Auslagerung der Daten). Der Nutzer ist verpflichtet, die Überprüfungen regelmäßig, abhängig vom Schutzbedarf der Daten, durchzuführen und die Überprüfungsergebnisse zu dokumentieren.

Übermittlung und Überlassung von Daten in das Ausland

Grundsätzlich ist die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes laut §12 DSG keinen Beschränkungen unterworfen. Dies gilt allerdings nicht für Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

Keiner Genehmigung gemäß §13 DSG bedarf der Datenverkehr mit Empfängern in Drittstaaten mit angemessenen Datenschutz. Die Europäische Kommission hat folgende Staaten als sichere Drittstaaten eingestuft[20] [36]:

- Andorra
- Argentinien
- Australien
- Kanada
- Schweiz
- Färöer Inseln
- Guernsey
- Israel
- Isle of Man
- Jersey
- USA – Transfer of Air Passenger Name Record (PNR) Data
- USA – Safe-Harbor-Abkommen
- Neuseeland
- Uruguay

Darüber hinaus ist der Datenverkehr ins Ausland genehmigungsfrei, wenn[21]

- die Daten im Inland zulässig veröffentlicht wurden,
- die Daten für den Empfänger nur indirekt personenbezogen sind,
- die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind,

[20] Commission decisions on the adequacy of the protection of personal data in third countries, abrufbar unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (letzter Zugriff: 24.03.2014)

[21] Auszug §12 DSG

- Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden,
- der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat,
- ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann,
- die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden,
- die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist,
- es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt,
- Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

Soll nicht genehmigungsfreier Datenverkehr in nicht sichere Drittstaaten erfolgen, so ist die Genehmigung der österreichischen Datenschutzkommission (DSK) einzuholen.

Rückgabe von Daten

§11 Abs. 1 Z5 DSG verlangt nach Beendigung der Dienstleistung, alle Verarbeitungsergebnisse und Unterlagen dem Auftraggeber zu übergeben, in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten. Aus diesem Grund muss auch diese „Rückgabe von Daten“ vertraglich geregelt und konkret vereinbart werden (z.B. technische Umsetzung der Rückgabe in Bezug auf Übermittlungswege, Dateiformate etc.).

Verwaltungsstrafbestimmungen

Bis zu 10.000 Euro werden lt. §52 Abs. 2 DSG unter anderem folgende Verwaltungsübertretungen geahndet:

- Ermittlung, Verarbeitung oder Übermittlung von Daten ohne der Meldepflicht gemäß §§ 17 oder 50c DSG erfüllt zu haben oder Betrieb der Datenanwendung in einer von der Meldung abweichenden Weise
- Übermittlung der Daten ins Ausland, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 Abs. 1 eingeholt zu haben
- Verletzung von Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, 25 oder 50d
- Nichtimplementierung von Sicherheitsmaßnahmen gemäß § 14 und § 50a Abs. 7 und § 50b Abs. 1
- Missachtung der Löschungsfrist gemäß § 50b Abs. 2

§52 Abs. 2a DSG: Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit einer Strafe bis zu 500 Euro zu ahnden ist, wer Daten entgegen den §§ 26, 27 oder 28 nicht fristgerecht beauskunftet, richtigstellt oder löscht.

Laut der Leitfäden von EuroCloud.Austria[22] [37] sind oben angeführte Verwaltungsübertretungen, zum Beispiel eine Missachten der Meldepflichten, ein Grund für eine außerordentliche Kündigung des Vertrages mit dem Cloud-Anbieter. Der Auftraggeber kann sich in weiterer Konsequenz mitschuldig machen, wenn bekannte Verstöße nicht entsprechend überwacht bzw. vertraglich abgesichert werden.

Informationspflicht des Auftraggebers (Data Breach Notification Duty)

§ 24 Abs. 2a DSG verlangt die unverzügliche Information der Betroffenen in geeigneter Form, sobald Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

Um dieser Informationspflicht als Unternehmen nachkommen zu können, sollten entsprechende Meldepflichten mit dem Cloud-Anbieter vertraglich vereinbart werden.

4.2.1.5 Bundesabgabenordnung

Gemäß §132 Bundesabgabenordnung (BAO) sind Bücher und Aufzeichnungen sowie die zu den Büchern und Aufzeichnungen gehörigen Belege sieben Jahre aufzubewahren. Hinsichtlich Belege, Geschäftspapiere und sonstigen Unterlagen kann die Aufbewahrung auf Datenträgern geschehen, wenn die vollständige, geordnete, inhaltsgleiche und urschriftgetreue Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfrist jederzeit gewährleistet ist. Soweit solche Unterlagen nur auf Datenträgern vorliegen, entfällt das Erfordernis der urschriftgetreuen Wiedergabe. §131 BAO schreibt vor, dass Bücher und Aufzeichnungen auf Verlangen der Abgabenbehörde innerhalb angemessenen Fristen in das Inland zu erbringen sind.

Werden für BAO-relevante Bücher und Aufzeichnungen also bei Cloud-Anbietern gelagert, so ist sicherzustellen, dass entsprechende Datensicherungsmechanismen die fristgerechte Aufbewahrung der Dokumente ermöglichen. Bei ausländischen Anbietern ist des Weiteren sicherzustellen, dass die Daten innerhalb angemessener Fristen in das Inland transferiert werden können.

[22] EuroCloud.Austria: 6. Cloud Services – Vertragsbruch in der Cloud – Was tun?, S. 15, anzufordern unter: http://www.eurocloud.at/projekte/publikationen/leitfaeden.html

4.2.1.6 Umsatzsteuergesetz

§18 Abs. 8 Umsatzsteuergesetz (UStG) bestimmt, dass Bücher und Aufzeichnungen im Inland zu führen und mit zugehörigen Unterlagen im Inland aufzubewahren sind, sofern die Besteuerung von einem buchmäßigen Nachweis abhängt[23].

4.2.1.7 Strafgesetzbuch

Potenzielle Verletzungen von Berufsgeheimnissen durch Berufsgeheimnisträger wie Ärzte oder Therapeuten sind in §121 Strafgesetzbuch geregelt. Eine Verlagerung von betroffenen Daten in die Cloud ist auch aufgrund der Sensibilität der Daten im Einzelfall genau zu prüfen[24].

4.2.1.8 Bundesvergabegesetz

Im Rahmen des Bundesvergabegesetz und der aktuell bis Ende 2013 gültigen Schwellwertverordnung können Bund, Länder und Gemeinden Aufträge im Bau-, Liefer- und Dienstleistungsbereich bis zu einem Volumen von 100.000 Euro direkt an Unternehmen vergeben[25] [39]. Die in dieser Studie adressierte Zielgruppe der kleinen Behörden wird sich im Kontext der Beschaffung von SaaS-Dienstleistungen unterhalb des Schwellwerts liegen, weshalb an dieser Stelle nicht weiter auf die Anforderungen des Bundesvergabegesetzes eingegangen wird.

Spezielle datenschutzrechtliche Anforderungen (z.B. im Falle einer Behörde) könnten bedingt durch standardisierte AGB der Cloud-Service-Anbieter ein Problem darstellen (mangelnde Zugriffs- und Kontrollrechte, benachteiligende Haftung). Bei Bedarf sollten, abweichend von den AGB, auf den Kunden abgestimmte Verträge erstellt werden.

4.2.1.9 Vertragsrecht

Ein auf den Einzelfall abgestimmtes Vertragswerk ist notwendig, um datenschutzrechtliche Anforderungen sicherzustellen. Diese Verträge müssen auch für Sub-Auftragnehmer des Cloud-Service-Anbieters gelten (DSG §11) und je nach Typ der Leitung die Haftung und Gewährleistungsansprüche regeln [40][26].

4.2.1.10 Strafprozessordnung

Laut österreichischer Strafprozessordnung ist eine Sicherstellung zulässig, wenn sie aus Beweisgründen, zur Sicherung privatrechtlicher Ansprüche oder zur Sicherung der Konfiskation, des Verfalls, des

---

[23] EuroCloud.Austria: Leitfäden, anzufordern unter: http://www.eurocloud.at/projekte/publikationen/leitfaeden.html

[24] ebd.

[25] Schwellenwerte-Verordnung 2014, abrufbar unter: http://portal.wko.at/wk/format_detail.wk?angid=1&stid=628847&dstid=335 (letzter Zugriff: 24.03.2014)

[26] Vgl. Reichstädter, P., Cloud Computing Positionspapier 2011, Bundeskanzleramt Österreich, 2011.

erweiterten Verfalls oder der Entziehung erforderlich scheint (§ 110). Die Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen. In Ausnahmefällen ist die Kriminalpolizei berechtigt, Sicherstellungen von sich aus durchzuführen (§ 110 Abs. 2).

Jede Person, welche Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet, diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen (§ 111). Laut § 111 Abs. 2 ist bei Sicherstellung von auf Datenträgern gespeicherten Informationen der Zugang zu den Datenträgern zu gewähren und auf Verlangen die Daten in einem allgemein gebräuchlichen Format auszufolgen. Die Herstellung einer Sicherheitskopie muss geduldet werden.

Laut § 119 Abs. 1 sind Durchsuchungen von Orten (z.B. Gebäuden) zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sich dort Gegenstände oder Spuren befinden, die sicherzustellen oder auszuwerten sind. Die Durchsuchung erfordert in der Regel eine richterliche Bewilligung, kann aber bei Gefahr im Verzug auch ohne Bewilligung durch die Kriminalpolizei durchgeführt werden (§ 120).

§ 138 Abs. 2 regelt, dass Anbieter (§ 92 Abs. 1 Z 3 TKG) und sonstige Diensteanbieter (§§ 13, 16 und 18 Abs. 2 des E-Commerce-Gesetzes) verpflichtet sind, Auskunft über Daten einer Nachrichtenübermittlung und über Vorratsdaten zu erteilen und an einer Überwachung von Nachrichten mitzuwirken.

Jeder Auftraggeber einer Datenanwendung, deren Daten in einen Abgleich nach § 141 einbezogen werden sollen, ist verpflichtet, die Datenanwendung auf die gesuchten Merkmale hin zu durchsuchen und alle Daten, die diese Merkmale enthalten, auf einem elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat zu übermitteln (§ 143 Abs. 1). Die Verpflichtung hat die Staatsanwaltschaft dem Auftraggeber mit gesonderter Anordnung aufzutragen. Behördlicher Zugriff ist in definierten Fällen auch im Inland möglich.

Exkurs Deutschland[27] [40]: Das journalistische Privileg des Zeugnis- bzw. Auskunftsverweigerungsrechts ist in Deutschland in der Strafprozessordnung (§ 53 Abs. 1 Nr. 5 StPO), in der Zivilprozessordnung (§ 383 Abs. 1 Nr. 5 ZPO) und analog z.B. in der Abgabenordnung (§ 102 Abs. 1Z. 4 AO) geregelt. Der dort geregelte Schutz bezieht sich nicht nur auf Informanten sondern auch auf Materialien, welche ein Journalist im Zuge seiner Recherchen gesammelt und zusammengestellt hat. Sowohl Redaktionsräume als auch der private Bereich eines Journalisten sind vor staatlichem Zugriff geschützt.

Der deutsche Bundesdatenschutzbeauftragte wies allerdings darauf hin, dass der journalistische Quellenschutz sich nur auf Daten bezieht, welche sich in direktem Gewahrsam von Journalisten befindet, nicht aber für Daten, welche online bei Dritten gespeichert werden (beispielsweise Cloud-Storage-Anbieter). Aus diesem Grund wird eine Verschlüsselung der externen Daten strengstens empfohlen.

[27] Teletrust Pressemitteilung vom 22.05.2013: „Achtung, Grauzone: Journalistischer Quellenschutz bei staatlichem Zugriff auf Cloud-Speicher“, abrufbar unter:
https://www.teletrust.de/de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=564&cHash=26a2c6b48933604968775edc5aa790c1
(letzter Zugriff: 25.03.2014)

4.2.2 Europäische und internationale Rechtslage

4.2.2.1 EU-Datenschutz-Richtlinie für elektronische Kommunikation 2002/58/EG

Die EU-Datenschutz-Richtlinie für elektronische Kommunikation 2002/58/EG ergänzt die EU-Datenschutzrichtlinie 95/46/EG (siehe nächster Abschnitt) und soll die Privatsphäre sowie den freien Datenverkehr innerhalb der EU gewährleisten. Die Richtlinie wurde zuletzt durch Richtlinie 2009/136/EG aktualisiert und enthält telekommunikationsspezifische Regeln zur Verbesserung des Datenschutzes (z.B. anbieterseitige Verpflichtung zur Implementierung von Mechanismen zur Unterbindung von Abhörversuchen und Manipulation des Kommunikationsinhaltes).

Die Richtlinie, welche in Österreich im Telekommunikationsgesetz 2003 umgesetzt wurde, kommt im Cloud-Kontext dann zur Anwendung, wenn ein öffentlich verfügbarer Telekommunikationsdienst (z.B. E-Mail) über die Cloud angeboten wird.

4.2.2.2 EU Datenschutzrichtlinie 95/46/EG und EU Datenschutzverordnung (2014)[28]

In diesem Abschnitt werden die wesentlichsten Auswirkungen des Datenschutzgesetzes auf die Verwendung von Cloud-Computing im europäischen Raum, in der aktuellen Situation und in einer (möglichen) zukünftigen Gesetzgebung behandelt.

Die Diskussion der Gesetzgebung in der aktuellen Situation basiert auf der EU-Datenschutzrichtlinie. Obwohl diese nicht immer direkt anwendbar ist, garantiert sie minimale Datenschutzstandards und harmonisiert somit, zumindest in gewissem Grade, mit dem EU-Datenschutzgesetz.

Allerdings lässt sich erkennen, dass die aktuelle Richtlinie nicht mehr für die ständig wachsenden praktischen Anforderungen im Bereich Datenschutz angemessen ist. Aufgrund des Rufs nach weiterer Vereinheitlichung im Europäischen Raum wurde eine neue Datenschutzbestimmung vorgeschlagen. Obwohl die Einführung dieser Bestimmung noch nicht beschlossen ist, wird die Diskussion der Möglichkeiten als notwendig betrachtet. Allerdings muss zu diesem Zeitpunkt (Jänner 2014) beachtet werden, dass, obwohl schon viele Novellen eingeführt wurden, die einzelnen Artikel noch geändert werden können. Somit werden die Artikel der vorgeschlagenen Datenschutzrichtlinie als Indikatoren für mögliche Zukunftsvoraussagen verwendet, welche durch Daten aus weiteren Quellen validiert werden. Es sollte allerdings beachtet werden, dass keine korrekten Zukunftsvoraussagen getroffen werden können, insbesondere in Hinsicht darauf, welche Paragraphen in Zukunft eingeführt werden, und somit können die hier diskutierten Annahmen nur als mehr oder weniger fundierte Spekulationen betrachtet werden. Allerdings soll dieser Umstand nicht die Diskussion über die zukünftigen gesetzgebenden Implikationen von Cloud-Computing beeinflussen, sondern wird als notwendig betrachtet, um die aktuelle Situation zu analysieren und somit zu evaluieren, ob weitere Aktionen notwendig sind, sei es von der breiten Öffentlichkeit, Cloud-Nutzern oder auch den Cloud-Anbietern.

Das Datenschutzgesetz in den Vereinigten Staaten (in den USA als „Privacy Law“ bekannt) stammt von dem Recht ab, in Frieden und Ruhe leben zu können. Im europäischen Raum ist auch heutzutage

[28] Wir danken Herrn Stephan Varga für die umfassende Unterstützung bei der Erstellung dieses Abschnitts.

noch das bundesdeutsche Recht auf informationelle Selbstbestimmung eine der wichtigsten Quellen des Datenschutzes.

Das Datenschutzgesetz ist nur indirekt mit dem Thema IT-Sicherheit verwandt. Es bildet stattdessen die Grundlage für den Schutz von personenbezogenen Daten. Wann immer personenbezogene Daten verarbeitet werden, muss es eine Ausnahmebedingung geben, welche die für die Verarbeitung zuständige Person hierfür berechtigt. Allerdings gilt auch im Fall einer Berechtigung, dass die Person, welcher die spezifischen Daten gehören beziehungsweise zugeordnet sind, immer verschiedenste Rechte innehat, um ihre persönlichen Interessen zu schützen.

Im europäischen Raum bezweckt das Datenschutzgesetz einen minimalen Standard für Datenschutz und Vereinheitlichung. Allerdings ist auch heutzutage die Vereinheitlichung nicht abgeschlossen und nicht allgemein durchgesetzt. Zudem ist das Datenschutzgesetz nicht immer direkt anwendbar, sondern nur seine nationale Realisierung.

Die vorgeschlagene Datenschutzrichtlinie, welche eine Harmonisierung und weitere Verbesserung bewirken soll, ist derzeit in der Diskussion.

EU-Datenschutzrichtlinie (DPD) – Räumlicher Geltungsbereich

Von einer technischen Sichtweise aus haben reale Grenzen zischen Ländern und Regionen keine Auswirkung auf den Datentransfer in der Cloud. Die Anwender sind meist auch nicht über den geographischen Speicherungsort ihrer Daten informiert. [41][29] Diese Umstände führen allerdings zu dem Problem, dass es kaum möglich ist, ein Datenschutzgesetz und dessen Verbindlichkeiten anzuwenden oder auch nur Betracht zu ziehen.

Im Gegensatz zu diesem technischen Blickwinkel ist der geographische Ort, an dem die Daten verarbeitet werden, einer der fundamentalen Aspekte des Datenschutzgesetzes. Der räumliche Ort bestimmt das anzuwendende Gesetz und somit die Freiheiten und Rechte der Konsumenten und Anbieter. Während die Gesetzgebung im Europäischen Raum den internationalen Datenaustausch unterstützt (siehe unter anderem Art 1 § 2 DPD)[30], verkompliziert es den Prozess, wenn personenbezogene Daten aus dem Europäischen Wirtschaftsraum (EWR) transferiert werden sollen.

Innerhalb des EWR (und gleichermaßen in anderen Territorien) bestimmt der geographische Ort des Unternehmens, welches die Daten verarbeitet, das anzuwendende Gesetz. (siehe: „[where] the processing is carried out in the context of the activities of an establishment of the controller“, Art 4 §1 (a) DPD). Im Falle, dass ein Unternehmen in mehreren Mitgliedstaaten vertreten ist, hat jede Einrichtung die jeweilige nationale Gesetzgebung anzuwenden, in welcher sie ansässig ist. Laut Preamble 19: „[establishment] implies the effective and real exercise of activity through stable arrangements“, unabhängig von der Rechtsform.

[29] Vergleiche: Weichert, Thilo / Clementi, Lillian [Translator]. Cloud Computing & Data Privacy. Verfügbar unter https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf (2011)

[30] ebd.

Wenn das Unternehmen nicht im EWR angesiedelt ist, kann trotzdem die Gesetzgebung eines Mitgliedstaates angewandt werden, wenn Equipment aus dem Mitgliedstaat verwendet wird, außer es wird nur für den Transit verwendet („unless such equipment is used only for purposes of transit through the territory of the Community", Art 4 § 1 c DPD). Allerdings sollte beachtet werde, dass der Begriff „use of equipment" oft weit ausgelegt werden kann.

Es stellt sich die Frage, wie diese abstrakten Prinzipien in Hinblick auf Cloud-Computing angewendet werden können. Im ersten Schritt wird hierfür zwischen Cloud-Anwendern und Cloud-Anbietern unterschieden.[31] [42]

Für den Cloud-Anwender kann festgehalten werden, dass das nationale Gesetz eines Mitgliedstaates, unter der Bedingung, dass das Datenschutzgesetz eingeführt wurde, auch anwendbar für ihn ist, wenn er in diesem Staat angesiedelt ist. Falls er nicht im EWR angesiedelt ist, hat das Gesetz eines Mitgliedstaates Gültigkeit, falls ihm gehörendes Equipment in einem Mitgliedstaat verwendet wird, ausgenommen für Transit-Zwecke.

Somit muss für einen nicht zum EWR gehörigen Cloud-Anwender das nationale Gesetz eines Mitgliedstaates, welcher das Datenschutzgesetz eingeführt hat, angewandt werden, wenn Daten von ihm auf einem Server eines Cloud-Anbieters verarbeitet werden, welcher in dem Mitgliedstaat angesiedelt ist. Es hat keine Vorteile zu wissen, wo der geographische Speicherort der Daten ist. Dieses Faktum ist irrelevant im Datenschutzgesetz und dessen Haftungsspielraum. Somit kann Skalierbarkeit, welche im Generellen einer der wichtigsten Vorteile von Cloud-Computing ist, in einem Nachteil resultieren, wenn Daten in Territorien mit verschiedenen Gesetzgebungen bezüglich des Datenschutzes verteilt werden.

Aufgrund der Tatsache, dass die genaue Position, an der Daten verarbeitet werden, kaum zu bestimmen ist, wird empfohlen, dass das nationale Datenschutzgesetz anzuwenden ist, sobald Cloud-Services für Kunden aus diesem Land zur Verfügung gestellt werden.[32]

Wie für den Anwender, muss auch für den Anbieter bestimmt werden, welche Gesetzgebung anzuwenden ist, wobei Art 17 §§ 1 und 2 keinen Aufschluss auf die Rechtsprechung geben. Allerdings, laut Art 17 § 3, muss der Cloud-Anwender den Cloud-Anbieter in dem Vertrag zwischen den beiden Parteien dazu verpflichten, dass der Cloud-Anbieter sich an die Prinzipien in § 1 hält. Diese Aussage lässt darauf schließen, dass das Gesetz eines im EWR angesiedelten Cloud-Anbieters aus dem jeweiligen Mitgliedstaat angewendet wird.

Rollenverteilung: Controllers and Processors

Im Allgemeinen wird zwischen drei generellen Rollen für Cloud-Anwender und Cloud-Anbieter unterschieden: Controller, Processor und Third Party. Unter einem Controller versteht man eine Entität, welche alleine oder unterstützt durch andere, den Zweck und die Maßnahmen für die Verarbeitung von personenbezogenen Daten bestimmt (siehe Art 2 lit d DPD). Unter einem Processor versteht man

[31] Vergleiche: Borges, Georg / Brennscheidt, Kirstin. Rechtsfragen des Cloud Computing – ein Zwischenbericht. In: Borges, Georg / Brennscheidt, Kirstin. Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. S. 58 (2012)

[32] ebd., S.58 f.

die Entität, welche die eigentliche Verarbeitung der personenbezogenen Daten übernimmt (Art 2 lit e DPD). Third Parties bezeichnet alle Entitäten, welche nicht unter die Folgenden gezählt werden: die eigentliche Person (Datensubjekt), Controller, Processor und den Personen, die unter der direkten Autorität des Controllers oder des Processors autorisiert sind, die Daten zu verarbeiten (Art 2 lit f DPD).

Dem Controller unterliegt der Großteil der Verantwortlichkeit bezüglich der Pflichten gegenüber den Personen, deren Daten von den zugehörigen Processors verarbeitet werden (zum Beispiel die Benachrichtigung des Datensubjektes über dessen Rechte).

Im Falle, dass ein Controller einen Verarbeitungsauftrag an einen Processor delegiert, muss er dafür sorgen, dass die ausreichende Sicherstellung von technischen Sicherheitsmaßnahmen und organisatorischen Maßnahmen, welche die Verarbeitung leiten, vorhanden sind und diese Maßnahmen auch eingehalten werden (Art 17 § 2 DPD). Sobald der Controller die Datenverarbeitung an den Processor delegiert gilt: „provid[e] sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.“ (Art 17 § 2 DPD).

Somit übergibt der Controller keine Verantwortlichkeit an den beauftragten Processor ab, allerdings können dem Processor zusätzliche Pflichten auferlegt werden.[33] Außerdem, falls der Processor in einem Land außerhalb des EWR angesiedelt ist, unterliegt er den Regeln bezüglich des Datenaustausches.

Die Umlegung der vorgestellten Rollen auf Cloud-Computing ist nicht trivial. Das Hauptproblem ergibt sich aus dem Faktum, dass Cloud-Anwender dem Cloud-Anbieter die Kontrolle und das Mikromanagement der Daten übergeben, allerdings aus der Sicht des Datenschutzes verantwortlich und haftbar bleiben.

Es sollte beachtet werden, dass in manchen Ländern (u.a. Deutschland) dieser Artikel auf Cloud-Anbieter außerhalb des EWR nicht anwendbar ist.[34] [43]

Bei Anwendung der oben erwähnten Prinzipen müssen der Cloud-Computing-Typ und das technische Set-up beachtet werden. Im ersten Schritt trifft der typische Cloud-Anwender die Entscheidung, seine Daten in die Cloud auszulagern. Er instruiert hierbei einen Cloud-Anbieter, für welche Zwecke und wie die Daten verarbeitet werden. Allerdings kann oft auch der Cloud-Anbieter Entscheidungen im eigenen Ermessen treffen.[35] [44]

Im Allgemeinen kann angenommen werden, dass je spezifischer das angebotene Service ist, desto mehr Kontrollfunktionen vom Cloud-Anbieter ausgeübt werden können (vergleiche die Möglichkeiten eines Anbieters für Speicher- oder Verarbeitungskapazität mit denen eines Anbieters für Software as a Service). Im Speziellen wird diese Annahme durch den aktuellen Trend von großen Cloud-Anbietern unterstützt, welche auf dem Prinzip von „take it or leave it“ ihre Services anbieten.

---

[33] Weichert, Thilo / Clementi, Lillian [Translator]. Cloud Computing & Data Privacy. [41]

[34] Eckhardt, Jens. Datenschutz im „Cloud Computing“ aus Anbietersicht. In: Borges, Georg / Brennscheidt, Kirstin. Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. S. 104. (2012)

[35] Giannakaki, Maria. The EU Data Protection Directive revised: New challenges and perspectives. Verfügbar unter http://www.kalaw.gr/wmt/userfiles/papers_184-giannakaki-full_text-en-v001(2).pdf

In all diesen Fällen kann nur von Fall zu Fall entschieden werden, wer die Rolle des Controllers und wer die des Processors hat (oder ob beide als Controller beurteilt werden müssen). Jede getroffene Entscheidung, wer die Rolle des Controllers einnimmt, würde zu großer Wahrscheinlichkeit angefochten werden. Im Generellen kann angenommen werden, dass Cloud-Anbieter – während sie soviel Spielraum als möglich für ihre Entscheidungen behalten möchten – nicht die Rolle des Controllers einnehmen möchten, da es ihnen zusätzliche Pflichten aufbürden würde.[36]

Andererseits kann die Rolle des Controllers nicht direkt an den Cloud-Anwender abgegeben werden. In diesem Fall wäre er letztendlich von Rechts wegen verantwortlich, ohne dass er große Möglichkeiten hätte, praktische Instrumente zu bestimmen und die Einhaltung der technischen und organisatorischen Maßnahmen zu garantieren.[37] Diese Situation würde einen Verstoß gegen Art 17 § 2 des DPD darstellen, da Controller die Wahl des Processors hätten, welcher die ausreichenden Mittel für technische und organisatorische Maßnahmen bereitstellen kann, um die Verarbeitung durchzuführen, wobei allerdings der Controller auch garantieren muss, dass die Maßnahmen eingehalten werden.

Allerdings gibt es zwei Instanzen, in welchen ein Cloud-Anbieter die Rolle des Controllers übernehmen würde. Erstens, wenn der Cloud-Anbieter seine gesamte Plattform als ein Service anbietet, oder zweitens, wenn er die Daten des Cloud-Anwenders für verhaltensbezogene Werbung analysiert.[38]

Eine dritte Möglichkeit wäre noch, wenn der Cloud-Anbieter weder die Rolle des Controllers noch des Processors einnimmt, sondern die eines Moderators/Vermittlers, da ihm nicht immer die Einsicht in die zu verarbeitenden Daten gewährt ist (z.B. wenn die Daten verschlüsselt sind).[39] [45]

Somit stellt sich die Frage, wie das Rollenproblem in der Cloud gelöst werden könnte.

Im ersten Schritt muss klargestellt werden, dass es keine einzigartige und alleinige Lösung für jeden Cloud-Anwender geben kann. Die Anwender unterliegen den verschiedensten Auflagen des jeweiligen gültigen Datenschutzgesetzes und sie verwenden die verschiedensten Kategorien von Daten (z.B. sensible Daten). Obwohl die Problemstellung nicht darauf hinausläuft, dass für jeden einzelnen Cloud-Anwender eine individuelle Lösung gefunden werden muss, ist eine Kategorisierung von Anwendergruppen von großer Bedeutung.

Wie kann somit ein individueller Controller einen Processor wählen, welcher sicherstellen kann, dass die technischen und organisatorischen Maßnahmen ausreichend abgedeckt sind, ohne sich in Diskussionen über die individuelle Anpassung von Services zu verstricken? Und wie kann sichergestellt werden, dass diese Maßnahmen auch vom Processor eingehalten werden, ohne dass eine tägliche Kontrolle aller seine Kunden nötig ist?

Eine Möglichkeit ist durch den vermehrten Einsatz von (Datenschutz-)Zertifikaten gegeben. Anstatt über einzelne technische und organisatorische Maßnahmen zu diskutieren, könnte der Cloud-Anwender im ersten Schritt ein oder mehrere Zertifikat(e) auswählen, welche(s) für seine individuellen Verarbeitungszwecke geeignet sind. Im zweiten Schritt kann der Anwender unter den einzelnen

[36] ebd.
[37] ebd.
[38] ebd.
[39] Schelleckens, B.J.A. The European Data Protection Reform in the Light of Cloud Computing, S. 25

Cloud-Anbietern anhand des gewählten Zertifikates eine vorläufige Auswahl treffen und anhand finaler Faktoren (z.B. Preisfaktoren) den angemessensten Anbieter auswählen. Idealerweise wären die verfügbaren Zertifikate in Kategorien unterteilt, welche bestimmten Benutzergruppen entsprechen. Allerdings muss beachtet werden, dass das Angebot an Zertifikaten limitiert ist, insbesondere unter Berücksichtigung des Datenschutzes. Dennoch wäre es ein erster Schritt in die richtige Richtung.

Allerdings stellt sich hierbei noch die Frage, wie sichergestellt werden kann, dass die Einhaltung der Maßnahmen garantiert ist, auch wenn diese durch ein Zertifikat festgelegt sind. Diese Frage lässt sich heutzutage noch nicht zufriedenstellend beantworten, insbesondere da noch keine regelmäßigen und standardisierten Datenschutz-Audits etabliert sind. Anstelle von regulären Audits hat der Cloud-Anwender das Recht, die Einhaltung individuell sicherzustellen.[40]

Data Transfer

Der Transfer von Daten in ein Drittland kann nur durchgeführt werden, wenn das Drittland einen entsprechendes Mindestmaß an Schutz sicherstellen kann (Art 25 § 1 DPD).

Wenn der Controller einen Processor beauftragen möchte, muss außerdem beachtet werden, dass der Controller nicht nur die Anforderungen des Art 17 erfüllt, sondern auch die Bedingungen von Art 25 § 1 DPD.

Allerdings ist die Auswahl von Ländern außerhalb des EWR mit adäquatem Schutzniveau heutzutage noch stark limitiert. Von der Kommission sind bisher nur folgende Länder identifiziert worden: „Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the US Department of Commerce's Safe Harbor Privacy Principles“[41] [46].

Allerdings lassen neue Erkenntnisse in Deutschland darauf schließen, dass die Safe-Harbor-Prinzipien nicht ausreichend sind, um den Transfer von Daten in die USA zu erlauben, und dass somit weitere Anforderungen hierfür nötig sein müssen.[42] [47]

Im Falle, dass das betreffende Land kein ausreichendes Mindestmaß an Schutz garantieren kann, gibt es eine limitierte Anzahl von Möglichkeiten, in denen der Datentransfer trotzdem durchgeführt werden kann (Art 26 DPD):

Erstens, wenn die Einwilligung des Datensubjektes vorliegt, dass die Daten transferiert werden dürfen. Diese Einwilligung muss allerdings spezifisch für den einzelnen Transfer erfolgen, ausreichende Informationen müssen dem Datensubjekt über den Transfer bereitgestellt worden sein, und der Transfer muss frei widerruflich sein.[43] Dieser Ansatz ist somit nicht immer praktikabel.

[40] EuroCloud Austria. Leitfaden Cloud Computing. Recht, Datenschutz & Compliance (2011) [9]

[41] European Commission. Commission decisions on the adequacy of the protection of personal data in third countries. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/ (2013)

[42] Wybitul, Tim / Patzak, Andrea. Safe Harbor: More Stringent Requirements for the Transfer of Data to the USA. Available at http://www.mayerbrown.com/files/Publication/613f8a8c-4731-47d6-8509-f08934d61f84/Presentation/PublicationAttachment/352ad8f2-8e3f-44be-aae4-f9cbcb9b9157/Legal_Update_SafeHarbor_14_6.pdf

[43] Giannakaki, Maria. The EU Data Protection Directive revised: New challenges and perspectives. [44]

Zweitens, im Falle dass der Transfer als notwendig angesehen wird, zum Beispiel um die Ausführung oder den Abschluss eines Vertrages sicherzustellen. Allerdings stellt die offene und vage Natur der erforderlichen Abstimmung der Interessensgruppen eine Vielzahl von praktischen Herausforderungen dar.[44]

Im letzten Fall muss der Contoller adäquate Sicherungsmaßnahmen erbringen, in Hinblick auf Datenschutz, dem Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen, sowie hinsichtlich der Ausübung der damit verbundenen Rechte nach Art 25 § 2 DPD. In der Praxis werden hierbei die Musterklauseln der EU oder verbindliche unternehmensinterne Vorschriften angewendet.

EU-Datenschutzverordnung (GDPR) – Räumlicher Geltungsbereich

Im Gegensatz zur aktuellen Richtlinie hat die EU-Datenschutzverordnung (GDPR) einen weiteren Geltungsbereich. Die GDPR findet Anwendung bei der Verarbeitung von personenbezogenen Daten, welche im Rahmen der Tätigkeiten einer Niederlassung im europäischen Raum erfolgen. Im neuesten Entwurf dieser Verordnung wird klargestellt, dass GDPR in jedem Falle anzuwenden ist, unabhängig davon, ob die Verarbeitung im EU-Raum durchgeführt wird oder nicht (Art 3 § 1 GDPR). Allerdings gilt die GDPR auch, wenn keine Daten im EWR-Raum verarbeitet werden und nur Controller und/oder Processor im EWR-Raum niedergelassen sind/ist. Außerdem wird die GDPR auch angewendet, wenn personenbezogene Daten eines Datensubjektes aus dem EU-Raum von einem nicht in der EU niedergelassenen Controller oder Processor verarbeitet werden (Art 3 § 2 (a) GDRP). Die Voraussetzung, dass das Datensubjekt eine Zahlung zu leisten hat, gilt nicht.

Der Geltungsbereich der GDPR basiert zwar auf dem Territorialitätsprinzip, wird aber durch das Personalitätsprinzip ergänzt. Die regionale Ansiedlung der Controller und Processor verliert somit an Einfluss bei der Entscheidung der Gültigkeit des jeweiligen Gesetzes, stattdessen werden die Kunden im EWR-Raum mehr oder weniger systematisch adressiert.

Das „Anbieten von Gütern und Services“ wird von der Verordnung definiert als des Controllers Absicht, Services an Datensubjekte im EWR-Raum anzubieten. Bei Anwendung der Rechtslehre im Bereich der Schutz und Urheberrechte müssen spezifische Faktoren, zum Beispiel die Verfügungsstellung einer Webseite in einer spezifischen Sprache oder die Berechnung von Steuern in einer Region, bei der Anwendung der GDPR berücksichtigt werden.

Außerdem existiert noch eine Widersprüchlichkeit in den verschieden Entwurfsversionen und Rezitationen, bei der einerseits von dem Schutz der Datensubjekte „in der EU“ oder dem Schutz von Datensubjekten „in der EU angesiedelt“ gesprochen wird.

In manchen Umständen bleibt die Anwendbarkeit der GDPR unklar und kann auf verschiedene Weisen ausgelegt werden. Wenn weder Controller noch Processor im EWR-Raum ansässig sind, ist die Durchsetzung der Verordnung kaum möglich. Aber auch wenn die GDPR anwendbar ist, kann der Controller und/oder Processor entscheiden, dass sie nicht in die Rechtsprechung des EWR-Raums fallen möchten.

[44] ebd.

Allerdings sollte beachtet werden, dass vom Standpunkt des Datensubjektes die vorgeschlagenen Artikel eine Verbesserung der aktuellen Situation darstellen, da es Situationen gibt, in denen die GDPR durchgesetzt werden kann. Eine dieser Situation könnte sein, wenn Equipment im EWR-Raum verwendet wird und dadurch Daten transferiert werden. Durch die Schwierigkeit der praktischen Umsetzung folgt, dass diese neue Verordnung keine Paradelösung in Hinblick auf Datenschutz darstellt, da die Restriktionen nicht einfach geändert werden können, unter welchen die Artikel für Datenschutz angewandt werden können. Vom Standpunkt des Controllers und Processors besteht einer der Vorteile in der Voraussehbarkeit der neuen Bestimmungen.

Rollenverteilung: Controllers and Processors

Die Definitionen von Controller und Processor bleiben im Großen und Ganzen unverändert. Somit nehmen Cloud-Kunden (normalerweise) die Rolle des Controllers ein, während Cloud-Service-Anbieter (normalerweise) die des Processors einnehmen. Allerdings ist zu erwähnen, dass kürzlich erfolgte Gerichtsurteile nicht immer diesem Rollenmodel folgen.

Die gebührende Sorgfaltspflicht bei der Auswahl eines Processors bleibt ebenfalls in der GDPR bestehen. Allerdings umfasst die GDPR nicht nur Bestimmungen für den Controller, sondern auch für den Processor. Obwohl es keine Vielzahl von Bestimmungen sind, sollte nicht unterschätzt werden, dass auch der Processor einige Verantwortung trägt. Marchini empfiehlt, dass die Regulatoren die Verpflichtungen im Allgemeinen durchsetzen können und nicht nur bei ausdrücklich vermerkten Verpflichtungen bei dem Processor.[45] [48]

Laut Artikel 26 Absatz 4 ist „jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche."

Somit müssen Subunternehmer durch den Kunden genehmigt werden (Art 26 § 2 (d)), ob Standardklauseln in den Verträgen diese Verpflichtungen auch erfüllen, steht zur Diskussion.[46]

Dem Processor ist nur erlaubt jene Daten zu verarbeiten, für die der Controller den Auftrag hierfür gibt (oder wenn die Notwendigkeit dazu besteht, gegeben durch das EU-Recht nach Art 27 GDPR). Sie sind außerdem dazu verpflichtet, dass sie regelmäßig die Dokumentationen aktualisieren (Art 27 GDPR) und dass sie mit der Aufsichtsbehörde kooperieren müssen (Art 29 GDPR).

Der Processor ist verpflichtet, dass er im Falle einer Verletzung des Schutzes personenbezogener Daten den Controller ohne unangemessene Verzögerung benachrichtigt (Art 31 GDPR) und eine Risikoanalyse (Art 32a GDPR) sowie eine Datenschutzfolgenabschätzung (Art 33 GDPR) durchführt.

Die Bestimmungen bezüglich Datenschutzbeauftragter (z.B. Art 35 GDPR) gelten auch für „einfache" Processors von Daten. Art 11 GDPR über Transparenz, welcher „prägnante, transparente, klar formu-

[45] Marchini, Renzo. Cloud Computing Under The European Commission's Proposed Regulation To Revise The EU Data Protection Framework. In World Data Protection Report Volume 12, Number 2 (2012).

[46] ebd.

lierte und einfach zugängliche Policies definiert“, könnte eine hilfreiche Referenzquelle für Service-Anbieter darstellen, um in diesem Bereich Regelkonformität zu erreichen.

Art 27 § 2 a (c) der GDPR ermöglicht der Aufsichtsbehörde einem Unternehmen bis zu 100.000.000 Euro oder bis zu 5% des weltweiten jährlichen Geschäftsumsatzes aufzuerlegen, je nachdem, welcher Betrag höher ist. Allerdings sollte beachtet werden, dass wenn der Controller oder Processor im Besitz eines validen „European Data Protection Seal“ ist, eine solche Geldstrafe nur im Falle eines vorsätzlichen oder fahrlässigen Verstoßes verhängt werden kann (Art 27 § 2b GDPR).

Die Vorschriften für den Datentransfer bleiben im Essenziellen bestehen. Allerdings legt Marchini dar, dass der scheinbare Schwerpunkt in diesem Bereich auf Ad-hoc-Transfer (nicht auf frequentierter oder großer Datenübertragung) gelegt wurde, was im Gegensatz zu dem anhaltenden Trend des Outsourcing steht.[47]

Somit stellt sich die Frage, ob sich durch die GDPR die aktuelle Situation der Cloud-Kunden verbessert. Selbst bei Anwendung der GDPR werden Kunden weiterhin wahrscheinlich nur Standard-Verträge angeboten, die aber nicht auf spezifische Sicherheits- und Privacy-Anforderungen ausgerichtet sind.

Zusätzlich kommt hinzu, dass Geldstrafen für Verstöße wahrscheinlich kaum über ausländische Cloud-Service-Anbieter verhängt werden können.[48] Somit könnten Cloud-Kunden vollständig von den Sicherheits- und Privacymaßnahmen des Anbieters abhängig sein, allerdings wäre dann immer noch der Kunde haftbar, unabhängig vom Cloud-Service-Anbieter, gegen den die Sanktionen wahrscheinlich nicht vollstreckt werden können. In der GDPR wird außerdem nicht definiert, wie die Einhaltung mit Sicherheitsmaßnahmen zu garantieren oder wie diese Aussage auszulegen ist. Wie zuvor erwähnt würde eine ständige physikalische Kontrolle vom Kunden eine gewaltige – wenn nicht unmöglich tragbare – Belastung für den Kunden bedeuten.

Zertifizierung im Kontext der GDPR

Art 39 der GDPR beschreibt das Konzept der „Zertifizierung“, welches von besonderem Interesse im Zusammenhang mit Cloud-Computing ist. Was versteht die GDPR folglich unter „Zertifizierung“?

Während in früheren Gesetzesvorlagen die Kommission „nur fördern“ sollte, dass Datenschutz-Zertifikatsmechanismen sowie Datenschutz-Siegel und -Kennzeichen begünstigt werden, bestimmt der aktuelle Entwurf, dass Controller als auch Processor das Recht haben, von der entsprechenden Aufsichtsbehörde zertifiziert zu werden, dass die Verarbeitung von Daten gemäß dieser Verordnung durchgeführt wird (Art 39 §1a GDPR). Zusätzlich muss gemäß § 2 die Zertifizierung freiwillig und erschwinglich sein, zugänglich mithilfe eines Prozesses, welcher transparent abläuft und keine übermäßige Belastung darstellt. Das Audit kann entweder direkt von den Datenschutzbehörden durchgeführt werden, oder es können Third-Party-Auditoren von ihnen dazu bevollmächtigt werden (§ 1d GDPR).

[47] ebd.
[48] ebd.

Controller und Processor werden nach einem bestanden Audit mit einem standardisierten europäischen Datenschutz-Gütesiegel ausgezeichnet und in ein öffentliches Register eingetragen (§§1e und 1g GDPR).

Ein bestandenes Audit ist nur so lange gültig, solange der Controller oder Processor den Anforderungen in vollen Umfang entspricht, längstens jedoch fünf Jahre (§§ 1f und 1g GDPR).

Die Präambeln der Verordnung legen dar, dass die Zertifizierung Vertrauen zwischen den Datensubjekten, Rechtssicherheit für Controller und zur gleichen Zeit den Export von europäischen Datenschutzstandards ermöglichen soll, sodass Unternehmen aus Drittstaaten einen einfacheren Zugang zum europäischen Markt bekommen, indem sie eine Zertifizierung vorweisen können.

Ursprünglich wurde angestrebt, dass Datensubjekte durch die Zertifizierung von Unternehmen rasch den versicherten Datenschutzlevel einschätzen können. Allerdings hat sich anscheinend mittlerweile der Fokus von der Perspektive des Datensubjektes zu der des Controllers/Processors verschoben und das Ziel, das Vertrauen der Datensubjekte in die Contoller zu stärken tritt in den Hintergrund. Stattdessen wird anscheinend angestrebt, dass Controllers und Processors mit einer gewissen Sicherheit von den Datenschutzbehörden ihre Verarbeitungsprozesse zertifizieren lassen können.

Zusammenfassende Bemerkungen

Im Cloud-Computing werden im Grunde die näheren Einzelheiten des Datenzentrum-Managements vom Cloud-Anwender zu dem spezialisierten Cloud-Anbieter delegiert. Cloud-Anbieter profitieren insbesondere durch die Kostenersparnis durch Massenproduktion (Economy of Scale), indem sie ihre standardisierten Services einer Vielzahl von Kunden anbieten, oft unter dem Grundsatz „take it or leave it“. Beide Effekte – Spezialisierung und Standardisierung – sind Gründe für die derzeitige und anhaltende Popularität des Cloud-Computings.

Aus Sicht des Datenschutzes sind diese Vorteile allerdings zur gleichen Zeit auch Nachteile. Unter dem derzeitigen Datenschutzgesetz ist die Anwendbarkeit der Datenschutzrichtlinie großteils durch die Niederlassung, wo die Daten verarbeitet werden, bestimmt. Allerdings könnte die Datenschutzrichtlinie auch dann anwendbar sein, wenn ein Controller nicht in EWR-Raum niedergelassen ist, wenn Equipment, welches sich in einem Mitgliedstaat befindet, verwendet wird, abgesehen von ausschließlichen Transportzwecken. Bei einer breiten Auslegung dieses Statements kann auch ein Cookie als Equipment gezählt werden, wie auch in einigen Präzedenzfällen in mehreren Ländern demonstriert wurde.

Die Delegierung bezüglich des Datenmanagements wandelten sich zum Nachteil für die Cloud-Anwender, unter anderem, weil sie aus Sicht des Datenschutzes meistens dennoch verantwortlich und haftbar sind. In einigen Fällen ist die Unterscheidung zwischen Controller und Processor nicht eindeutig und je mehr Entscheidungsgewalt dem Anbieter überlassen wird, desto wahrscheinlicher wird er als Processor klassifiziert werden.

In vielen Fällen kann die Klassifizierung allerdings nur von Fall zu Fall entschieden werden. Aufgrund des „Economy of Scale“-Vorteils auf Seiten der Cloud-Anbieter sind diese abgeneigt, Services an

individuelle Bedürfnisse zu adaptieren, sondern bieten wenige und standardisierte Services an, welche an einen breiten Kundenkreis adressiert sind.

Eine Lösung für dieses Problem scheint die vermehrte Verwendung von Datenschutz-Zertifikaten zu sein. Der Cloud-Anwender könnte anhand seiner individuellen Anforderungen ein Zertifikat auswählen und dann einen passenden Service-Anbieter, welcher Services unter diesem Zertifikat zertifiziert hat.

Aus juristischer Sicht wäre es wichtig, dass regelmäßige und standardisierte Audits eine Art von Vergleichbarkeit mit den Anforderungen für Cloud-Anwender anbieten. Zusätzlich muss erwähnt werden, dass die Bestimmungen bezüglich Datentransfers beachtet werden müssen, wenn Processor nicht im EWR-Raum niedergelassen sind.

Die Datenschutzrichtlinie wird mittlerweile durch weitere Bestimmungen ergänzt, welche den räumlichen Geltungsbereich vergrößern, indem auch Fälle inkludiert werden, in welchen Services und Güter an Datensubjekte in der EU angeboten werden. Somit können auch Fälle, in denen eine Webseite in einer gewissen Sprache angeboten wird oder Steuern basierend auf einer gewissen Region berechnet werden, beachtet werden, wenn die Anwendbarkeit der GDPR bestimmt wird. Die praktischen Implikationen des erweiterten Geltungsbereiches bleiben allerdings vorerst unklar aufgrund der Tatsache, dass die Durchsetzbarkeit möglicherweise problematisch ist.

Die GDPR würde auch einige Bestimmungen beinhalten, welche an den Processor gerichtet sind und nicht nur ausschließlich an den Controller. Allerdings bleibt das fundamentale Problem der Differenzierung zwischen Controller und Processor bestehen. Außerdem würden im praktischen Sinne Controller alleinig für Datenschutzverletzungen haftbar bleiben, auch wenn sie Kontrolle abgetreten haben. Wie die Zertifizierung der GDPR schlussendlich implementiert wird, resultiert in der Tat in einer interessanten Diskussion. Der momentane Trend geht in Richtung Schaffung einer Vertrauensbasis für Controller, allerdings nicht aus der Perspektive der Datensubjekte, sondern indem die Bestimmungen geändert werden, sodass Controller nicht nur ermutigt werden, sich von der Aufsichtsbehörde zertifizieren zu lassen, sondern auch zusätzliche Rechte ihr gegenüber erhalten.

4.2.2.3 Artikel 13a der EU-Richtlinie 2009/140/EG

Die EU-.Richtlinie 2009/140/EG betreffend eines gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste regelt in Artikel 13a die Sicherheit und Integrität von elektronischen Netzen und Diensten:

- **Absatz 1:** „Die Mitgliedsstaaten stellen sicher, dass Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, angemessene technische und organisatorische Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten ergreifen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau gewährleisten, dass angesichts des bestehenden Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen für Nutzer und zusammengeschaltete Netze zu vermeiden und so gering wie möglich zu halten.“

- **Absatz 2:** „Die Mitgliedstaaten stellen sicher, dass Unternehmen die öffentliche Kommunikationsnetze bereitstellen, alle geeigneten Maßnahmen ergreifen, um die Integrität ihrer Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen."

- **Absatz 3:** „Die Mitgliedstaaten stellen sicher, dass Unternehmen die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, der zuständigen nationalen Regulierungsbehörde eine Verletzung der Sicherheit oder einen Verlust der Integrität mitteilen, die bzw. der beträchtliche Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste hatte. […]"

Die EU-weit harmonisierte Implementierung des Artikels 13a ist mit Stand Juni 2013 noch in Gange. Eine momentane Fragestellung, welche in diversen Arbeitsgruppen ausgearbeitet wird ist, inwieweit sich Artikel 13a auf Cloud-Computing im Allgemeinen oder nur auf über Cloud-Computing-Strukturen angebotene Kommunikationsdienste bezieht.

4.2.2.4 Safe-Harbor-Abkommen (USA)

Die europäische Datenschutzrichtlinie (Richtlinie 95/46/EG), wie auch das daran angelehnte österreichische Datenschutzgesetz, verbieten es grundsätzlich, personenbezogene Daten aus EU-Mitgliedsstaaten in nicht sichere Drittstaaten zu übertragen (siehe Abschnitt 4.2.1.4). Auch die USA ist aufgrund der dort geltenden Datenschutzgesetzgebung als ein nicht sicherer Drittstaat eingestuft. Das Safe Harbor-Abkommen wurde zwischen 1998 und 2000 entwickelt und ermöglicht es US-Unternehmen, welche sich diesem Abkommen unterwerfen, Daten mit EU-Mitgliedsstaaten und den darin befindlichen Unternehmen auszutauschen. US-Unternehmen verpflichten sich, die „Safe Harbor Principles" zu beachten.

Zum gegenwärtigen Zeitpunkt sind auf der Website des US-Handelsministeriums mehr als 1000 Safe–Harbor-Unternehmen gelistet[49] [49]. Darunter auch viele Cloud-Anbieter wie Dropbox, Microsoft oder Apple. Grundsätzlich unterwerfen sich Unternehmen dem Abkommen freiwillig und keine unabhängige europäische Stelle überprüft die Einhaltung der folgenden Safe Harbor Principles (Datenschutzvorschriften)[50] [50]:

- **Notice**
  Organisationen müssen ihre Kunden über den Zweck der Informationssammlung und deren Verarbeitung informieren und darüber hinaus ausreichende Kontaktmöglichkeiten für Anfragen, Beschwerden und Datenweiterleitung an potenzielle Subauftragnehmer zur Verfügung stellen. Bei Subauftragnehmern muss angegeben werden, welche Informationen an diese weitergeleitet und welche Maßnahmen bzgl. Datensicherheit umgesetzt werden.

[49] U.S.-EU Safe Harbor List, abrufbar unter: https://safeharbor.export.gov/list.aspx (letzter Zugriff: 24.03.2014)
[50] U.S.-EU Safe Harbor Overview, abrufbar unter: http://export.gov/safeharbor/eu/eg_main_018476.asp (letzter Zugriff: 24.03.2014)

- **Choice**
  Organisationen müssen ihren Kunden die Wahl lassen, ob gesammelte personenbezogene Informationen an weitere Organisationen entgegen dem ursprünglichen Sammlungszweck verbreitet werden darf (opt-out). Für sensible Informationen muss der Kunde einer Weiterleitung eindeutig zustimmen (opt-in).

- **Transfers to Third Parties**
  Neben der Berücksichtigung der Prinzipien Notice und Choice muss die Organisation bei der Weiterleitung von Daten sicherstellen, dass der Subauftragnehmer sich ebenfalls zu den Safe-Harbor-Prinzipien bekennt, der Europäischen Datenschutzgesetzgebung oder einer gleichwertigen Gesetzgebung unterliegt.

- **Access**
  Kunden muss die Möglichkeit gegeben werden, die über sie gespeicherte Informationen einsehen, ergänzen, korrigieren oder löschen zu können, sofern die Informationen nicht korrekt gespeichert sind. Davon ausgenommen sind Fälle, in welchen der Zugang unverhältnismäßig teuer oder unzweckmäßig bezüglich der dadurch entstehenden Risiken für die Privatsphäre des Kunden oder einer betroffenen dritten Person ist.

- **Security**
  Organisationen müssen zweckmäßige Vorkehrungen für den Schutz (Verlust, Missbrauch, unautorisierter Zugang, unautorisierte Veröffentlichung, unbefugte Änderung und Zerstörung) der personenbezogenen Daten treffen.

- **Data Integrity**
  Personenbezogene Informationen müssen für den jeweiligen Verarbeitungszweck relevant sein. Die Organisation muss sicherstellen, dass die verwendeten Informationen zweckmäßig, genau, vollständig und aktuell sind.

- **Enforcement**
  Um die Einhaltung der Safe-Habor-Prinzipien sicherzustellen, müssen folgende Maßnahmen umgesetzt sein: (a) verfügbare unabhängige Mechanismen, um die von Kunden eingebrachten Beschwerden und Missstände zu untersuchen und zu lösen bzw. entstandene Schäden anzuerkennen, (b) Mechanismen, um die Implementierung der Safe-Harbor-Prinzipien zu verifizieren und (c) Verpflichtung, die durch Verletzung der Safe-Harbor-Prinzipien verursachten (kundenseitigen) Probleme zu lösen. Sanktionen müssen in einer ausreichenden Höhe definiert werden, um bei teilnehmenden Organisationen Safe Harbor Compliance sicherzustellen. Organisationen, welche keine jährliche Safe-Harbor-Selbstzertifizierung ausstellen, werden von der Liste teilnehmender Organisationen gestrichen. Grundsätzlich wird das zwischen Europäischer Union und USA abgeschlossene Abkommen gemäß US-Gesetzgebung durchgesetzt.

Laut Beschluss des Düsseldorfer Kreises (informelle Vereinigung der obersten deutschen Aufsichtsbehörden zur Überwachung des Datenschutzes im privatwirtschaftlichen Bereich) vom 28.4.2010[51] [51] muss die Einhaltung des Datenschutzniveaus bei Verarbeitung von personenbezogenen Daten bei einem im US-amerikanischen Rechtsraum befindlichen Unternehmen wie folgt geprüft werden:

- schriftlicher Nachweis über den Beitritt zum Abkommen
- Nachweis über die Einhaltung der Informationspflichten des Unternehmens gegenüber den Betroffenen der Datenverarbeitung

Die Überprüfung kann durch Dritte oder beauftragte Unternehmen vor Ort durchgeführt werden und sollte in regelmäßigen Abständen erfolgen (z.B. jährlich).

4.2.2.5 Patriot Act (USA)

Der US Patriot Act (Abkürzung für „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001“) wurde im Oktober 2001 als Reaktion auf die Terroranschläge des 11. Septembers 2001 vom US-amerikanischen Gesetzgeber verabschiedet. Die Aussagen eines englischen Microsoft-Managers im Zuge einer Startveranstaltung des Cloud-Dienst Office365 im Juni 2011 zeigten, dass US-amerikanische Unternehmen auf Basis des US Patriot Acts zur Herausgabe europäischer Daten verpflichtet sind, auch wenn diese ausschließlich auf europäischen Boden gespeichert werden[52] [52]. Im Gegensatz zur europäischen Datenschutzgesetzgebung und zum Safe-Harbor-Abkommen muss der Betroffene über diese Datenweitergabe auch nicht informiert werden, wenn diese Benachrichtigung von der US-Sicherheitsbehörde auf Basis eines „National Security Letter“ oder „Gag Order“ verboten wäre[53] [53]. Der US Patriot Act trifft darüber hinaus nicht nur US-Unternehmen, sondern auch europäische Unternehmen, welche in einem Eigentumsverhältnis zu einem US-Unternehmen stehen, sonstige Konzernverflechtungen zu US-Unternehmen aufweisen oder irgendeine Form der Niederlassung in den USA unterhalten.

Voraussetzung für die Erlangung der Daten ist die Bestätigung durch das Office of International Affairs (OIA) und die dringende Notwendigkeit des Beweises sowie eine Wahrscheinlichkeit, dass andere Erhebungsmethoden erfolglos sein werden. Neben dem Patriot Act können auch andere Bestimmungen wie der Foreign Intelligence Surveillance Act[54] [54] die Vertraulichkeit europäischer personenbezogener Datenbestände gefährden. Genau aus diesem Grund nehmen immer mehr europäische Anwender von der Verwendung US-basierter Cloud-Dienste Abstand (beispielsweise die niederländische

51 Beschluss des Düsseldorfer Kreises am 28./29. April 2010. Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html (letzter Zugriff: 24.03.2014)

52 Microsoft admits Patriot Act can access EU-based cloud data,, abrufbar unter: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225 (letzter Zugriff: 24.03.2014)

53 Inanspruchnahme des Patriot Acts und anderer US-rechtlicher Regelungen zur Beschaffung von personenbezogenen Daten aus dem Raum der Europäischen Union durch US-Behörden abrufbar unter: https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html (letzter Zugriff: 24.03.2014)

54 50C36, abrufbar unter: http://uscode.house.gov/download/pls/50C36.txt (letzter Zugriff: 24.03.2014)

Regierung[55]) [55]. Rechtlich sind die sich entgegenstehenden amerikanischen und europäischen Bestimmungen noch nicht eindeutig geklärt.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein empfiehlt daher in Cloud-Computing-Verträgen ein explizites Verbot der Herausgabe von Daten an US-Behörden in Verbindung mit dementsprechenden Verwaltungsstrafen zu vereinbaren.

An dieser Stelle ist allerdings anzumerken, dass die Herausgabe von Daten nicht auf den US-Rechtsraum beschränkt ist. Auch in anderen Industriestaaten wie zum Beispiel Australien, Kanada, Frankreich, Deutschland, Irland, Japan oder England können die in diesen Staaten zuständigen Behörden die Herausgabe von Daten fordern und erzwingen[56] [56].

4.3 Betriebswirtschaftliche Grundlagen

Cloud-Computing kann sowohl kleine, mittlere als auch große Organisationen bei der Erreichung ihrer Ziele unterstützen[57,58] [57] [58]. Während für große Organisationen Cloud-Computing und im Speziellen private und hybride Clouds keine neuen Themen sind, sind kleine und mittlere Organisationen erst seit einigen Jahren mit den Chancen und Risiken von Cloud-Computing konfrontiert[59] [59]. In Zeiten stetig steigenden Wettbewerbsdrucks ermöglicht es Cloud-Computing kleinen und mittleren Organisationen, ihre organisationsinternen Abläufe und IT-gestützten Prozesse effizienter zu betreiben. Folgende Cloud-Computing-Anwendungen sind unter anderen für kleine und mittlere Organisationen von Relevanz:

- E-Mail
- Instant Messaging
- Video- und Audio-Conferencing
- geteilte Kalender
- geteilter Speicherplatz
- Datensicherung und Datenarchivierung
- Synchronisation zu mobilen Geräten
- Textverarbeitung und Tabellenkalkulation
- Personalverwaltung
- Abrechnung und Rechnungserstellung
- Projektmanagement
- Customer Relationship Management (CRM)
- Content Management Systeme (CMS)

---

[55] Dutch government to ban U.S. providers over Patriot Act concerns, abrufbar unter: http://www.zdnet.com/blog/btl/dutch-government-to-ban-u-s-providers-over-patriot-act-concerns/58342 (letzter Zugriff: 24.03.2014)

[56] Hogan Lovells' Revealing Study About Governmental Access to Data in the Cloud Detailed in White Paper Released at Brussels Program, abrufbar unter: http://www.hoganlovells.com/hogan-lovells-revealing-study-about-governmental-access-to-data-in-the-cloud-detailed-in-white-paper-released-at-brussels-program-05-23-2012/ (letzter Zugriff: 24.03.2014)

[57] Staten, James. Is Cloud Computing Ready For The Enterprise? Forrester Research, Inc, 2008.

[58] Aljabre, Abdulaziz. Cloud Computing for Increased Business Value. International Journal of Business and Social Science Vol. 3 No. 1; January 2012.

[59] Chorafas N. Dimitris. Cloud Computing Strategies. CRC Press, 2011.

- Zeiterfassungssysteme
- Personalgeschäftsprozessunterstützung (z.B. Urlaubsanträge)
- Enterprise Resource Planning (ERP)
- Dokumentenmanagementsysteme (DMS)
- Softwareentwicklungswerkzeuge
- Produktivitätswerkzeuge (To-do-Listen, Notizanwendungen etc.)
- Virtuelle Server
- Sicherheitsdienstleistungen (E-Mail-Filter, SPAM-Abwehr, Verschlüsslung etc.)

Organisationen sollten vor dem Einsatz von Cloud-Computing dessen Wirtschaftlichkeit im organisationsspezifischen Kontext bewerten. Bei der Wirtschaftlichkeit von Cloud-Computing spielen folgende Faktoren eine wesentliche Rolle[60] [60]:

- Mehrbenutzerumgebung
- Skalierbarkeit und Flexibilität
- Time to Value/Time to Market
- Zugang zu neuen Technologien
- laufende variable Kosten statt einmaliger fixer Investitionskosten
- Energieeffizienz
- Systemredundanz und Datensicherung

Mehrbenutzerumgebung

In Cloud-Computing-Umgebungen teilen sich mehrere Benutzer die zugrunde liegende Infrastruktur. Dadurch teilen sich diese Benutzer laufende Kosten wie Lizenzkosten für Betriebssysteme und Datenbanken und auch Patches und Updates müssen für alle Benutzer nur einmal eingespielt und verwaltet werden. Da die Funktionalität auf dem Server und über das Netzwerk an den Kunden ausgeliefert wird, sind keine Client-seitigen Updates notwendig. Overheadkosten wie Sicherheit, Wartung oder Kühlung werden zwischen den Benutzern aufgeteilt und zusätzliche Einsparungen können über den Kauf größerer Mengen (beispielsweise Software oder Rechenzentrenkapazitäten) erzielt werden.

Skalierbarkeit und Flexibilität

Studienergebnisse haben gezeigt, dass Organisationen die Flexibilität von Cloud-Anwendungen wichtiger sind als unmittelbare Kosteneinsparungen[61] [61]. Da Cloud-Computing nach der tatsächlichen Verwendung abgerechnet wird, können beispielsweise veränderte Zugriffsvolumina (z.B. beim Start und anschließendem Wachstum einer Website) kosteneffizient bedient werden. Ein weiteres Beispiel wären saisonbedingte Schwankungen beim Bedarf der Rechenkapazität (z.B. Weihnachten). Abbildung 3 zeigt die notwendige Dimensionierung eines traditionellen Rechenzentrums. Die Rechenkapa-

[60] Metzger, Christian; Reitz, Thorsten; Villar Juan. Cloud Computing Chancen und Risiken aus technischer und unternehmerischer Sicht. München: Carl Hanser Verlag München, 2011.

[61] Anwendungspotenziale von Cloud Computing im Handel, abrufbar unter: http://winfwiki.wifom.de/index.php/Anwendungspotenziale_von_Cloud_Computing_im_Handel (letzter Zugriff: 24.03.2014)

zität muss über der vorhersagbaren Spitzenlast liegen. Dies hat zur Folge, dass Rechenkapazitäten außerhalb von Spitzenlastzeiten ungenutzt bereitgestellt werden müssen. Abbildung 4 zeigt hingegen die Dimensionierung von cloud-gestützten Rechenzentren. Rechenleistung wird bei Bedarf von Cloud-Computing-Anbietern zugekauft, womit unnötige Überdimensionierungen und Kosten vermieden werden.

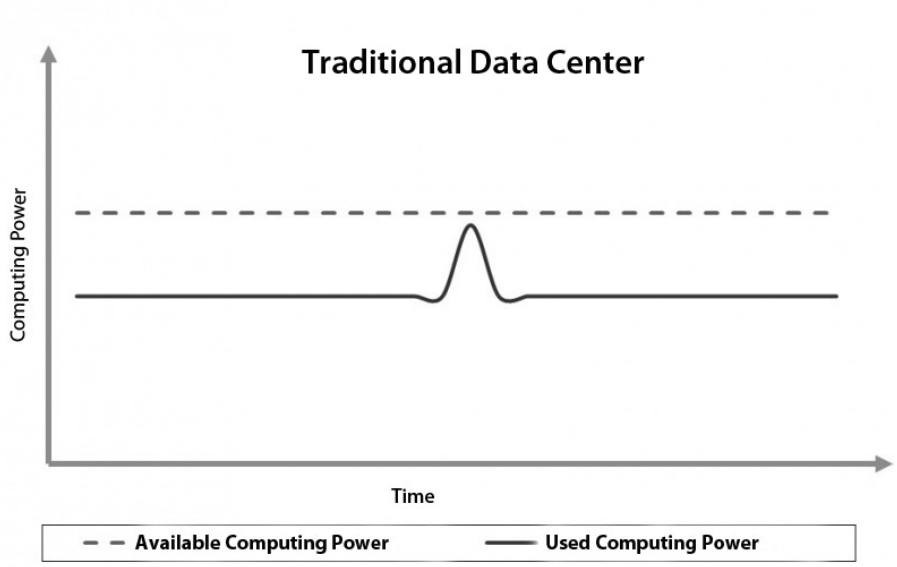

Abbildung 3: Dimensionierung traditioneller Rechenzentren[62]

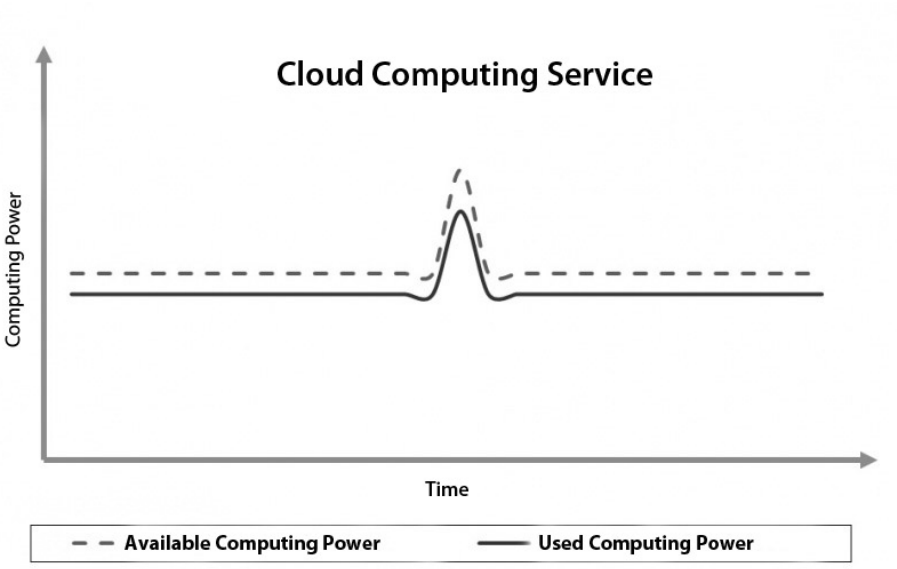

Abbildung 4: Dimensionierung Cloud-unterstützer Rechenzentren[63]

Time to Value/Time to Market

Die meisten Cloud-Computing-Angebote sind sofort nach Registrierung für den Kunden verfügbar. Aufwändiger Kauf und Installation von Hard- und Software sowie Systemkonfigurationen sind in der

[62] ebd.
[63] ebd.

Regel nicht erforderlich. Anpassungen können schneller vorgenommen werden und das Deployment beim Benutzer erfordert durch die Web-basierte Architektur in der Regel nur einen Browser und die Übermittlung der entsprechenden URL.

Zugang zu neuen Technologien

Speziell kleine und mittlere Organisationen beschaffen ihre IT-Infrastruktur nur in längeren Zyklen und haben somit nicht immer Zugang zu neuester Technologie (z.B. energieeffizienten Rechnern). Durch Cloud-Computing und die externe Verwaltung der Rechnerressourcen haben auch kleinstrukturierte Organisationen die Möglichkeit an neuer Technologie zu partizipieren und diese ihren Kunden und Mitarbeitern zur Verfügung zu stellen[64] [62].

Laufende variable Kosten statt einmaliger fixer Investitionskosten

Bei Cloud-Computing sind in der Regel folgende Kostenarten mit der Entrichtung der Servicegebühr abgedeckt[65]:

- Kosten des Serverbetriebs (Hardware, Betriebssystem, Energie, Gebäudekosten, Personal etc.)
- Lizenzkosten der Softwareapplikationen
- Updates bestehender Software
- Wartung

Traditionelle IT Deployments sind hingegen mit hohen Investitionskosten und erheblichen Planungsaufwand verbunden und erfordern somit längere Vorlaufzeiten als die Anschaffung von Cloud-Services. Zusätzlich müssen traditionelle Umgebungen für die zu erwartende Spitzenlast dimensioniert werden und ziehen somit neben hohen Initialkosten auch höhere laufende Kosten nach sich.

Energieeffizienz

Die Auslagerung von Rechenleistung an Cloud-Service-Anbieter bringt für kleine und mittlere Organisationen Energieeinsparungen aufgrund der nicht mehr benötigten Rechner. Zwar werden Energiekosten als Teil der Cloud-Computing-Kosten fällig, jedoch sind diese nur nach Bedarf zu entrichten. Der Betrieb aufwändiger Kühl- und Rechnersysteme im eigenen Haus entfällt somit[66] [63].

Systemredundanz und Datensicherung

Speziell kleine und mittlere Organisationen haben oft keine angemessenen Sicherheitsmaßnahmen bzgl. Ausfalls von Rechnersystemen und Datenverlust implementiert[67] [64]. Cloud-Computing bietet

[64] Gonzalez, Reyes; Gasco, Jose; Llopis, Juan. Information systems outsourcing reasons and risks: a new assessment. In: Industrial Management & Data Systems.

[65] vgl. Metzger et al. [60]

[66] Antonopoulos, Nick; Gillam. Lee. Cloud Computing Principles, Systems and Applications. Springer-Verlag, London. 2010.

[67] Vgl. DaMon Studie 2012

eine kosteneffiziente Möglichkeit, sowohl Hardwarefehlern als auch lokale Bedrohungen (z.B. Naturkatastrophen) entsprechend zu begegnen. Es ist jedoch zu beachten, den Cloud-Service-Anbieter hinsichtlich der Angemessenheit der von ihm getätigten Sicherheitsmaßnahmen zu überzeugen.

4.3.1 Service Level Agreements

Service Level Agreements (SLAs) werden im Bereich des Cloud-Computings zur Definition und Vereinbarung von Qualitätskriterien (zumeist bzgl. Verfügbarkeit) der angebotenen Dienste verwendet. Vom Anbieter wird ein bestimmter Verfügbarkeitsgrad (z.B. 99,9%) garantiert und Unterschreitungen können abhängig vom konkreten Vertragsmodell in Form von Pönalezahlungen rückerstattet werden. Der SLA-Detailgrad unterscheidet sich von Anbieter zu Anbieter und speziell die zeitliche Basis für den versprochenen Verfügbarkeitsgrad kann stark variieren. Während 99% Verfügbarkeit pro Jahr Ausfälle von mehreren aufeinanderfolgenden Tagen erlaubt, erlaubt eine 99%ige Verfügbarkeit auf monatlicher Basis lediglich 0,3 Tage andauernde Ausfälle pro Monat. Die Kernpunkte eines jeden Service Level Agreements sind[68] [65]:

- **Service-Level-Parameter** beschreiben eine messbare Eigenschaft des Services.
- **Metrik** beschreibt, anhand welcher Metrik die Service-Level-Parameter gemessen werden.
- **Funktion** beschreibt, anhand welcher Funktion Service-Level-Parameter berechnet werden.

Der Lebenszyklus einer SLA umfasst folgende fünf Phasen:

1. **Vertragsdefinition:** Meist basierend auf Standardvorlagen, welche vom Cloud-Service-Anbieter an die eigenen Bedingungen angepasst werden.

2. **Veröffentlichung:** Die SLA wird veröffentlicht und wird nach Entdeckung durch den Kunden zu anderen Anbietern verglichen.

3. **Verhandlung:** Im Fall von Standardanwendungen erfolgt dieser Schritt automatisch und ist speziell bei größeren Anbietern selten oder nur sehr eingeschränkt verhandelbar. Im Fall von individualisierten Lösungen werden die genauen SLA Spezifikationen zwischen Anbieter und Kunden verhandelt.

4. **Operationalisierung:** Diese Phase beinhaltet SLA Monitoring (Parameterwerte werden gemessen, Metriken werden basierend auf den Parameterwerten berechnet und Abweichungen dargestellt), SLA Accounting (Compliance, Reporting, eventuell anfallende Pönalezahlungen) und SLA Enforcement (Durchsetzung der SLA bei Nichteinhaltung).

[68] Buyya, Rajikumar; Broberg, James; Goscinski, Andrzej. CLOUD COMPUTING Principles and Paradigms. Hoboken, NJ 07030, USA: John Wiley & Sons, Inc., 2011.

5. **Dekommissionierung:** Beschreibt die Außerkraftsetzung der SLA aufgrund einer Beendigung des Vertragsverhältnisses zwischen Kunde und Anbieter. Unter welchen Umständen das Vertragsverhältnis beendet werden kann, ist im dementsprechenden Vertrag genau zu regeln.

Beispielhafte Service Level Agreements

Im Kontext von SaaS-Angeboten existieren unter anderem Infrastruktur-SLAs (z.B. Netzwerkkonnektivität, Stromversorgung oder Verfügbarkeit von Hardware) und Anwendungs-SLAs (z.B. Website Response Time oder Latenz der Datenbank).

Beispiel Infrastruktur SLA:

- **Hardware Verfügbarkeit:** 99% innerhalb eines Kalendermonats
- **Stromversorgung:** 99,99% innerhalb eines Kalendermonats
- **Netzwerkanbindung Rechenzentrum:** 99,99% innerhalb eines Kalendermonats
- **Backbone Netzwerkanbindung:** 99,999% innerhalb eines Kalendermonats
- **Pönale für Nichtverfügbarkeit:** Refundierung der Service-Kosten innerhalb der Störungszeit
- **Ausfallsverständigungsgarantie:** innerhalb einer Stunde ab Beginn eines Totalausfalls
- **Latenzzeiten:** nicht über 60ms zum nächsten Upstream-Anbieter
- **Paketverlust:** nicht über 1% innerhalb eines Kalendermonats

Beispiel Anwendung SLA:

- **Service-Level-Parameter**
  - Website Response Time (max. 3,5 Sek. pro Abfrage)
  - Web-Server-Latenz (max. 0,2 Sek. pro Abfrage)
  - Datenbank-Latenz (max. 0,5 Sek. pro Abfrage)

- **Funktion**
  - Durchschnittliche Web-Server-Latenz = Summe aller Web-Server-Latenz-Messungen dividiert durch die Anzahl der Messungen
  - Website Response Time = durchschnittliche Latenz des Webservers plus durchschnittliche Datenbank-Latenzzeit

- **Veröffentlichung der Messungen**
  - Datenbank-Latenz: http://mgmtserver/db/latency
  - Web-Server-Latenz: http://mgmtserver/ws/instanceno/latency

- **Service-Level-Ziel**
  - Sicherstellung der vereinbarten Qualitätsziele
  - Website-Latenz unter 1 Sekunde, wenn unter 1.000 gleichzeitige Zugriffe

- **Pönale**
    - 1.000,- Euro für jede Minute Überschreitung der in der SLA definierten Ziele

Typische Probleme in Service Level Agreements[69] [66]

- **Datenverschlüsselung:** Hier ist genau zu prüfen, ob und in welchem Umfang die Datenverschlüsselung im Vertrag geregelt ist. Welche Daten (Logdaten, Backupdaten, Produktivdaten, Testdaten, Metadaten etc.) sind mit welchen Verschlüsselungsmethoden verschlüsselt? Wer hat unter welchen Umständen Zugang zu den Schlüsseln?

- **Verschlüsselung am Transportweg:** Die Übermittlung von Daten zwischen Kunden und Cloud-Computing-Anbieter sollte verschlüsselt erfolgen. Aus diesem Grund muss vertraglich vereinbart werden, welche Art der Verschlüsselung unter welchen Vorrausetzungen zu Einsatz kommt, um ein Ausspähen der Daten am Transportweg zu verhindern.

- **Exit-Szenarien:** Der Vertrag sollte mögliche Beendigungsgründe und Exit-Prozeduren exakt definieren:
    - Löschung von Daten von allen Systemen des Cloud-Service-Anbieters und eventuell beteiligter Subunternehmen
    - Die Löschung sollte mithilfe von Techniken erfolgen, welche eine Wiederherstellung unmöglich machen.
    - Beim Cloud-Service-Anbieter gespeicherte Daten sollten vor Löschung in einem geeigneten Format an den Kunden zurückgegeben werden.
    - Beim Einsatz von Verschlüsselung muss die Übergabe der Schlüssel geregelt werden.
    - Definition einer festen Zeitspanne innerhalb welcher die Rückgabe der Daten abgeschlossen sein muss.

- **Messbarkeit des Sicherheitsniveaus:** Eine Möglichkeit, um ein gewisses Sicherheitsniveau vertraglich zu vereinbaren ist, Sicherheitszertifikate nach ISO 27001 oder EuroCloud Star Audit SaaS zum Vertragsbestandteil zu machen. Dies stellt sicher, dass der Cloud-Service-Anbieter bestimmte IT-Sicherheitsanforderungen erfüllt.

- **Evaluierung der technischen Machbarkeit:** Dem Kunden sollte es vertraglich ermöglicht werden, die zugesagten Sicherheitsmaßnahmen vor Ort durch sich selbst oder durch Dritte überprüfen lassen zu können.

[69] Cloud Computing und Vertragsgestaltung, abrufbar unter: http://www.business-cloud.de/cloud-computing-und-vertragsgestaltung/ (letzter Zugriff: 24.03.2014)

4.3.2 Abrechnungs- und Preismodelle

Höllwarth (2012)[70] [67] unterscheidet folgende Abrechnungsmodelle innerhalb der momentan angebotenen Cloud-Computing-Produkte:

- **kostenlos**
  - Einstiegsservice für private Nutzer
  - normalerweise mit eingeschränkter Funktionalität
  - Daten können möglicherweise für andere Zwecke (z.B. Marketing) verwendet werden (Prüfung der AGB erforderlich!)
  - normalerweise über Werbung finanziert
  - Upgrade auf Pro-Version möglich, aber kostenpflichtig

- **pro Nutzer**
  - namensgebundene Accounts (z.B. über E-Mail-Konto)
  - häufig rollenbasiertes Zugriffsmanagement

- **pro Volumen**
  - Abrechnung erfolgt über tatsächlich in Anspruch genommene Ressourcen (z.B. Speicher, Anzahl der Transaktionen etc.).
  - Verwendung üblicherweise für sich stark verändernde Ressourcenansprüche

Zur Kostenabschätzung der Cloud-Computing–Angebote im SaaS-Bereich sind unter anderen, folgende Parameter erforderlich:

- Anzahl der Nutzer
- benötigter Speicherplatz für Dateien, E-Mails etc.
- erwarteter Datenfluss vom und zum Cloud-Computing-Anbieter

Cloud-Computing Produkte werden sowohl zu fixen als auch zu variablen Preismodellen angeboten:

Fixes Preismodell

Vor allem bei SaaS-Angeboten werden fixe Preismodelle verwendet, um bestmögliche Planbarkeit für den Kunden zu erreichen[71] [68]. Meistens werden die Kosten monatlich für eine limitierte Anzahl von Benutzern angegeben. Alle mit der Leistung verbundenen Kosten (Bandbreite, Rechenkapazität etc.) sind in den monatlichen Fixpreisen enthalten und erlauben es somit dem Kunden, basierend auf dessen voraussichtlicher Nutzerzahl, die Kosten genau abzuschätzen. Wächst die Nutzerzahl über das im je-

[70] Höllwarth, Tobias, Cloud Migration. German Edition, Heidelberg, München, Landsberg, Frechen, Hamburg, Huethig Jehle Rehm GmbH, 2012.

[71] Meir-Huber, Mario. Cloud Computing, Praxisratgeber und Einstiegsstrategien. Frankfurt am Main, Software & Support Media GmbH, 2011.

weiligen Paket definierte Limit, so können erweiterte Pakete mit meist minimalem administrativem Mehraufwand zugekauft werden.

Variables Preismodell

Variable Preismodelle finden häufig in der PaaS- und IaaS-Domäne Anwendung. Die Leistungen können unter anderem nach folgenden Kostenarten abgerechnet werden:

- Rechenstunden: Die Abrechnung erfolgt nach den konsumierten Rechenleistungen in Stunden.
- Eingehender und ausgehender Netzwerkverkehr: Der durch die eigene Applikation verursachte ein- und ausgehende Netzwerkverkehr wird als Abrechnungsgrundlage verwendet.
- Speichermenge: Die Größe der beim Cloud-Service-Anbieter gelagerten Datenbestände ist Abrechnungsgrundlage (sehr oft in GB-Schritten angegeben).
- Speichertransaktionen: Kosten fallen an, wenn Speicheroperationen wie „Erstellen“ oder „Ändern“ durchgeführt werden (meistens in Einheiten von 1.000-10.000 Transaktionen abgerechnet). Löschoperationen sind bei manchen Anbietern mit keinen Kosten verbunden.
- Sonstige Aktivitäten: Ausführung von sonstigen Aktivitäten, zum Beispiel das regelmäßige Ausführen von Aufgaben in Form von Cronjobs oder das Senden von E-Mails.

Hybride Preismodelle

Neben Preismodellen, welche fixe und variable Bestandteile mischen, sind auch Nachfrage-abhängige Preismodelle verfügbar. Je mehr Kunden des Cloud-Service-Anbieters gleichartige Leistungen zur gleichen Zeit anfordern, umso teurer wird es für den einzelnen Kunden. Häufig sind solche Preismodelle mit Auktionen verknüpft, bei welchen die Kunden Maximalpreise setzen können.

4.3.3 TCO – Total Cost of Ownership

Die ökonomische Evaluierung von Cloud-Service-Angeboten im Vergleich zu inhouse Client/Server-Lösungen ist ein zentrales Entscheidungskriterium für kleine und mittlere Organisationen. Dieser Abschnitt vergleicht anhand der Methode „Total Cost of Ownership (TCO)“ beide Varianten und gibt anschließend ein Praxisbeispiel für gängige SaaS-Lösungen.

TCO berücksichtigt Kosten über den gesamten Applikationslebenszyklus für: Hard- und Softwarebeschaffung, Management und Support, Kommunikation, Endverbraucher-Ausgaben, Opportunitätskosten bei Ausfall, Training und weiteren Produktivitätsverlusten. TCO wird in vier Schritten durchgeführt:

1. Definition des Geschäftsfalls: Welche Ziele sollen mit der Anwendung erreicht werden?
2. Einholung von Angeboten alternativer Produkte: Implementierungskosten, Betriebskosten und Rollout-Kosten sollten berücksichtigt werden.

3. Identifikation und Aufschlüsselung der Kostenarten: Ziel ist es, die Kosten eines jeden erhaltenen Angebots in einer normalisierten Form zwecks Vergleichbarkeit aufzustellen. Zum Beispiel in Bezug auf die Kategorien Anwendung, Server, Implementierung, Support, andere Kosten.
4. Identifikation der Zahlungstermine. Wann fallen welche Kosten an?

Tabelle 2 zeigt beispielhaft die Umsetzung der TCO-Methode im Zusammenhang mit zwei Varianten eines CRM-Systems.

Tabelle 2: TCO Beispiel: CRM Lösung

Kosten	Bemerkung	Client-Server	Cloud-Computing
1. Anwendung			
a) Lizenzen	Lizenzen für CRM-Module und zusätzlich benötigte Produkte	✔	
b) monatliche Gebühr	monatliche Zahlungen für die Verwendung des Cloud-Computing-Angebots		✔
c) Wartung	Wartungskosten, üblicherweise 15%-25% der Lizenzkosten	✔	
2. Server			
a) Hardware	Hardwarekosten des Servers	✔	
b) Lizenzen	Lizenzkosten für Datenbanken, Betriebssystem, Security Tools etc.	✔	
c) Wartung	15%-25% der Lizenzpreise	✔	
d) Backup	Kosten des Backup-Mechanismus	✔	
e) Betriebskosten	Miete, Energie, Personal, Wartung	✔	
3. Implementierung			
a) interne Kosten	Schnittstellen, Adaptionen	✔	✔

b)	externe Kosten	Anpassungen an organisationsspezifische Gegebenheiten	✔	✔
c)	Trainings	Trainingskosten (Reisekosten, Unterlagen etc.)	✔	
d)	Deployment	Kosten für das Deployment: In der Client/Server-Variante müssen alle Client-Computer dementsprechend konfiguriert werden.	✔	
4.	**Support**			
a)	Administrator		✔	✔
b)	Hotfixes, Service-Packs	einspielen und testen von Updates	✔	
c)	Release - Change	Anpassungen im laufenden Betrieb	✔	✔
d)	User Support		✔	✔
5.	**Andere Kosten**			
a)	zusätzlicher Speicherplatz			✔
b)	zusätzliche Transaktionen			✔
c)	Finanzierungskosten		✔	

Nach Identifikation und Zuweisung aller Kostenarten wird für jede Kostenart deren Fälligkeit identifiziert und im zeitlichen Verlauf dargestellt. Abbildung 5 zeigt eine beispielhafte Abbildung eines solchen Kostenverlaufs und lässt erkennen, dass die Anfangskosten der inhouse Client/Server-Variante deutlich über der Cloud-Computing-Variante liegen.

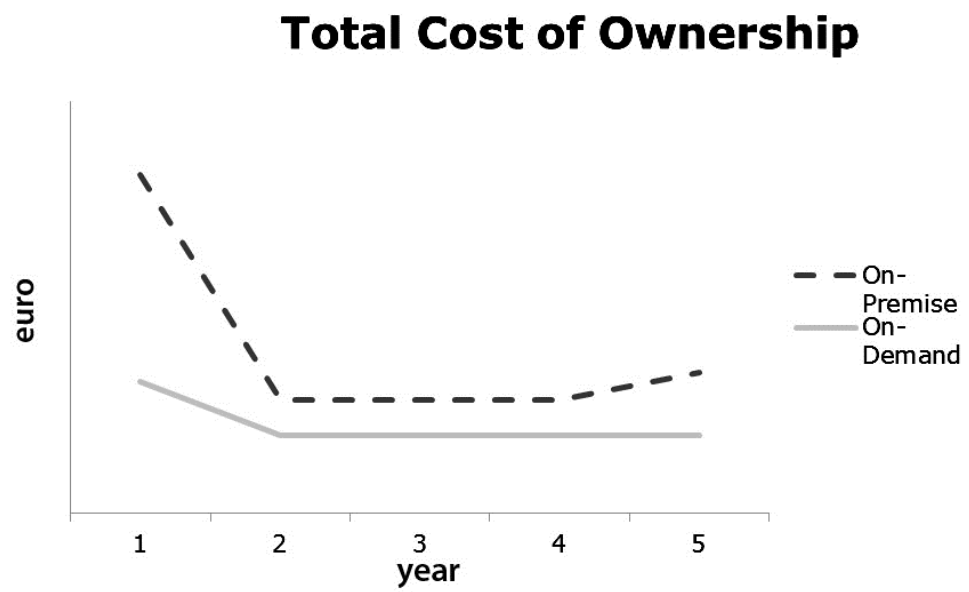

Abbildung 5: TCO - Kostenverlauf einer inhouse Client/Server- und Cloud-Computing-Variante

Beispielhafter Kostenvergleich

In diesem Abschnitt werden, basierend auf der eingeführten TCO-Methode, die Einsparungspotenziale von SaaS-Lösungen in Cloud-Computing anhand von Beispielen verdeutlicht.

- **Lizenzen, Wartungskosten versus monatlicher Gebühren**

Eine typische Client/Server-Lösung wird mit einmaligen Lizenzkosten gekauft und anschließend mit jährlichen Wartungskosten in der Höhe von 15%-25% der Anschaffungskosten vom Hersteller gewartet. Somit betragen die monatlichen Kosten für eine 2.000-Euro-Einzelplatzlizenz zwischen 25 und 42 Euro. Erfolgt ein „major release“ (z.B. von Version 2.x zu 3.x), ist in den meisten Fällen ein kostenpflichtiges Upgrade notwendig. Über einen Verwendungszeitraum von 5 Jahren betragen die monatlichen Kosten pro Nutzer unter Berücksichtigung von Lizenz- und Wartungskosten (allerdings ohne neue Releases) zwischen 59 und 76 Euro. Zusätzlich muss geprüft werden, ob zusätzliche Lizenzkosten für Infrastruktur der Client/Server-Lösung anfallen (Webserver, Datenbanken, Betriebssysteme etc.).

Dem gegenübergestellt werden die monatlichen Kosten einer Cloud-basierten Lösung, welche jedoch im Gegensatz zum Client/Server-Modell über eine meist flexible Anpassung der Nutzerzahlen verfügt. Zusätzliche Nutzer werden bei Bedarf kurzfristig zugekauft oder bei abnehmenden Anforderungen dementsprechend reduziert.

- **Server**

Die Kosten für den Serverbetrieb sind bei cloud-basierten Angeboten mit der monatlichen Gebühr abgedeckt. Im Client/Server-Szenario muss geprüft werden, ob verfügbare inhouse Lösungen denselben Servicegrad wie Cloud-basierte Lösungen bieten, und ob vergleichbare Verfügbarkeitswerte er-

zielt werden. Für die Client/Server-Lösung müssen mit dem Serverbetrieb verbundene Kosten (Miete, Energie, Personal, Sicherheit etc.) aliquot berücksichtigt werden.

- **Netzwerkanbindung**

Während inhouse Client/Server-Lösungen für den internen Gebrauch ohne externe Netzwerkanbindung verwendet werden können, benötigen Cloud-basierte Angebote eine leistungsstarke Internetanbindung. Falls die vorhandene Internetanbindung unter den Anforderungen des Cloud-Service-Anbieters liegt, müssen die Kosten für die Erweiterung zu den monatlichen Kosten des Cloud-Angebots hinzugerechnet werden.

- **Implementierung**

Das Deployment wird bei Client/Server-Lösungen meist als Dienstleistung zusätzlich zu Lizenz- und Wartungskosten verkauft. In diesem Fall sind die Kosten stark von der Anzahl und der notwendigen Konfiguration der Clients abhängig. Bei Cloud-basierten Produkten ist diese Form des Deployments nicht notwendig, da die Nutzer über den bereits existierenden Webbrowser auf die Anwendung zugreifen.

5 RECHTLICHE UND TECHNISCHE EVALUIERUNG

Auf Basis des vorangegangenen Kapitels erfolgt in diesem Kapitel eine strukturierte Analyse der österreichischen Gesetzeslage und der EU-Datenschutzverordnung sowie die Ableitung von konkreten rechtlichen und technischen Anforderungen an Cloud-Computing im EU-Raum. In einem zweiten Schritt werden bestehende Cloud-Service-Anbieter identifiziert und gemeinsam mit den Bedarfsträgern eine Auswahl dieser Anbieter für die rechtliche und technische Analyse ausgewählt. In einem letzten Schritt werden die Anforderungen der österreichischen Gesetzgebung und der EU-Datenschutzverordnungen den rechtlichen und technischen Analyseergebnissen gegenübergestellt und eventuelle Lücken identifiziert.

5.1 Anforderungen der österreichischen Gesetzeslage

Basierend auf Kapitel 4.2.1 werden in diesem Abschnitt die rechtlichen Anforderungen für Cloud-Computing Nutzer abgeleitet.

- **Unternehmensgesetzbuch**
  - Die Unternehmensführung ist bzgl. IT-Sicherheit letztverantwortlich.

- **Verbandsverantwortlichkeitsgesetz (für EPU nicht relevant)**
  - Die Organisation haftet für das Verschulden ihrer Entscheidungsträger als auch Mitarbeiter. Organisatorische und technische Maßnahmen sollten die unerlaubte Verwendung von Cloud-Services und die dortige Verarbeitung personenbezogener und sensibler Daten unterbinden.

- **Datenschutzgesetz**
  - Unternehmen bleibt auch bei der Verwendung von Cloud-Computing für den Schutz der Daten letztverantwortlich (§10 DSG).
  - Der Nutzer muss sich der rechtmäßigen und sicheren Datenverarbeitung beim Cloud-Service-Anbieter versichern und diese vertraglich als Leistungspflicht festlegen:
    - Daten dürfen nur im Rahmen des Auftrags verarbeitet werden.
    - Die Verwendung von Subauftragnehmern erfordert die Zustimmung des Auftraggebers.
    - Technische und organisatorische Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht müssen erfüllt sein.
    - Nach Beendigung der Dienstleistung sind alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in des-

sen Auftrag für ihn weiter aufzubewahren oder zu vernichten (§11 Abs. 1 Z5 DSG).

- Regelmäßige Überprüfung, ob organisatorische und technische Schutzmaßnahmen angemessen gemäß § 14 DSG umgesetzt werden (§11 Abs. 1 Z 6 DSG)
  - Auszug § 14 Abs. 1 DSG: Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten für Unbefugte nicht zugänglich sind.
  - Auszug § 14 Abs. 2 DSG: Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

    1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,

    2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,

    3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,

    4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,

    5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,

    6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,

    7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,

    8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

    Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

  - Übermittlung und Überlassung von Daten in das Ausland ist abgesehen von EWR-Staaten und sicheren Drittstaaten untersagt. Ausnahmebestimmungen sind in §12 DSG festgelegt.
  - § 24 Abs. 2a DSG verlangt die unverzügliche Information der Betroffenen in geeigneter Form sobald Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht.

- Bundesabgabenordnung
  - Die Aufbewahrungspflicht für Bücher und Aufzeichnungen beträgt sieben Jahre (§ 132 BAO). §131 BAO schreibt vor, dass Bücher und Aufzeichnungen auf Verlangen der Abgabenbehörde innerhalb angemessenen Fristen im Inland zu erbringen sind.
  - Werden BAO-relevante Bücher und Aufzeichnung bei Cloud-Anbietern gelagert, so ist sicherzustellen, dass diese sieben Jahre verfügbar sind und in angemessener Zeit ins Inland transferiert werden können.

5.2 Anforderungen der EU-Datenschutzverordnung

Die EU-Datenschutzverordnung (GDPR) findet Anwendung, sobald personenbezogene Daten von einem Controller, Processor oder Datensubjekt, welche innerhalb des EWR-Raums niedergelassen sind, verarbeitet werden. Die Voraussetzung, dass das Datensubjekt eine Zahlung zu leisten hat, gilt nicht. Es reicht die Absicht des Controllers, Güter und Services an Datensubjekte innerhalb des EWR-Raums anzubieten. Cloud-Kunden nehmen (normalerweise) die Rolle des Controllers ein, während Cloud-Service-Anbieter (normalerweise) die des Processors einnehmen.

- Laut Artikel 26 Absatz 4 ist „jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.“ Somit müssen Subunternehmer durch den Kunden genehmigt werden (Art 26 § 2 (d)), ob Standardklauseln in den Verträgen diese Verpflichtungen auch erfüllen, ist offen.

- Dem Processor ist nur erlaubt jene Daten zu verarbeiten, für die der Controller den Auftrag hierfür gibt (oder wenn die Notwendigkeit dazu besteht, gegeben durch das EU-Recht nach Art 27 GDPR). Sie sind außerdem dazu verpflichtet, die Dokumentationen regelmäßig zu aktualisieren (Art 27 GDPR) und mit der Aufsichtsbehörde zu kooperieren (Art 29 GDPR).

- Der Processor ist verpflichtet, dass er im Falle einer Verletzung des Schutzes personenbezogener Daten den Controller ohne unangemessene Verzögerung benachrichtigt (Art 31 GDPR) und eine Risikoanalyse (Art 32a GDPR) sowie eine Datenschutzfolgenabschätzung (Art 33 GDPR) durchführt.

- Die Bestimmungen bezüglich Datenschutzbeauftragter (z.B. Art 35 GDPR) gelten auch für „einfache“ Processors von Daten. Art 11 GDPR über Transparenz, welcher „prägnante, transparente, klar formulierte, und einfach zugängliche Policies definiert“, könnte eine hilfreiche Referenzquelle für Service-Provider darstellen, um in diesem Bereich Regelkonformität zu erreichen.

- Art 27 § 2 a (c) der GDPR ermöglicht der Aufsichtsbehörde einem Unternehmen bis zu 100.000.000 Euro oder bis zu 5% des weltweiten jährlichen Geschäftsumsatzes aufzuerlegen, je nachdem, welcher Betrag höher ist. Allerdings sollte beachtet werden, dass wenn der Controller oder Processor im Besitz eines validen „European Data Protection Seal“ ist, eine solche Geldstrafe nur im Falle eines vorsätzlichen oder fahrlässigen Verstoßes verhängt werden kann (Art 27 § 2b GDPR).

- Art 39 der GDPR beschreibt das Konzept der „Zertifizierung“, welches von besonderem Interesse im Zusammenhang mit Cloud-Computing ist. Während in früheren Gesetzesvorlagen die Kommission „nur fördern“ sollte, dass Datenschutz-Zertifikatsmechanismen sowie Datenschutz-Siegel und -Kennzeichen begünstigt werden, bestimmt der aktuelle Entwurf, dass sowohl Controller als auch Processor das Recht haben, von der entsprechenden Aufsichtsbehörde zertifiziert zu werden, dass die Verarbeitung von Daten gemäß dieser Verordnung durchgeführt wird (Art 39 §1a GDPR). Zusätzlich, gemäß § 2, muss die Zertifizierung freiwillig und erschwinglich sein, zugänglich mithilfe eines Prozesses, welcher transparent abläuft und keine übermäßige Belastung darstellt. Das Audit kann entweder direkt von den Datenschutzbehörden durchgeführt werden, oder es können Third-Party-Auditoren von ihnen dazu bevollmächtigt werden (§ 1d GDPR). Controller und Processor werden nach einem bestandenen Audit mit einem standardisierten europäischen Datenschutz-Gütesiegel ausgezeichnet und in ein öffentliches Register eingetragen (§§1e und 1g GDPR). Ein bestandenes Audit ist nur so lange gültig, wie der Controller oder Processor den Anforderungen in vollen Umfang entspricht, längstens jedoch für fünf Jahre (§§ 1f und 1g GDPR). Die Präambeln der Verordnung legen dar, dass die Zertifizierung Vertrauen zwischen den Datensubjekten, Rechtssicherheit für Controller und zur gleichen Zeit den Export von europäischen Datenschutzstandards ermöglichen soll, sodass nicht-europäische Unternehmen einen einfacheren Zutritt in den europäischen Markt bekommen, indem sie eine Zertifizierung vorweisen können.

Die Delegierung bezüglich des Datenmanagements wandelten sich zum Nachteil für die Cloud-Anwender, unter anderem, weil sie aus der Sicht des Datenschutzes meistens dennoch verantwortlich und haftbar sind. In einigen Fällen ist die Unterscheidung zwischen Controller und Processor nicht eindeutig, und je mehr Entscheidungsgewalt dem Anbieter überlassen wird, desto wahrscheinlicher wird er als Processor klassifiziert werden.

Die Datenschutzrichtlinie wird mittlerweile durch weitere Bestimmungen ergänzt, welche den räumlichen Geltungsbereich vergrößern, indem auch Fälle inkludiert werden, in welchen Services und Güter an Datensubjekte in der EU angeboten werden. Somit können auch Fälle, in denen eine Webseite in

einer gewissen Sprache angeboten wird oder Steuern basierend auf einer gewissen Region berechnet werden, beachtet werden, wenn die Anwendbarkeit der GDPR bestimmt wird. Die praktischen Implikationen des erweiterten Geltungsbereiches bleiben allerdings vorerst unklar aufgrund der Tatsache, dass die Durchsetzbarkeit möglicherweise nicht unproblematisch ist.

Die GDPR würde auch einige Bestimmungen beinhalten, welche an den Processor gerichtet sind, und nicht nur ausschließlich an den Controller. Allerdings bleibt das fundamentale Problem der Differenzierung zwischen Controller und Processor bestehen. Außerdem würden im praktischen Sinne Controller alleinig für Datenschutzverletzungen haftbar bleiben, auch wenn sie Kontrolle abgetreten haben. Wie die Zertifizierung der GDPR schlussendlich implementiert wird, ist zum Zeitpunkt März 2014 noch offen. Der momentane Trend geht in Richtung Schaffung einer Vertrauensbasis für Controller, allerdings nicht aus der Perspektive der Datensubjekte, sondern indem die Bestimmungen geändert werden, sodass Controller nicht nur ermutigt werden, sich von der Aufsichtsbehörde zertifizieren zu lassen, sondern auch zusätzliche Rechte ihr gegenüber erhalten.

5.3 Betriebliche Anforderungen bezüglich Cloud-Computing

Neben rechtlichen, technischen und organisatorischen Anforderungen (siehe nächster Abschnitt) sind auch betriebliche Anforderungen zu evaluieren, um einen erfolgreichen Einsatz von Cloud-Computing zu gewährleisten. Übergeordnetes Ziel dafür geeigneter strukturierter Vorgehensmodelle ist es, die Cloud-Computing-Risiken zu minimieren und vorhandene Potenziale bestmöglich auszuschöpfen[72]:

1. **Vorbereitung des Projekts**
    a. Zusammenstellung Projektteam
    b. Entwicklung einer Cloud-Strategie
    c. Geschäftszieldefinition und Entwicklung einer Migrations-Roadmap
        – Was ist der maximal tolerierbare Aufwand für die Migration eines Prozesses bzw. einer Anwendung in die Cloud? Wie steht dies zu den erwartenden Einsparungen?

2. **Analysephase**
    a. Identifizierung der Risiken im Falle eines Cloud Ausfalls
        – Welche Risiken sind für das Unternehmen aufgrund von Service-Ausfällen tragbar?
    b. Anforderungen und Abhängigkeiten der betrieblichen IT-Anwendungen
        – Ab wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden?
        – Wann ist der Schwellwert für Ausfallszeiten erreicht?

[72] vgl. Bundeskanzleramt Österreich – Cloud-Computing-Positionspapier [12]

  - Welche Anwendungen können aufgrund der Verarbeitung sensibler Daten nicht in die Cloud ausgelagert werden?
  - Hat die IT-Anwendung zu viele interne Abhängigkeiten, um in die Cloud ausgelagert zu werden?
- c. Kostenvergleich: Cloud vs. inhouse Lösung
- d. Änderungen der internen Organisation
- e. Bestimmung des passenden Service- (SaaS, IaaS, PaaS) und Betriebsmodells (public, private, hybrid)

3. Auswahl des Cloud-Anbieters

- a. Auswahl geeigneter Evaluierungsverfahren
- b. Abgleich des Leistungsprofils mit erstellten Anforderungen

4. Planung einer Exit-Strategie

- a. Vertragsgestaltung dementsprechend anpassen
- b. Verwendung offener Datenformate und Schnittstellen

5. Planung des laufenden Betriebs

- a. Erstellung von Governance-Regeln

5.4 Technische und organisatorische Anforderungen bezüglich Cloud-Sicherheit

Die folgenden technischen und organisatorischen Maßnahmen sollten durch den Cloud-Service-Anbieter als Grundschutz zur Absicherung der Cloud-Infrastruktur implementiert werden. Maßnahmen, welche in Umgebungen mit erhöhten Verfügbarkeits- und Vertraulichkeitsschutz erforderlich sind, wurden explizit als solche gekennzeichnet (kursiv). Die Maßnahmen entsprechen den Empfehlungen des deutschen Bundesamts für Sicherheit in der Informationstechnik (nachfolgende Auflistung wurde den BSI-Sicherheitsempfehlungen für Cloud-Computing-Anbieter [15] entnommen) und wurden auf den SaaS-Fokus des Projekts angepasst.

1. Sicherheitsmanagement

- a. definiertes Vorgehensmodell für alle IT-Prozesse (z.B. ITIL, COBIT)
- b. Implementierung eines anerkannten Informationssicherheits-Management-Systems (z.B. ISO 27001)
- c. nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud
- *d. Nachweis einer ausreichenden Informationssicherheit (Zertifizierung)*
- e. angemessene Organisationsstruktur für Informationssicherheit beim Cloud-Service-Anbieter (Ansprechpartner für Sicherheitsfragen)

2. **Sicherheitsarchitektur – Rechenzentrumssicherheit**
    a. redundante Auslegung aller wichtigen Versorgungskomponenten (Strom, Klimatisierung der Rechenzentren, Internetanbindung, Verkabelung etc.)
    b. Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme etc.
    c. Zwei-Faktor-Authentifizierung für den Zutritt ins Rechenzentrum
    d. Brandschutz: Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmäßige Brandschutzübungen
    e. robuste Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet
    f. Redundante Rechenzentren, die mindestens so weit voneinander entfernt sind, dass ein beherrschbares Schadensereignis nicht gleichzeitig das ursprünglich genutzte Rechenzentrum und das, in dem die Ausweichkapazitäten genutzt werden, beeinträchtigen.

3. **Sicherheitsarchitektur – Server-Sicherheit**
    a. technische Maßnahmen zum Schutz des Hosts (Host-Firewalls, regelmäßige Integritätsüberprüfungen, Host-based Intrusion Detection Systems)
    b. sichere Grundkonfiguration des Hosts (z.B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste etc.)
    c. Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)

4. **Sicherheitsarchitektur – Netzsicherheit**
    a. Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz etc.)
    b. Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway etc.)
    c. Distributed Denial of Service (DDoS) Mitigation (Abwehr von DDoS-Angriffen)
    d. geeignete Netzsegmentierung (Isolierung des Management-Netzes vom Datennetz)
    e. sichere Konfiguration aller Komponenten der Cloud-Architektur.
    f. Fernadministration durch einen sicheren Kommunikationskanal (z.B. SSH, IPSec, TLS/SSL,VPN)
    g. verschlüsselte Kommunikation zwischen Cloud-Computing-Anbieter und -Nutzer (z.B. TLS/SSL)
    h. verschlüsselte Kommunikation zwischen Cloud-Computing-Standorten
    i. verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind
    j. redundante Vernetzung der Cloud-Rechenzentren

5. **Sicherheitsarchitektur – Anwendungs- und Plattformsicherheit**
    a. Sicherheit muss Bestandteil des Software Development Life Cycles sein (Reviews, automatisierte Tests, Vulnerability-Tests etc.).
    b. Einhaltung von Sicherheits-Mindeststandards der zur Verfügung gestellten Web-Anwendungen (z. B. Prinzipien zur sicheren Software-Entwicklung nach OWASP)
    c. Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service-Packs) sowie Release-Management
    d. Sicherstellung der Verträglichkeit von Patches auf Testsystemen vor dem Einspielen in den Echtbetrieb

6. **Sicherheitsarchitektur – Datensicherheit**
    a. Datensicherheit im Lebenszyklus der Kundendaten definieren und umsetzen
    b. sichere Isolierung der Kundendaten (z. B. virtuelle Speicherbereiche, Tagging etc.)
    c. regelmäßige Datensicherungen, deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte und Speicherdauer) für die Kunden nachvollziehbar sind
    d. Daten müssen auf Wunsch des Kunden vollständig und zuverlässig gelöscht werden

7. **Sicherheitsarchitektur – Verschlüsselung und Schlüsselmanagement.**
    a. Best Practices der Schlüsselverwaltung umsetzen
    b. verwendete kryptografische Verfahren für Kunden zugänglich machen

8. **ID- und Rechtemanagement**
    a. starke Authentifizierung (mindestens Zwei-Faktor-Authentifizierung) für Administratoren des CSP
    b. rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte
    c. „least privilege“-Modell (Nutzer bzw. CSP-Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen.)
    d. Vier-Augen-Prinzip für kritische Administrationstätigkeiten
    e. starke Authentifizierung (z.B. Zwei-Faktor-Authentifizierung) für Cloud-Kunden

9. **Kontrollmöglichkeiten für Nutzer**
    a. Kunden müssen die Möglichkeit haben, messbare, z.B. im SLA vereinbarte Größen, überwachen zu können.

10. **Monitoring und Security Incident Management**
    a. umfassende Überwachung der Cloud-Dienste rund um die Uhr sowie zeitnahe Reaktion bei Angriffen bzw. Sicherheitsvorfällen

b. Erfassung und Auswertung von Datenquellen (z.B. Systemstatus, fehlgeschlagene Authentifizierungsversuche etc.)
c. rund um die Uhr erreichbares, handlungsfähiges Team für Security Incident Handling und Trouble-Shooting
d. Mitteilungspflichten des CSP gegenüber dem Kunden über Sicherheitsvorfälle oder Hinweise auf Sicherheitsvorfälle, die den Kunden betreffen könnten
e. geeignete Bereitstellung relevanter Logdaten durch den CSP
f. Logging und Monitoring der Aktivitäten von Administratoren

11. Notfallmanagement

a. Der Cloud-Anbieter muss ein Notfallmanagement aufsetzen und betreiben.
b. Der CSP muss seinen Kunden die Priorisierung des Wiederanlaufs für die angebotenen Cloud-Dienste transparent machen.
c. regelmäßige Notfall-Übungen (z.B. Ausfall eines Cloud-Computing-Standorts)
d. Der CSP sollte nachweisen, dass sein Notfallmanagement auf einem international anerkannten Standard wie BS 25999 oder BSI-Standard 100-4 basiert (z.B. anhand Notfallvorsorgekonzept und Notfallhandbuch).

12. Portabilität und Interoperabilität

a. Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen und gegebenenfalls Offenlegung der damit verbundenen Kosten
b. standardisierte oder offen gelegte Schnittstellen (API und Protokolle)

13. Sicherheitsprüfung und -nachweis

a. Cloud-Service-Anbieter haben den Cloud-Nutzern regelmäßig über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle, die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests berichten.
b. regelmäßige Penetrationstests
c. regelmäßige Penetrationstests bei Subunternehmen
d. regelmäßige und unabhängige Sicherheitsrevisionen
e. regelmäßige und unabhängige Sicherheitsrevisionen bei Subunternehmern

14. Anforderungen an das Personal

a. vertrauenswürdiges Personal
b. Ausbildung der Mitarbeiter des Cloud-Service-Anbieters (regelmäßige Schulungen)
c. Sensibilisierung der Mitarbeiter des Cloud-Service-Anbieters für Informationssicherheit und Datenschutz
d. Verpflichtung der Mitarbeiter auf Informationssicherheit, Datenschutz, angemessenen Umgang mit Kundendaten

15. Vertragsgestaltung – Transparenz

a. Offenlegung der Standorte des Cloud-Service-Anbieters (Land, Region), an denen die Kundendaten gespeichert und verarbeitet werden
b. Offenlegung der Subunternehmer des Cloud-Service-Anbieters, die für die Erbringung der Cloud-Services wesentlich sind
c. Transparenz, welche Eingriffe der Cloud-Service-Anbieter oder Dritte in Daten und Verfahren der Kunden vornehmen dürfen
d. regelmäßige Unterrichtung über Änderungen (z.B. neue oder abgekündigte Funktionen, neue Subunternehmer, andere Punkte, die für das SLA relevant sind)
e. Transparenz, welche Software durch den Cloud-Service-Anbieter aufseiten des Kunden installiert wird sowie über die daraus resultierenden Sicherheitserfordernisse bzw. -risiken.
f. Transparenz bezüglich staatlicher Eingriffs- und Einsichtrechte, über gerichtlich festlegbare Einsichtrechte Dritter und über Prüfpflichten zu gespeicherten Daten durch den Cloud-Service-Anbieter an allen potenziellen Standorten
g. Darlegung der Rechts- und Besitzverhältnisse des Cloud-Service-Anbieters sowie der Entscheidungsbefugnisse

16. Vertragsgestaltung – Service Level Agreement

a. definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben
b. Sicherstellung des Betriebs oder der Bereitstellung der Daten im Falle einer Insolvenz des Cloud-Service-Anbieters unter Beachtung von Vertraulichkeitszusagen und Datenschutzanforderungen

17. Datenschutz und Compliance

a. Gewährleistung des Datenschutzes nach österreichischem Recht
b. Datenschutzrichtlinien und -gesetze, denen der Cloud-Nutzer unterliegt, müssen eingehalten werden
c. bei Datenübermittlung: Rechtsgrundlage für die Übermittlung
d. bei Auftragsdatenverarbeitung: Schriftliche Vereinbarung zwischen Cloud-Nutzer und Cloud-Anbieter mit Mindestinhalt: „Beschreibung von Gegenstand und Dauer des Auftrags“, „Genaue Bezeichnung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten“, „Festlegung des genauen Ortes der Verarbeitung personenbezogener Daten beim Cloud-Anbieter einschließlich der technischen und organisatorischen Verarbeitungsumgebung“, „Umgang mit Ansprüchen Betroffener auf Berichtigung, Sperrung und Löschung personenbezogener Daten“, „Festlegung oder Verbot etwaiger Unterauftragsverhältnisse“, „Rückgabe bzw. Löschung von Daten nach Beendigung des Auftrags“
e. bei Übermittlung und Auftragsdatenverarbeitung: Speicherung und Verarbeitung der personenbezogenen Daten innerhalb der Mitgliedsstaaten der EU oder eines Vertrags-

staats des EWR **oder** außerhalb der EU oder eines Vertragsstaats des EWR, wenn ein angemessenes Datenschutzniveau gewährleistet werden kann z. B. durch: Entscheidung der EU-Kommission, Beitritt zum Safe-Harbor-Abkommen (USA), EU-Standardvertragsklauseln, Genehmigung der Aufsichtsbehörde

f. keine Einbindung von Unterauftragnehmern, die eine Verarbeitung der personenbezogenen Daten unter den oben genannten Voraussetzungen nicht gewährleisten können; Kontrollrechte des Kunden zur datenschutzkonformen Verarbeitung der personenbezogenen Daten bei der Auftragsdatenverarbeitung durch Kontrolle vor Ort oder Testat eines unabhängigen Sachverständigen
g. bei Auftragsdatenverarbeitung: Kontrollrecht der für den Cloud-Nutzer zuständigen Aufsichtsbehörde
h. bei Auftragsdatenverarbeitung: Weisungsrechte des Cloud-Nutzers gegenüber dem Cloud-Anbieter
i. Für den Cloud-Nutzer relevante gesetzliche Bestimmungen müssen durch den Anbieter eingehalten werden.

5.5 Rechtliche und technische Analyse ausgewählter Cloud-Computing-Anbieter

Gemeinsam mit den Bedarfsträgern BISC der WKO und BMLVS wurden für die vorliegende Analyse Anbieter von SaaS-Cloud-Computing anhand folgender Kriterien ausgewählt: (i) mindestens ein Repräsentant aus dem US-, EU- und AT-Raum, (ii) klarer Fokus auf Software as a Service und (iii) Produkte, welche einen möglichst hohen Verbreitungsgrad innerhalb österreichischer KMUs und Behörden haben. Bei der Suche nach geeigneten Analysekandidaten wurde auf Workshop-Techniken und Web-Recherche inkl. der dort auffindbaren Nutzerzahlen zurückgegriffen. Da keine expliziten Nutzerzahlen für österreichische KMUs und Behörden verfügbar sind, mussten globale Nutzerzahlen mit der persönlichen Einschätzung der Projektteilnehmer hinsichtlich der Verbreitung in Österreich kombiniert werden. Folgende Produkte wurden für die Analyse ausgewählt:

- US: Google Apps (Gmail, Google Docs)
- US: Microsoft Office 365
- US: Dropbox
- US: Salesforce.com
- AT: Fabasoft Folio Cloud
- EU: SAP Sales on Demand

Trotz intensiver Recherche konnten keine weiteren den Kriterien entsprechenden EU-/AT-Anbieter identifiziert werden. Größere europäische Cloud-Computing-Anbieter wie beispielsweise T-Systems wurden aufgrund eines fehlenden breitenwirksamen SaaS-Angebots nicht in die Analyse miteinbezogen.

5.5.1 Analysemethodik

Die Analyse wurde im August 2013 durchgeführt und stützt sich ausschließlich auf vom Anbieter bereitgestellte Dokumentationen in Form von Webseiten, White Papers, AGB, Serviceverträgen, SLAs, Spezifikationen und dergleichen. Konnten diesen Quellen bestimmte Informationen nicht entnommen werden, so wurde versucht, diese via E-Mail direkt vom Hersteller einzuholen.

Die in Abschnitt 5.1 und 5.2 spezifizierten Anforderungen der österreichischen und europäischen Gesetzeslage sowie die in Abschnitt 5.4 spezifizierten technischen und organisatorischen Anforderungen bilden die Analysegrundlage. Die Analyse wurde in folgenden Domänen (zum Teil basierend auf den BSI-Sicherheitsempfehlungen für Cloud-Computing-Anbieter) durchgeführt:

- Vertragsgestaltung
- Datenschutz
- Sicherheitsmaßnahmen
- Anwendungssicherheit
- Datensicherheit
- Verschlüsselung und Schlüsselmanagement
- Identifikations- und Rechtemanagement
- Monitoring und Security Incident Management
- Notfallmanagement
- Portabilität und Interoperabilität
- Sicherheitsprüfung und -nachweis
- Personalanforderungen

Die Quellenangaben sind direkt bei den Analyseergebnissen hinterlegt; eine komplette Liste findet sich in der Bibliographie unter [69].

5.5.2 Analyseergebnisse

5.5.2.1 Vertragsgestaltung

a. Besteht die Möglichkeit des Abschlusses eines schriftlichen Vertrages oder kann dieser nur online abgeschlossen werden?
Dropbox
Dropbox bietet Business-Abos online an, eine Referenz auf schriftliche Verträge konnte nicht gefunden werden (Dropbox, Buy Dropbox for Business, 2013).
Fabasoft Folio Cloud
Fabasoft bietet seine Business-Abos online an, falls schriftliche Verträge möglich sind, so konnte dies der Website nicht entnommen werden (Fabasoft, Business Shop, 2013).
Google Apps
Laut der Website von Google Apps erfolgt der Vertragsabschluss nur online. „Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie auf die unten stehende Schaltfläche ‚Ich stimme zu' klicken." (Google, Vereinbarung, 2013). Ohne Zustimmung ist die Nutzung dieses Dienstes ausgeschlossen.
Microsoft Office 365
Nach Angaben seitens Microsoft wird der Vertrag schriftlich abgeschlossen. [(Microsoft, Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit , 2013), (Die zehn wichtigsten Fragen, die Sie Ihrem Anbieter von Cloud-Diensten stets stellen sollten) und (Microsoft, Unabhängig geprüft, 2013)].
Salesforce

Laut Salesforce-Homepage beziehungsweise dem Master Subscription Agreement (Salesforce, Master Subscription Agreement, 2013) erfolgt die Zustimmung zu den Allgemeinen Geschäftsbedingungen sobald entweder die Checkbox zur Zustimmung aktiviert ist oder ein Formular ausgefüllt wurde, dass das Agreement in irgendeiner Form referenziert. (Salesforce, Master Subscription Agreement, 2013, S. Präamble). Folglich erfolgt der Abschluss online.
SAP Sales OnDemand
Die Kontaktaufnahme mit SAP ist vor Kauf gewünscht und wird empfohlen. Der eigentliche Kauf wird über den SAP Marketplace abgewickelt und scheint zumindest bis auf Ausnahmen ohne schriftliche Verträge auszukommen. (SAP, SAP Store Quick Guide, 2013)
b. Bestehen für Subauftragnehmer dieselben Verpflichtungen wie für den Auftragnehmer? Ist dieser Umstand vertraglich geregelt?
Dropbox
(Dropbox, Datenschutzrichtlinien, 2013) Punkt 3, Freigabe und Offenlegung von Informationen, Dienstanbieter, Geschäftspartner und andere: „[…] Diese Drittparteien haben möglicherweise Zugriff auf Ihre Informationen, allerdings nur sofern dies zur Durchführung der von uns beauftragten Tätigkeiten erforderlich ist und im Rahmen von Bedingungen, die den vorliegenden Datenschutzrichtlinien ähnlich sind. […]“.
Fabasoft Folio Cloud
Da Fabasoft ISO 27001 zertifiziert ist und laut A.6.2.3 alle relevanten Sicherheitsaspekte vertraglich geregelt sein müssen, ist davon auszugehen, dass Sicherheit Teil der Abkommen zwischen Fabasoft und Subauftragnehmern ist. Dass hingegen bei diesen dieselben Verpflichtungen bestehen, ist nicht (i) durch ISO 27001 oder (ii) durch Fabasofts Dokumente belegbar. Allerdings betreibt Fabasoft laut eigenen Angaben seine Dienste mit eigener Wertschöpfung, dürfte folglich ohne Subauftragnehmer auskommen. (Fabasoft, Cloud Assurance, 2013), Punkt: Supply-Chain-Assurance.
Google Apps
Laut (Google, Google Apps for Business (Online) Agreement, 2013) den Punkten 2.6 und 2.11 muss Google sicherstellen, dass Subauftragnehmer Maßnahmen bereitstellen, um die Datenvertraulichkeit zu gewährleisten.
Microsoft Office 365
Dieselben Verpflichtungen bestehen und sind vertraglich geregelt. (Microsoft, Third Parties, 2013), (How does Office 365 or Dynamics CRM Online ensure subcontractors comply with Microsoft’s privacy requirements?).
Salesforce
Ja. Laut Salesforce AGB wird dies gewährleistet (Salesforce, Master Subscription Agreement, 2013), Punkt 8.2.
SAP Sales OnDemand
Ja. Siehe (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 3.
c. Wird der Kunde über Einsatz bzw. Wechsel von Subauftragnehmern informiert und ist dessen Zustimmung erforderlich (§10 DSG)?
Dropbox
(Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 3.c: „Sollte Dropbox die Dienste in einer Art und Weise ändern, die deren Funktionalität entscheidend reduziert, setzt Dropbox den Kunden davon in Kenntnis“. Im allgemeinen Fall dürfte keine Benachrichtigung stattfinden bzw. eine Zustimmung wird nicht erforderlich sein. Allerdings sollte der Kunde laut Safe-Harbor-Abkommen die Wahl haben, ob Daten an Dritte weitergegeben werden dürfen. (US Department of Commerce, 2013), Punkte „Notice“, „Choice“ und „Onward Transfer“.
Fabasoft Folio Cloud
Laut Fabasoft (Fabasoft, Cloud Assurance, 2013), Punkt „Nationale und europäische Datenschutzgesetze“ sollte Fabasoft die dort aufgelisteten Gesetze erfüllen. Folglich kann angenommen werden, dass Bestimmungen wie §10 DSG erfüllt werden.

Google Apps
Google (Google, Online Agreement, 2013) geht nicht dezidiert darauf ein, was bei einem Wechsel von Subauftragnehmern passiert. Allerdings sollte dies mit dem Safe-Harbor-Abkommen abgedeckt sein (US Department of Commerce, 2013), Punkte „Notice“, „Choice“ und „Onward Transfer“.
Microsoft Office 365
Als Administrator sind solche Benachrichtigungen möglich, sofern diese Einstellung im Benutzerprofil aktiviert ist. (Microsoft, Konformitätsbenachrichtigungen, 2013). Allerdings sollte dieser Zustand mit dem Safe-Harbor-Abkommen abgedeckt sein. (US Department of Commerce, 2013), Punkte „Notice“, „Choice“ und „Onward Transfer“.
Salesforce
(Salesforce, Master Subscription Agreement, 2013) geht nicht darauf ein. Sollte mit dem Safe-Harbor-Abkommen abgedeckt sein (US Department of Commerce, 2013), Punkte „Notice“, „Choice“ und „Onward Transfer“.
SAP Sales OnDemand
SAP geht darauf in Anlage 2 Punkt 3 ein (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013). Allerdings besteht gegebenenfalls nur Auskunftspflicht über vertragliche Bestimmungen mit Subauftragnehmern. Der Kunde wird möglicherweise nicht über den Wechsel informiert beziehungsweise die Zustimmung des Kunden ist dazu nicht nötig.
d. Sind Regelungen vorgesehen, welche im Falle einer Insolvenz des Auftragnehmers die Daten des Kunden schützen und die Verfügbarkeit seiner Anwendungen sicherstellen?
Dropbox
Laut Dropbox dürfen der Kunde und Dropbox im Falle einer Insolvenz (sofern das Verfahren innerhalb von 90 Tagen nicht abgewiesen wird) seine Tätigkeit einstellen; siehe (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 10.b. Folglich besteht kein Anrecht auf Verfügbarkeit im Falle einer Insolvenz seitens Dropbox.
Fabasoft Folio Cloud
Die Allgemeinen Geschäftsbedingungen von Fabasoft erwähnen nichts dergleichen. (Fabasoft, AGB, 2013). Folglich kann keine Verfügbarkeit von Diensten garantiert werden.
Google Apps
Ja, Google sieht solche Regelungen vor, allerdings nur für einen „wirtschaftlich vernünftigen Zeitraum“ (Google, Online Agreement, 2013), Punkt 11.2 iv.
Microsoft Office 365
Zitat: „We always give you access to your customer data.“ (Microsoft, Administrative Access, 2013)-(What is the Office 365 and Microsoft Dynamics CRM Online position on data access?), Sollte Microsoft auch im Falle einer Insolvenz Zugriff auf die Dienste gestatten. Explizite vertragliche Regelungen konnten nicht gefunden werden.
Salesforce
Im Falle einer Insolvenz seitens Salesforce hat das die Kündigung zur Folge und somit letztendlich die Löschung der Daten. (Salesforce, Master Subscription Agreement, 2013), Punkt 12.3. Folglich kann die Verfügbarkeit nicht garantiert werden.
SAP Sales OnDemand
Die Allgemeinen Geschäftsbedingungen nennen folgende Textpassage: „[…] Der Auftraggeber hat jederzeit während eines Subskriptionszeitraums die Möglichkeit, auf seine Daten zuzugreifen […]“ (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Punkt 7. Also sollte auch im Falle einer Insolvenz seitens SAP Verfügbarkeit gegeben sein.
e. Besteht im Falle einer Insolvenz das Recht auf Herausgabe der jüngsten Datensicherungskopien an den Kunden?
Dropbox
Ja, dies kann allerdings unter Umständen mit einer Gebühr verbunden sein (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 10.e.
Fabasoft Folio Cloud

Im Falle einer Kündigung (in Folge einer Insolvenz) werden Daten 30 Tage lang gehalten und danach gelöscht. Es wird empfohlen, die Daten vor Vertragsende bzw. Kündigung zu exportieren. (Fabasoft, AGB, 2013), Punkte 4.7 bzw. 7.3.3.
Google Apps
Ja, dieses Recht besteht (Google, Online Agreement, 2013), Punkte 11.1 und 11.2.
Microsoft Office 365
Nach Auslaufen bzw. Beendigung oder Kündigung des Vertrags (u.a. im Falle einer Insolvenz) werden die Daten nach 90 Tagen gelöscht, bis dahin kann ein Backup herausgegeben werden. (Microsoft, Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit , 2013), Punkt: „Die zehn wichtigsten Datenschutz- und Sicherheitsfunktionen von Office 365“.
Salesforce
Ja, Salesforce gesteht dem Kunden dieses Recht zu (Salesforce, Master Subscription Agreement, 2013), Punkt 12.5.
SAP Sales OnDemand
Laut folgender Aussage: „[…] Ferner darf der Auftraggeber nach angemessener Anforderung die Daten des Auftraggebers während eines Subskriptionszeitraums exportieren und abrufen […]“ (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Punkt 7, b Recht auf Zugriff. Ob die Insolvenz die Gültigkeit der Subskription aufhebt, bleibt unbeantwortet.
f. Wie wird bei Speicherung aufbewahrungspflichtiger Daten (z.B. Rechnungen, Bücher im Kontext von BAO, UGB) die Einhaltung der Aufbewahrungsfristen (z.B. 7 Jahre) gewährleistet?
Dropbox
Speicherung von Daten wird nur innerhalb eines gültigen Abonnements gewährleistet. Folglich muss das Abonnement für die Dauer der Aufbewahrungsfrist behalten werden.
Fabasoft Folio Cloud
Fabasoft bietet ein spezielles Produkt hierfür an, Archiv 2010 (Fabasoft, Sicherheit und Datenschutz , 2013), Punkt „Revisionssichere Archivierung – Archiv 2010“. Dies ist allerdings nicht Teil der Folio Cloud, folglich müsste auch hier das Abonnement für die Dauer der Aufbewahrungsfrist bewahrt werden.
Google Apps
Die Speicherung von Daten wird nur innerhalb eines gültigen Abonnements gewährleistet. Auch hier muss das Abonnement für die Dauer der Aufbewahrungsfrist gehalten werden.
Microsoft Office 365
Die Speicherung von Daten wird nur innerhalb eines gültigen Abonnements gewährleistet. Auch hier muss das Abonnement für die Dauer der Aufbewahrungsfrist gehalten werden.
Salesforce
Salesforce gewährleistet die Verfügbarkeit im Rahmen eines gültigen Abonnements, folglich muss auch hier das Abonnement für die Dauer der Aufbewahrungsfrist gehalten werden, um diese Anforderung zu erfüllen.
SAP Sales OnDemand
SAP gewährleistet Verfügbarkeit im Rahmen eines gültigen Abonnements. Auch hier muss das Abonnement für die Dauer der Aufbewahrungsfrist gehalten werden.
g. Existieren Regelungen für Rückgabe und Löschung der Daten nach Vertragsende (§11 DSG)?
Dropbox
Ja, siehe AGB (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 10.e. Der Kunde kann seine Informationen nach Vertragsende exportieren, was mit Gebühren verbunden sein kann. Nach dem Ablauf einer gewissen Frist löscht Dropbox die Daten.
Fabasoft Folio Cloud
Ja, solche Regelungen sind laut den Allgemeinen Geschäftsbedingungen vorgesehen (Fabasoft, AGB, 2013) Punkt 4.6.
Google Apps

Ja, Google sieht solche Regelungen vor. (Google, Online Agreement, 2013), Punkt 11 bzw. (Google, IT Security White Paper, 2013).
Microsoft Office 365
Ja, solche Regelungen existieren (Microsoft, Administrative Access, 2013) (What does Microsoft do to support its customers' rights to access their data? Will customers have access to their data at all times?)
Salesforce
Ja, Salesforce sieht derartige Regelungen vor (Salesforce, Master Subscription Agreement, 2013), Punkt 12.5.
SAP Sales OnDemand
Ja, SAP hat solche Regelungen definiert (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Punkt 7.4.
h. Ist im Fall von Streitigkeiten zur Leistungserbringung oder bei Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?
Dropbox
Es ist nicht ausgeschlossen, dass Dropbox Daten löscht. Laut Ausschlussklausel (Dropbox, Official Blog of Dropbox for Business, 2013), Punkt 8 wird weiters keine Haftung übernommen, wenn Daten gelöscht oder nicht gespeichert wurden.
Fabasoft Folio Cloud
Nein, denn nach spätestens 30 Tagen Zahlungsverzug werden die Daten von Fabasoft gelöscht.
Google Apps
Nein, eine Löschung ist nicht ausgeschlossen. (Google, Online Agreement, 2013), Punkt 11.2.
Microsoft Office 365
(Microsoft, Vertrag über Microsoft Dienste, 2013), Punkt 9.11 spricht von Sperrung oder Kündigung im Fall von verspäteten Zahlungen. Im Fall einer Kündigung wird 90 Tage später gelöscht.
Salesforce
Innerhalb von 30 Tagen werden die Daten gelöscht. (Salesforce, Master Subscription Agreement, 2013), Punkt 12.5.
SAP Sales OnDemand
Nach 30 Tagen Zahlungsverzug wird der Vertrag gekündigt. Die Daten werden 30 Tage nach Kündigung gelöscht. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Punkte 7.2 und 7.4.
i. Werden Änderungen des technischen und organisatorischen Schutzmaßnahmenkonzepts an den Kunden kommuniziert und muss dieser zustimmen?
Dropbox
(Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), 3.c „Sollte Dropbox die Dienste in einer Art und Weise ändern, die deren Funktionalität entscheidend reduziert, setzt Dropbox den Kunden davon in Kenntnis“. Zustimmung erfolgt durch weitere Benutzung des Dienstes (Dropbox, Allgemeine Geschäftsbedingungen, 2013), Punkt „Änderungen“.
Fabasoft Folio Cloud
Wird nicht kommuniziert beziehungsweise diese Art der Kommunikation wird nicht in der AGB erwähnt und fällt nicht unter die Gewährleistungsklausel (Fabasoft, AGB, 2013), Punkt 8.
Google Apps
Der Wechsel wird kommuniziert (Google, Online Agreement, 2013), Punkt 1.2. Die Zustimmung des Kunden wird nicht erwartet.
Microsoft Office 365
Als Administrator sind solche Benachrichtigungen möglich sofern diese Einstellung im Benutzerprofil aktiviert ist. (Microsoft, Konformitätsbenachrichtigungen, 2013). Die Zustimmung zum Wechsel scheint nicht erforderlich zu sein.
Salesforce

Der Wechsel von Subauftragnehmern ist in der AGB zu finden (Salesforce, Master Subscription Agreement, 2013).
SAP Sales OnDemand
SAP teilt Änderungen bei Subauftragnehmern mit, es wird keine Zustimmung erwartet (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013).
j. Besteht für den Kunden oder für einen von ihm beauftragten Dritten ein Kontrollrecht hinsichtlich der Umsetzung der vereinbarten technischen und organisatorischen Schutzmaßnahmen?
Dropbox
Nichts dergleichen konnte bezüglich Kontrollrechten in den AGB (Dropbox, Allgemeine Geschäftsbedingungen, 2013) bzw. Datenschutzbedingungen (Dropbox, Datenschutzrichtlinien, 2013) gefunden werden.
Fabasoft Folio Cloud
(Fabasoft, Sicherheit und Datenschutz , 2013), Punkt „Deutschland – Auftragsdatenverarbeitung“: „[…] Fabasoft bietet seinen Business Kunden auf Wunsch auch einen Vertrag zum deutschen §11 Datenschutzgesetz […]“, welches derartige Kontrollrechte unterstützt.
Google Apps
Die Datenschutzbestimmungen gehen nicht darauf ein (Google, Certification & data privacy, 2013).
Microsoft Office 365
Datenschutzbestimmungen gehen nicht darauf ein (Microsoft, Microsoft Datenschutzrichtlinien, 2013). (Microsoft, Security, Audits and Certification, 2013), Punkt „Does Microsoft allow customers to audit Office 365 or Dynamics CRM Online controls or infrastructure?“: „Allowing potentially thousands of customers to audit our services would not be a scalable practice and might compromise security.“
Salesforce
Salesforce geht nicht darauf ein. (Salesforce, Internationale Datenschutzgesetze, 2013).
SAP Sales OnDemand
Ja, falls ein Vertrag mit SAP Österreich abgeschlossen wird (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2 Punkt 4.
k. Sind Sicherheitsleistungen im Vertrag definiert und durch Security SLA oder SLA weiter spezifiziert?
Dropbox
Die Vereinbarung dazu: „[...] alle zur Speicherung und Verarbeitung von Kundendaten genutzten Einrichtungen müssen einem wirtschaftlich zumutbaren Sicherheitsstandard entsprechen [...]“ (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 3.a. Weiter spezifiziert werden die Maßnahmen nicht.
Fabasoft Folio Cloud
Fabasoft spezifiziert seine Sicherheitsmaßnahmen genau in einem Sicherheitspaper (Fabasoft, Performance Characteristics of Data Security, 2013), die AGB gehen nicht auf spezielle Sicherheitsleistungen ein, gewährt aber „Vertragserfüllung und das Feststellen zugesicherter Eigenschaften und/oder vereinbarten Beschaffenheit des jeweils mit dem Kunden vereinbarten Servicepakets […]“. (Fabasoft, AGB, 2013), Punkt 8.1.
Google Apps
Was die Verfügbarkeit der Dienste betrifft, so deckt dies die SLA (Google, Google Apps Service Level Agreement, 2013) ab. Spezifische Sicherheitsmaßnahmen werden in den AGB nicht erwähnt, es wird nur von „angemessenen Sicherheitsstandards“ gesprochen (Google, Online Agreement, 2013), Punkt 1.1.
Microsoft Office 365
Ja, Microsoft nennt spezifische Sicherheitsmaßnahmen (Microsoft, Dienstkontinuität, 2013).
Salesforce
Salesforce führt im Agreement dazu folgendes an: „[…] We will maintain administrative, physical,

and technical safeguards for protection of the security, confidentiality and integrity of Your Data, as described in the Documentation.“ (Salesforce, Master Subscription Agreement, 2013), Punkt 3. Unter Dokumentation (Salesforce, Sicherheitsüberblick, 2013) werden die Maßnahmen detaillierter angeführt.
SAP Sales OnDemand
SAPs AGB beschreiben die Leistungen in (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Punkt 3 bezüglich Sicherheit und Verfügbarkeit, spricht allerdings nur von „[…] Sicherheitstechnologien in wirtschaftlich angemessenen Umfang“ (Punkt 3.2).

5.5.2.2 Datenschutz

a. Existiert ein definierter Datenschutzbeauftragter als Ansprechpartner für den Kunden?
Dropbox
Keine definierte Person mit derartigen Funktionen beziehungsweise keine entsprechenden Referenzen gefunden.
Fabasoft Folio Cloud
Keine definierte Person mit derartigen Funktionen beziehungsweise keine entsprechenden Referenzen gefunden.
Google Apps
Es existiert ein Account-Manager („ […] ist jene Person bei Google, die Kunden beim Erwerb von Diensten betreut.“ (Google, Vereinbarung, 2013), Punkt 15. Allerdings fungiert diese Person nicht als Datenschutzbeauftragter.
Microsoft Office 365
Keine definierte Person mit derartigen Funktionen beziehungsweise keine entsprechenden Referenzen gefunden.
Salesforce
Keine definierte Person mit derartigen Funktionen beziehungsweise keine entsprechenden Referenzen gefunden.
SAP Sales OnDemand
Ja. (SAP, AGB, 2013) Anhang „Anlage Auftragsdatenverarbeitung“, Punkt 4.6. In neuerer AGB ist nichts davon zu finden (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013).

b. Existieren Regeln für die Benachrichtigung, Auskunft und Löschung von personenbezogenen Daten auf Anfrage von Betroffenen?
Dropbox
Nein, müssten aber laut Safe-Harbor-Abkommen gegeben sein. (US Department of Commerce, 2013), Access.
Fabasoft Folio Cloud
Ja, solche Regelungen sind vorhanden (Fabasoft, Performance Characteristics of Data Security, 2013), Punkte 17, 18 und 19.
Google Apps
Ja, Google bietet dies an (Google, Vereinbarung, 2013), Punkt 6. Weiters müssten derartige Regeln laut Safe-Harbor-Abkommen vorhanden sein.
Microsoft Office 365

Ja. (Microsoft, Es sind ihre Daten, 2013).
Salesforce
Ja. Müssten auch laut Safe-Harbor-Abkommen vorhanden sein. (Salesforce, Unterstützung der Datenschutzeinhaltung, 2013).
SAP Sales OnDemand
Ja, SAP hat derartige Regelungen bedacht (SAP, AGB, 2013), Punkt „Anlage Auftragsdatenverarbeitung“ 3
c. Wo werden die Daten gespeichert und verarbeitet? i. ausschließlich in Österreich ii. ausschließlich im EU/EWR Raum iii. ausschließlich in Staaten mit angemessenen Datenschutzniveau lt. Definition der EU Kommission (Schweiz, Australien etc.) iv. international
Dropbox
Dropbox nutzt Amazon S3 zur Speicherung, folglich könnte eine Region zur Speicherung und Verarbeitung spezifiziert werden (Amazon, Amazon S3, 2013)-(Amazon S3 Functionalities). Datenzentren für den EU-Raum befinden sich in Irland. Inwieweit Dropbox die Möglichkeit der regionalen Verarbeitung und Speicherung verwendet ist offen.
Fabasoft Folio Cloud
Ausschließlich in Österreich, Deutschland oder Schweiz. (Fabasoft, Performance Characteristics of Data Security, 2013), Punkt 4.
Google Apps
Laut Google sind Googles Rechenzentren weltweit verteilt (Google, Standorte Rechenzentren, 2013). Insofern kann gefolgert werden, dass Daten international gespeichert und verarbeitet werden. Siehe auch (Google, Vereinbarung, 2013), Punkt 1.1.
Microsoft Office 365
Daten aus dem EU-Raum werden im EU-Raum oder in den USA gespeichert. (Microsoft, Where is my Data, 2013) (Microsoft, Office 365 – Datenschutzbestimmungen, 2013).
Salesforce
Die Details über den Speicherort waren nicht auffindbar, die Datenzentren sind allerdings an internationalen Standorten (USA, Asien und Europa) angesiedelt (Salesforce, System status, 2013). Salesforce ist dem Safe-Harbor-Abkommen beigetreten.
SAP Sales OnDemand
SAPs Datenzentren befinden sich in den USA, EU und Australien (SAP, NAVIGATOR (SAP-Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“. Wie weit man als Kunde auf den Speicherort der Daten eingehen kann, ist aktuell nicht bekannt.
d. Werden die Daten außerhalb des EU/EWR Raums verarbeitet und gespeichert? i. Wenn ja, ist ein angemessenes Datenschutzniveau sichergestellt (Safe-Harbor-Abkommen etc.)? ii. Besteht die Möglichkeit die Datenhaltung auf Österreich oder den EU-/EWR-Raum einzugrenzen?
Dropbox
Sowohl Dropbox als auch Amazon sind Safe-Harbor-zertifiziert. (Amazon, Amazon Agreement,

2013), Punkt 3.2, und (Dropbox, Dropbox Sicherheit, 2013), Punkt „Zertifizierungen und Konformität“.
Fabasoft Folio Cloud
Verarbeitung und Speicherung erfolgt ausschließlich in Österreich, Deutschland oder Schweiz. (Fabasoft, Performance Characteristics of Data Security, 2013), Punkt 4.
Google Apps
Google ist dem Safe-Harbor-Abkommen beigetreten, folglich ist ein gewisses Datenschutzniveau gegeben. Über den Standort der Datenverarbeitung gibt Google keine Auskünfte, eine Begrenzung auf den EU-Raum ist auf jeden Fall nicht vorgesehen (Google, Certification & data privacy, 2013), Punkt „Are there any legal provisions that stipulate that a company’s data must be stored within its own country, the EU, the EEA?“.
Microsoft Office 365
Zu (i.): Ja. (Microsoft, Office 365 – Datenschutzbestimmungen, 2013) (Speicherort der Daten). Zu (ii.): Beschränkungen auf Österreich sind nicht möglich, da hier keine Datenzentren unterhalten werden.
Salesforce
Salesfore steht unter dem Safe-Harbor-Abkommen. Datenzentren im EU-Raum sind verfügbar, inwieweit sie wählbar sind bzw. welche Zentren speziell für Backups ausgewählt werden, ist offen. (Salesforce, System status, 2013).
SAP Sales OnDemand
Zu (i.) (SAP, AGB, 2013), Anhang „Auftragsdatenverabeitung“, Punkt 8.3 nennt „EU-Standardvertragsklauseln“. Zu (ii.) Eingrenzung sollte möglich sein (SAP, NAVIGATOR (SAP-Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „physical security“ („Customer data always stays in same national jurisdiction.“); inwieweit dies umgesetzt wird, ist nicht bekannt.
e. Sind die Verantwortlichkeiten des Auftragnehmers hinsichtlich der Umsetzung von Weisungen und technischen Schutzmaßnahmen gemäß DSG exakt definiert?
Dropbox
(Dropbox, Dropbox Sicherheit, 2013) nennt Details. (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 3 nennt einen „wirtschaftlich zumutbaren Sicherheitsstandard“.
Fabasoft Folio Cloud
Sie sind nicht in den AGB (Fabasoft, AGB, 2013), aber in (Fabasoft, Performance Characteristics of Data Security, 2013) genauer definiert.
Google Apps
Die Verantwortlichkeiten sind definiert (Google, Vereinbarung, 2013), Punkt 1.1. Allerdings wird hier nicht genauer auf technische Details eingegangen. Einige Details findet man in (Google, IT Security White Paper, 2013).
Microsoft Office 365
(Microsoft, Security, Audits and Certification, 2013), Punkt „Does Microsoft allow customers to audit Office 365 or Dynamics CRM Online controls or infrastructure?“ – „Allowing potentially thousands of customers to audit our services would not be a scalable practice and might compromise security.“
Salesforce
(Salesforce, Master Subscription Agreement, 2013), Punkt 9.2 garantiert Schutzmaßnahmen auf Basis der Dokumentation des Produkts.
SAP Sales OnDemand
Ja, Verantwortlichkeiten bezüglich technischer Schutzmaßnahmen sind definiert (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.

f. Sind der Umfang, die Art und der Zweck der Verarbeitung und Speicherung von Daten und der Kreis der Betroffenen definiert?
Dropbox
Ja, ist definiert. (Dropbox-Datenschutzrichtlinien, 2013), Punkte 1, 2 und 3.
Fabasoft Folio Cloud
Ja., Fabasoft hat Umfang, Art und Zweck definiert (Fabasoft, AGB, 2013), Punkt 13.
Google Apps
(Google, Datenschutzerklärung und Nutzungsbestimmung, 2013) legt Art, Zweck und Verarbeitung fest bzw. inwieweit und unter welchen Umständen Daten weitergegeben werden. Das Safe-Harbor-Abkommen sollte die Vertrauenswürdigkeit von Subauftragnehmern regeln.
Microsoft Office 365
Ja, Umfang, Art und Zweck sind definiert (Microsoft, Vorreiter in Sachen Transparenz, 2013) (Microsoft, Administrative Access, 2013).
Salesforce
Ja, Umfang, Art und Zweck sind definiert (Salesforce, Salesforce Privacy Policy, 2013).
SAP Sales OnDemand
Ja, Umfang, Art und Zweck sind definiert (SAP, Privacy, 2013).
g. Wie lange und wo werden Daten, welche sich auf die eigentlichen Nutzerdaten beziehen (Verkehrs- und Metadaten) gehalten?
Dropbox
Laut (Dropbox-Datenschutzrichtlinien, 2013), Punkt 5: „Wir speichern Ihre Informationen solange Ihr Konto aktiv ist oder dies zur Erbringung unserer Leistungen für Sie erforderlich ist [...]“. Auf die Verkehrs- bzw. Metadaten wird nicht eingegangen.
Fabasoft Folio Cloud
Es wurden keine Angaben dazu gefunden.
Google Apps
Löschung von Daten wird in (Google, IT Security White Paper, 2013), Punkt „Data Deletion“ beschrieben. Auf die Metadaten bzw. Verkehrsdaten wird nicht genauer eingegangen.
Microsoft Office 365
Es wurden keine Angaben dazu gefunden.
Salesforce
Es wurden keine Angaben dazu gefunden.
SAP Sales OnDemand
„SAP hält persönliche Daten nur so lange vor, wie es der Zweck oder die rechtlichen Bestimmungen erfordern, für die sie erhoben wurden.“ (SAP, Privacy, 2013), Punkt „Datenhaltung“
h. Sind jene Fälle, welche den Schutz personenbezogener Daten verletzen exakt definiert, sodass der Kunde Betroffene gemäß DSG benachrichtigen kann?
Dropbox
Es sind keine Fälle definiert beziehungsweise nicht öffentlich zugänglich.
Fabasoft Folio Cloud
Es sind keine Fälle definiert beziehungsweise nicht öffentlich zugänglich.

Google Apps
Es sind keine Fälle definiert beziehungsweise nicht öffentlich zugänglich.
Microsoft Office 365
(Microsoft, Office 365 – Datenschutzbestimmungen, 2013), Punkt „Sicherheit“ spezifiziert zumindest wann keine Benachrichtigung erfolgt.
Salesforce
Es sind keine Fälle definiert beziehungsweise nicht öffentlich zugänglich.
SAP Sales OnDemand
Es sind keine Fälle definiert beziehungsweise nicht öffentlich zugänglich.
i. Sind technische und organisatorische Schutzmaßnahmen gemäß §14 DSG ausreichend dokumentiert und dem Kunden zugänglich?
Dropbox
(Dropbox-Datenschutzrichtlinien, 2013), Punkt 8 geht minimal auf technische Maßnahmen ein. Details finden sich in (Dropbox, Dropbox Sicherheit, 2013), Punkt „Datenschutz“. Amazon (Amazon Overview of Security Processes- WhitePaper, 2013) informiert umfassend über die verwendeten Schutzmaßnahmen.
Fabasoft Folio Cloud
Fabasofts Sicherheitsdokumentation der Datenzentren (Fabasoft, Performance Characteristics of Data Center Operation, 2013) bzw. Dokumentation der Datensicherheit (Fabasoft, Performance Characteristics of Data Security, 2013) ist ohne weiteres zugänglich. Was organisatorische Maßnahmen betrifft, so muss man sich auf diverse Zertifikate verlassen, ohne genaue Details zu erfahren. (Fabasoft, Fabasoft Zertifikate, 2013).
Google Apps
Ausreichende Schutzmaßnahmen sind attestiert über SAS 70 Type II. Allerdings sind Details darüber dem Kunden nicht zugänglich. (Google, IT Security White Paper, 2013) ist dafür öffentlich zugänglich.
Microsoft Office 365
Technische Details sind via White Papers gut zugänglich (Microsoft, Security in Office 365 White Paper, 2013) und Websites (Microsoft, Privacy in the Public Cloud: The Office 365 Approach, 2013). Details über organisatorische Maßnahmen sind nicht ohne weiteres einsehbar.
Salesforce
Technische Details sind via White Papers (Salesforce, Security White Paper, 2013) und Websites (Salesforce, Sicherheitsüberblick, 2013) zu ermitteln.
SAP Sales OnDemand
Ja. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.3.
j. Wie wird der Kunde im Falle eines Datenverlustes oder einer Verletzung der Datenvertraulichkeit informiert?
Dropbox
Dazu wurde in den Bedingungen oder Dokumentationen, die Dropbox veröffentlicht hat, nichts gefunden.
Fabasoft Folio Cloud
Dazu wurde in den Bedingungen oder Dokumentationen, die Fabasoft veröffentlicht hat, nichts gefunden.
Google Apps

Mitteilungen sind in schriftlicher Form zu verfassen (Google, Online Agreement, 2013), Punkt 14.1. (Google, Online Agreement, 2013), Punkt 9.1 „Security Breach Notification Law“.
Microsoft Office 365
Mitteilung erfolgt schriftlich (Brief oder E-Mail), allerdings nur für Unternehmen (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 13.e. Ansonsten wird z.B. per E-Mail benachrichtigt (Microsoft, Office 365 – Datenschutzbestimmungen, 2013), Punkt „Sicherheit“.
Salesforce
Dazu wurde in den Bedingungen oder Dokumentationen, die Salesforce veröffentlicht hat, nichts gefunden.
SAP Sales OnDemand
Ja, der Kunde wird informiert (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.5.

5.5.2.3 Sicherheitsmaßnahmen

a. Sind alle wichtigen Versorgungskomponenten (Strom, Klimatisierung des Rechenzentrums, Verkabelung etc.) redundant angelegt?
Dropbox
Ja, die verwendeten Rechenzentren sind derartig angelegt (Amazon Overview of Security Processes-WhitePaper, 2013).
Fabasoft Folio Cloud
Ja, die Rechenzentren sind derartig angelegt (Fabasoft, Performance Characteristics of Data Center Operation, 2013), Punkt 1.2 bzw. (Fabasoft, Cloud Assurance, 2013), Punkt „Physical Security“.
Google Apps
Laut (Google, Rechenzentren- Daten und Sicherheit, 2013) verfügen die Rechenzentren über Notfall–Generatoren, um bei Stromausfall weiter versorgt werden zu können. Die Rechenzentren als solches sind redundant angelegt, sh. (Google, Rechenzentren- Daten und Sicherheit, 2013).
Microsoft Office 365
Durch ISO 27001 gegeben beziehungsweise auf Website (Microsoft, Microsoft Dynamics CRM Online Security and Service Continuity, 2013), Punkt „Physical security“, beschrieben.
Salesforce
Ja, Salesforces Rechenzentren sind so angelegt (Salesforce, Sicherheitsüberblick, 2013), Punkt „Power“, „Network“.
SAP Sales OnDemand
Ja, laut (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“, so ist dies gegeben.
b. Werden Zutritte zum Rechenzentrum durch Zutrittskontrollsysteme, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal und Alarmsysteme angemessen überwacht und geregelt?
Dropbox
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (Amazon, Amazon Web Services: Overview of Security Processes, 2013), Punkt „Physical Security“.
Fabasoft Folio Cloud
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (Fabasoft, Performance Characteristics of Data Center Operation, 2013), Punkt 2.1.; weiter durch ISO 27001 Zertifikat gegeben.

Google Apps
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (Google, Google Apps Trust- Sicherheit, 2013), Punkt „Wie garantiert Google die physische Sicherheit der Datenzentren-Standorte?“
Microsoft Office 365
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (Microsoft, Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit , 2013) (Datenschutz- und Sicherheitsfunktionen von Office 365) bzw. (Microsoft, Microsoft Dynamics CRM Online Security and Service Continuity, 2013), Punkt „Physical Security“.
Salesforce
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (Salesforce, Sicherheitsüberblick, 2013), Punkt „Access Control and Physical Security“.
SAP Sales OnDemand
Ja, der Zutritt zu Rechenzentren wird überwacht und geregelt (SAP, NAVIGATOR (SAP- Partner) - Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“.
c. Wird der Zutritt zum Rechenzentrum durch Zwei-Faktor-Authentifizierung geregelt?
Dropbox
Ja. (Amazon, Amazon Web Services: Overview of Security Processes, 2013), Punkt „Physical Security“.
Fabasoft Folio Cloud
Nichts dergleichen wird in der Dokumentation erwähnt (Fabasoft, Performance Characteristics of Data Center Operation, 2013). Möglicherweise deckt allerdings eines der Zertifikate diese Maßnahme ab.
Google Apps
Zwei-Faktoren-Authentifizierung wird nicht erwähnt, allerdings nennt Google biometrische Verfahren, um physische Sicherheit zu gewährleisten. (Google, Google Apps Trust- Sicherheit, 2013), Punkt „Wie garantiert Google die physische Sicherheit der Datenzentren-Standorte?“.
Microsoft Office 365
Ja. (Microsoft, Administrative Access, 2013) („What controls are in place to restrict physical access to my data?“).
Salesforce
Ja. (Salesforce, Sicherheitsüberblick, 2013), Punkt „Access Control and Physical Security“.
SAP Sales OnDemand
Ja. (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“.
d. Sind Maßnahmen zur Brandbekämpfung und -vermeidung angemessen umgesetzt (Brandmeldeanlagen, Branderkennung, Löschanlagen, Brandschutzübungen etc.)?
Dropbox
Ja. (Amazon Overview of Security Processes- WhitePaper, 2013), Punkt „Fire detection and suppression“
Fabasoft Folio Cloud
Ja. (Fabasoft, Performance Characteristics of Data Center Operation, 2013), Punkt 2.1.
Google Apps
Ja, laut Googles' Video zu den Datenzentren (Google, Data center security video, 2013).
Microsoft Office 365
Ja, durch ISO 27001 gegeben bzw. (Microsoft, Microsoft Dynamics CRM Online Security and Service

Continuity, 2013), Punkt „Physical Security“.
Salesforce
Ja, (Salesforce, Sicherheitsüberblick, 2013), Punkt „Fire“.
SAP Sales OnDemand
Ja. (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“ bzw. ISO 27001.
e. Ist die bauliche Infrastruktur robust genug ausgeführt, um Elementarschäden und Einbruchsversuchen entgegenzuwirken?
Dropbox
Ja, muss nach ISO 27001 A.9.1.4 gegeben sein, Amazon ist ISO 27001 zertifiziert.
Fabasoft Folio Cloud
Durch ISO 27001 gegeben. Weiters bestätigt Fabasoft dies auch in der Dokumentation (Fabasoft, Cloud Assurance, 2013), Punkt „Umweltbedingte Sicherheitsmaßnahmen“.
Google Apps
Ja. (Google, IT Security White Paper, 2013), Punkt „Physical security“.
Microsoft Office 365
Ja. Durch ISO 27001 gegeben bzw. wird dies in der Dokumentation bestätigt (Microsoft, Microsoft Dynamics CRM Online Security and Service Continuity, 2013), Punkt „Physical security“.
Salesforce
Ja. (Salesforce, Sicherheitsüberblick, 2013), Punkt „Access Control and Physical Security“.
SAP Sales OnDemand
Ja. (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Physical Security“ bzw. ISO 27001.
f. Sind die Rechenzentren redundant ausgelegt und so weit voneinander entfernt, dass Schadensfälle nicht beide Rechenzentren gleichzeitig treffen können, um den Betrieb im Falle des Ausfalls eines Rechenzentrums aufrechterhalten zu können?
Dropbox
Amazon garantiert laut (Amazon, Amazon SLA, 2013) eine 99,999999999 %ige Langlebigkeit und 99,99 %-ige Verfügbarkeit aller gespeicherten Objekte. (Amazon, Amazon Web Services: Overview of Security Processes, 2013), Punkt „Backups“ bzw. (Amazon, Amazon S3, 2013), Punkt „Data Durability and Reliability“.
Fabasoft Folio Cloud
Ja. (Fabasoft, Cloud Assurance, 2013), Punkt „Umweltbedingte Sicherheitsmaßnahmen“.
Google Apps
Ja. Laut (Google, Rechenzentren- Daten und Sicherheit, 2013) bzw. (Google, Standorte Rechenzentren, 2013) und (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google protect the systems from computer outages and natural catastrophes?“.
Microsoft Office 365
Ja. (Microsoft, Dienstkontinuität, 2013) bzw. (Microsoft, Microsoft Dynamics CRM Online Security and Service Continuity, 2013), Punkt „Physical Security“.
Salesforce
Ja. (Salesforce, System status, 2013) bzw. (Salesforce, Security White Paper, 2013), Punkt „Physical Security“.
SAP Sales OnDemand
Ja. (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security &

Compliance Update, 2013), Punkt „Backup & Recovery“ bzw. ISO 27001.
g. Sind technische Maßnahmen zum Schutz der Server angemessen implementiert (Firewalls, regelmäßige Integritätsüberprüfungen, host-based intrusion detection systems etc.)?
Dropbox
Ja, Amazon führt derartiges in seinen White Papers an (Amazon Overview of Security Processes- WhitePaper, 2013), Punkt „Network Security“.
Fabasoft Folio Cloud
Ja, Fabasoft führt solche Maßnahmen in der Dokumentation an (Fabasoft, Performance Characteristics of Data Center Operation, 2013), Punkt 1.2.
Google Apps
Ja, Google nennt solche Maßnahmen (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google protect the infrastructure from hackers and other threats?“.
Microsoft Office 365
ISO 27001 Zertifikat sollte sicherstellen, dass solche Maßnahmen implementiert sind.
Salesforce
Ja, Salesforce führt solche Maßnahmen in der Dokumentation an (Salesforce, Sicherheitsüberblick, 2013), Punkt „Interne Tests/Bewertungen und Tests/Bewertungen durch Dritte“.
SAP Sales OnDemand
Ja, Solche Maßnahmen sind in der Präsentation genannt (SAP, NAVIGATOR (SAP- Partner) - Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security“.
h. Besitzen die Server eine sichere Grundkonfiguration (Deaktivierung unnötiger Dienste, gehärtete Betriebssysteme etc.)?
Dropbox
Ja, laut Amazons White Paper (Amazon Overview of Security Processes- WhitePaper, 2013).
Fabasoft Folio Cloud
Ja, laut der Fabasoft Dokumentation (Fabasoft, Performance Characteristics of Data Center Operation, 2013).
Google Apps
Ja, laut Googles Trust-Website (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google protect the infrastructure from hackers and other threats? “und einem White Paper (Google, IT Security White Paper, 2013), Punkt „Operating System Security“.
Microsoft Office 365
Microsoft macht dazu keine Angaben.
Salesforce
Ja, laut der Salesforce Dokumentation (Salesforce, Security White Paper, 2013), Punkt „Force.com cloud platform security“.
SAP Sales OnDemand
Es können keine Angaben über die Betriebssysteme in Datenzentren gefunden werden.
i. Sind Sicherheitsmaßnahmen gegen Malware angemessen implementiert (Virenschutz, Firewall etc.)?

Dropbox
Ja, laut Amazons White Paper (Amazon Overview of Security Processes- WhitePaper, 2013).
Fabasoft Folio Cloud
Ja, laut Fabasofts Dokumentation (Fabasoft, Performance Characteristics of Data Center Operation, 2013).
Google Apps
Ja, Googles Trust-Website führt derartiges an (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google protect the infrastructure from hackers and other threats?“ ebenso, wie Googles Security White Paper (Google, IT Security White Paper, 2013), Punkt „Operational security“.
Microsoft Office 365
ISO 27001 Zertifikat sollte sicherstellen, dass solche Maßnahmen implementiert sind. Ansonsten wurden keine Angaben dazu gefunden.
Salesforce
Ja, laut Salesforces Dokumentation sind solche Maßnahmen implementiert (Salesforce, Security White Paper, 2013), Punkt „Force.com cloud platform security“.
SAP Sales OnDemand
Ja. (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security“.
j. Sind Sicherheitsmaßnahmen gegen netzbasierte Angriffe angemessen implementiert (IPS/IDS-Systeme, Firewalls, Gateways etc.)?
Dropbox
Ja, laut Amazons White Paper (Amazon Overview of Security Processes- WhitePaper, 2013).
Fabasoft Folio Cloud
Ja, laut Fabasofts Dokumentation sind solche Maßnahmen implementiert (Fabasoft, Performance Characteristics of Data Security, 2013).
Google Apps
Ja, Googles White Paper führt solche Maßnahmen an (Google, IT Security White Paper, 2013), Punkt „Operational security“.
Microsoft Office 365
Das ISO 27001 Zertifikat soll sicherstellen, dass solche Maßnahmen implementiert sind. Ansonsten wurden keine Angaben dazu gefunden.
Salesforce
Ja, Salesforce führt solche Maßnahmen in einem White Paper an (Salesforce, Security White Paper, 2013), Punkt „Force.com cloud platform security“.
SAP Sales OnDemand
Ja, laut einer SAP Presentation (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security“.
k. Sind Maßnahmen zur DDoS-Angriffsabwehr implementiert?
Dropbox
Ja, Amazons White Paper führt solche Maßnahmen an (Amazon Overview of Security Processes- WhitePaper, 2013), Punkt „Network Monitoring and Protection“.
Fabasoft Folio Cloud
Es wurden keine Details dazu gefunden, allerdings sollten Maßnahmen dazu implementiert sein, um dem ISO 27001 Zertifikat zu genügen.
Google Apps

Ja, laut Googles Website (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google protect the infrastructure from hackers and other threats? “und Googles Whitepaper (Google, IT Security White Paper, 2013), Punkt „Network Security“.
Microsoft Office 365
Ja. Microsoft beschreibt Maßnahmen in einem Whitepaper (Microsoft, Security in Office 365 White Paper, 2013).
Salesforce
Laut der Sicherheitsdokumentation (Salesforce, Secure, private, and trustworthy: enterprise cloud computing with Force.com, 2013) sind Maßnahmen dazu implementiert.
SAP Sales OnDemand
Ja, laut einer SAP Presentation führt solche Maßnahmen an (SAP, NAVIGATOR (SAP- Partner) - Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security. multiple redundant Internet connections“.
l. Existiert eine geeignete Netzsegmentierung (Managementnetz vs. Datennetz)?
Dropbox
Es waren keine Angaben seitens Dropbox dazu auffindbar. Amazon trennt sein Netze laut einer Website (Amazon, Amazon Web Services: Overview of Security Processes, 2013), Punkt „Network security – Amazon Corporate Segregation“
Fabasoft Folio Cloud
Es wurden keine Angaben dazu gefunden.
Google Apps
Laut einem Google Whitepaper werden die Netze getrennt (Google, IT Security White Paper, 2013), Punkt „Network Security“.
Microsoft Office 365
Ja, laut einem Whitepaper erfolgt eine Trennung der Netze (Microsoft, Security in Office 365 White Paper, 2013), Punkt „Secure Network“.
Salesforce
Es wurden keine Angaben dazu gefunden.
SAP Sales OnDemand
Es wurden keine Angaben dazu gefunden.
m. Sind alle Komponenten der Cloud-Architektur sicher konfiguriert?
Dropbox
Keine exakten Angaben dazu gefunden. Aussage Dropbox Website: „Die Sicherheit der Website und auch der Client-Software von Dropbox wird ständig verbessert, um sie widerstandsfähiger zu machen und vor Angriffen zu schützen.“ (Dropbox, Wie sicher ist Dropbox?, 2013).
Fabasoft Folio Cloud
Ja, laut Fabasoft Website (Fabasoft, Sicher und Zuverlässig, 2013).
Google Apps
Laut Googles Whitepaper (Google, IT Security White Paper, 2013) sind die Komponenten sicher konfiguriert.
Microsoft Office 365
Es wurden keine exakten Angaben dazu gefunden. Microsoft Security Website (Microsoft, Security, Audits and Certification, 2013) geht nicht weiter auf die Sicherheit von Desktop-Applikationen bzw. Webpages ein.
Salesforce

Es wurden keine exakten Angaben dazu gefunden. Salesforce scheint OWASP als Web-Standard zu berücksichtigen. Wie sicher mobile Applikationen sind, ist offen. (Salesforce, Secure, private, and trustworthy: enterprise cloud computing with Force.com, 2013)
SAP Sales OnDemand
Keine exakten Angaben dazu gefunden. Die SAP Website (SAP, Protecting your data – and your business securely with SAP, 2013) gibt an, sich intensiv mit Sicherheit und Software-Qualität zu beschäftigen.
n. Ist sichergestellt, dass die Fernadministration nur über einen sicheren Kommunikationskanal (SSH, IPSec, VPN etc.) erfolgen kann?
Dropbox
Es wurden keine Angaben dazu gefunden.
Fabasoft Folio Cloud
Es wurden keine Angaben dazu gefunden.
Google App
Ja. Google nutzt SSH für die Fernadministration (Google, IT Security White Paper, 2013), Punkt „Information Access“
Microsoft Office 365
Es wurden keine Angaben dazu gefunden.
Salesforce
Es wurden keine Angaben dazu gefunden.
SAP Sales OnDemand
Die SAP Support Website (SAP, Setup von Serviceverbindungen für den Remote Support durch SAP, 2013) beschreibt drei Verbindungstypen für den Zugriff auf NetWeaver Server (ob diese Systeme in der Cloud benutzt werden, war nicht herauszufinden). Wie sicher diese Verbindungstypen sind, war der Beschreibung nicht zu entnehmen.
o. Erfolgt die Verschlüsselung zwischen den Cloud-Standorten mit ausreichend sicherer Verschlüsselung?
Dropbox
Dropbox nutzt während der Übertragung AES-256 (Dropbox, Dropbox Security Guide, 2013).
Fabasoft Folio Cloud
Fabasofts Kommunikation erfolgt über SSL bzw. HTTPS (Fabasoft, Cloud Assurance, 2013), Punkt „Identitäts- und Zugriffsmanagement“.
Google Apps
Laut Googles Whitepaper (Google, IT Security White Paper, 2013) wird der Verkehr zwischen Standorten mit SSL verschlüsselt.
Microsoft Office 365
Ja, laut Microsofts Whitepaper (Microsoft, Security in Office 365 White Paper, 2013)-(Encryption).
Salesforce
Ja, laut der Salesforce Website (Salesforce, Is all traffic to and from Salesforce.com APIs are encrypted ?, 2013).
SAP Sales OnDemand
Ja, SAP nutzt TLS 256-Bit Verschlüsselung zwischen den Standorten (SAP, NAVIGATOR (SAP-Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security“.

p. Erfolgt die Verschlüsselung mit Subauftragnehmern mit ausreichend sicherer Verschlüsselung?
Dropbox
Ja, Amazon nutzt sichere Verschlüsselung (Amazon, Amazon S3, 2013), Punkt „Data Security Details“.
Fabasoft Folio Cloud
Laut Fabasoft Website (Fabasoft, Cloud Assurance, 2013), Punkt „Supply-Chain Assurance “ werden “Cloud-Dienste […] ausschließlich mit Fabasoft-eigener Wertschöpfung zur Verfügung […] gestellt”.
Google Apps
Laut dem Whitepaper verschlüsselt Google keine gespeicherten Daten, sondern lediglich die Kommunikation (Google, IT Security White Paper, 2013).
Microsoft Office 365
Microsofts Whitepaper (Microsoft, Security in Office 365 White Paper, 2013), Punkt „Built-in Security“ bzw. „Advanced Encryption“ geht detailliert auf die Verschlüsselung von Kundendaten ein.
Salesforce
Salesforces Whitepaper (Salesforce, Security White Paper, 2013) beschreibt, wie auch ruhende Daten verschlüsselt werden können. Zur Übermittlung wird SSL benutzt. Allerdings wird nicht weiter auf eventuelle Subauftragnehmer eingegangen.
SAP Sales OnDemand
Laut SAPs AGB (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2 darf der Subauftragnehmern nicht weniger Schutz bieten als SAP selbst, folglich muss auch dieser Verschlüsselung unterstützen.
q. Wie wird der Zugriffsschutz auf die gespeicherten Daten, insbesondere in Hinsicht auf internes Personal, gewährleistet?
Dropbox
Seitens Dropbox bestehen Regeln (Dropbox, Dropbox Security Guide, 2013), Punkt „Access Control“. Amazon macht dazu keine Angaben.
Fabasoft Folio Cloud
Laut Fabasofts Dokumentation (Fabasoft, Performance Characteristics of Data Security, 2013), Punkt „Sicherheit auf Anwendungsebene“ kommt eine ACL zum Einsatz.
Google Apps
Google stellt die Zugriffkontrolle durch eindeutige User ID und Zugriffsrechte basierend auf der Personalposition sicher (Google, IT Security White Paper, 2013), Punkt „Access Control“. In der Regel haben Mitarbeiter keinen Zugriff auf Kundendaten.
Microsoft Office 365
Office 365 bietet Zugriff auf Rollenbasis. Ein Zugriff kann eindeutig auf eine Person zurückgeführt werden. Zugriff auf Kundendaten von internem Personal kann nur unter bestimmten Umständen erfolgen, wobei dazu Regelungen existieren. (Microsoft, Administrative Access, 2013), Punkt „Who has administrative rights to Office 365 or Microsoft Dynamics CRM Online?“
Salesforce
Es wird gewährleistet, dass Mitarbeiter keinen unerlaubten Zugriff auf Daten haben (Salesforce, Master Subscription Agreement, 2013), Punkt 3.2.
SAP Sales OnDemand
SAP garantiert, dass Mitarbeiter keinen Zugriff auf Kundendaten haben (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.3.

5.5.2.4 Anwendungssicherheit

a. Ist Sicherheit Bestandteil des Software Development Life Cycle Prozesses (Reviews, automatisierte Tests, Vulnerability Tests etc.)
Dropbox
Dropbox macht keine Angaben über den intern genutzten Software Development Life Cycle. (Dropbox, Dropbox Sicherheit, 2013), Punkt „Ihre Daten sind sicher“ nennt nur „Sicherheitstests“, aber ob diese Teil des Entwicklungsprozesses sind, ist aus den gesichteten Unterlagen nicht erkennbar.
Fabasoft Folio Cloud
Ja. SCRUM und automatisierte Tests in Continous Integration Umgebungen. (Fabasoft, Cloud Assurance, 2013), Punkt „Betriebssicherheit“.
Google Apps
Ja. Google Website (Google, Google Apps Trust- Sicherheit, 2013), Punkt „How does Google prevent and resolve security flaws in applications?“ und ein Whitepaper (Google, IT Security White Paper, 2013), Punkt „Systems Development and Maintenance“ gehen darauf ein.
Microsoft Office 365
Ja. Ein Whitepaper geht darauf ein (Microsoft, Security in Office 365 White Paper, 2013).
Salesforce
Wie in (Salesforce, Security White Paper, 2013), Punkt „How we build secure products-testing phase“ beschrieben, wird auf Sicherheit getestet. Sicherheits-Reviews können von Kunden eingesehen werden.
SAP Sales OnDemand
Automatische Tests sind Teil des Entwicklungsprozesses. Security wird nicht detailliert erwähnt (SAP, Application Lify cycle management, 2013), Punkt „Test Management“.

b. Werden Sicherheits-Mindeststandards der zu Verfügung gestellten Web-Anwendungen eingehalten (z.B. OWASP)?
Dropbox
Es wurde nichts dergleichen gefunden, auch nicht auf der Entwicklerseite (Dropbox, Dropbox Developer, 2013).
Fabasoft Folio Cloud
Es wurde nichts dergleichen gefunden.
Google Apps
Es wurden keine Mindeststandards erwähnt, allerdings betreibt Google Forschung, um weltweite Sicherheits-Standards zu etablieren (Google, IT Security White Paper, 2013), Punkte „Information security“ und „Security in the Context of Googles Software LifeCycle“.
Microsoft Office 365
Sollte durch SDL (Microsoft, Security Development Lifecycle, 2013) gegeben sein, allerdings wird OWASP nicht erwähnt.
Salesforce
Ja, OWASP Empfehlungen werden eingehalten (Salesforce, Security White Paper, 2013), Punkt „How we build secure products“.
SAP Sales OnDemand
Ja. SAP geht auf OWASP ein (SAP, How SAP Protects Your Web Applications from Security Vulnerabilities, 2013).

c. Existiert ein definiertes Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service-Packs)?
Dropbox
Dropbox macht dazu keine Angaben. (Dropbox, Dropbox-Versionshinweise, 2013) zeigt eine gewisse Regelmäßigkeit an Updates (bzw. Bug Fixes).
Fabasoft Folio Cloud
Ja, ein monatliches Cloud-Update existiert (Fabasoft, Cloud Assurance, 2013), Punkt „Betriebssicherheit“.
Google Apps
Ja, ein Update-System existiert (Google, IT Security White Paper, 2013), Punkt „Operating System Security“.
Microsoft Office 365
Sollte durch SDL (Microsoft, Security Development Lifecycle, 2013) gegeben sein.
Salesforce
Ja, Salesforce unterstützt Patch-Management (Salesforce, Push Patch Updates, 2013).
SAP Sales OnDemand
Ja, SAP unterstützt Patch-Management (SAP, Security Patch Process FAQ, 2013).

d. Werden Patches vor dem Einspielen auf Produktivsystemen in Testumgebungen getestet?
Dropbox
Es wurden keine Angaben dazu gefunden.
Fabasoft Folio Cloud
Ja, es wird getestet (Fabasoft, Cloud Assurance, 2013), Punkt „Betriebssicherheit“, Stichwort: Continous-Integration-Umgebung.
Google Apps
Der Software Development Prozess (Google, IT Security White Paper, 2013), Punkt „Systems Development and Maintenance“ nennt „dynamic analysis of live application“. Inwieweit es sich hier um Testumgebungen handelt, ist unklar.
Microsoft Office 365
Sollte durch SDL (Microsoft, Security Development Lifecycle, 2013) gegeben sein.
Salesforce
Testen ist Teil des Software Development Life Cycle, den Salesforce forciert. (Salesforce, Security White Paper, 2013), Punkt „How we build secure products“.
SAP Sales OnDemand
Ja, SAP testet ausgiebig (SAP, Security Patch Process FAQ, 2013), Punkt 12.

5.5.2.5 Datensicherheit

a. Werden Kundendaten durch Maßnahmen wie virtuelle Speicherbereiche sicher voneinander isoliert?
Dropbox
Amazon EC2 würde so etwas bieten; S3, welches von Dropbox verwendet wird, scheinbar nicht (Amazon Overview of Security Processes- WhitePaper, 2013).
Fabasoft Folio Cloud
Es wurden keine Angaben dazu gefunden, außer ACL gilt als sichere Maßnahme (Fabasoft,

Performance Characteristics of Data Center Operation, 2013), Punkt „Sicherheit auf Anwendungsebene“.
Google Apps
Ja, Google nennt solche Maßnahmen auf der Website (Google, Google Apps Trust- Sicherheit, 2013), Punkt „Is data actually safe when it is stored on the same servers as that of other companies“.
Microsoft Office 365
Ja, Microsoft nennt solche Maßnahmen in einem Whitepaper (Microsoft, Security in Office 365 White Paper, 2013), Punkt „Isolated Customer Data“.
Salesforce
Es wurden keine Angaben dazu gefunden.
SAP Sales OnDemand
Es wurden keine Angaben dazu gefunden.
b. Werden regelmäßige Datensicherungen durchgeführt und sind deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte, Speicherdauer) für den Kunden nachvollziehbar?
Dropbox
Die Daten werden generell redundant gespeichert, allerdings nicht für den Kunden einsehbar.
Fabasoft Folio Cloud
Ja, regelmäßige Datensicherung wird in der Dokumentation erwähnt. (Fabasoft, Performance Characteristics of Data Center Operation, 2013), Punkt 2.2 „Datensicherheit“.
Google Apps
Daten werden redundant sowohl innerhalb des Datenzentrums als auch gespiegelt in anderen Datenzentren abgelegt. (Google, Rechenzentren- Daten und Sicherheit, 2013)
Microsoft Office 365
Daten werden automatisch redundant in primären und sekundären Datenzentren abgelegt. Für den Kunden nur bedingt nachvollziehbar (Speicherort sollte in der „Nähe“ sein, sonstige Backupfunktionen werden eher vor dem Kunden versteckt) (Microsoft, Where is my Data, 2013).
Salesforce
Ja, Datensicherung wird von Salesforce behandelt (Salesforce, Sicherheitsüberblick, 2013), Punkt „Systemwiederherstellung“. Für den Kunden ist dies allerdings nicht unbedingt nachvollziehbar.
SAP Sales OnDemand
Ja, SAPs Presentation nennt Datensicherung als Maßnahme (SAP, NAVIGATOR (SAP- Partner) - Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Backup and Recovery“. Für den Kunden ist die Datensicherung nicht unbedingt nachvollziehbar.
c. Ist die technische Umsetzung der Löschung von Daten genau definiert und ihre tatsächliche nachweisliche Lösung gewährleistet (welche Policy, Löschverfahren, Umgang mit Backup-Medien, Wiederverwendung der Datenträger)?
Dropbox
Die Dropbox-AGB (Dropbox, Allgemeine Geschäftsbedingungen, 2013), Punkt 5 beschreiben, dass Dropbox auch endgültig löscht. Amazon ist ISO 27001 zertifiziert, sollte folglich auch A.9.2.6 implementieren.
Fabasoft Folio Cloud
Fabasoft ist unter ISO 27001 zertifiziert, wo der Löschprozess genau definiert ist: ISO 27001 Annex A.10.7.2 gibt solche Maßnahmen vor.
Google Apps
Die Google-AGB (Google, Vereinbarung, 2013), Punkt 11.2 behandeln die Löschung der Daten nach

Kündigung. Weiters zerstört Google Festplatten, deren Lebensdauer überschritten wurde (Google, Rechenzentren- Daten und Sicherheit, 2013) bzw. (Google, IT Security White Paper, 2013), Punkt „Media Disposal“, folglich ist auch die Wiederverwendung von Datenträger limitiert.
Microsoft Office 365
ISO 27001 Annex A.10.7.2 gibt solche Maßnahmen vor (Microsoft Office 365 ist ISO 27001 zertifiziert).
Salesforce
(Salesforce, Master Subscription Agreement, 2013) Punkt 12.5 geht auf die Löschung ein, gibt allerdings keine Details preis: „[…] will thereafter delete or destroy all copies of Your Data in Our systems or otherwise in Our possession or control as provided in the Documentation, unless legally prohibited.“ Das ISO 27001 Zertifikat sollte allerdings gewährleisten, dass derartige Maßnahmen implementiert sind.
SAP Sales OnDemand
Ja. SAP nennt solche Maßnahmen in den AGB (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.8

5.5.2.6 Verschlüsselung und Schlüsselmanagement

a. Werden alle Daten des Kunden verschlüsselt gespeichert?
Dropbox
Daten, die der Kunde speichert, werden AES-256 verschlüsselt. (Dropbox, Dropbox Security Guide, 2013). Was Daten bzw. Metadaten über den Kunden betrifft, waren keine Angaben zu finden.
Fabasoft Folio Cloud
Kommunikation wird SSL bzw. HTTPS verschlüsselt, Daten werden mithilfe von Self Encrypting Disks verschlüsselt (Fabasoft, Cloud Assurance, 2013), Punkt „Identitäts- und Zugriffsmanagement“.
Google Apps
Google verschlüsselt nur die Übertragung mit SSL, Dateinamen werden anonymisiert bzw. Daten auf zahlreiche Computer verteilt. (Google, Rechenzentren- Daten und Sicherheit, 2013).
Microsoft Office 365
Ja. Sowohl während der Übertragung als auch im Ruhezustand möglich (Microsoft, Security in Office 365 White Paper, 2013) und (Microsoft, Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit , 2013), Punkt „Die zehn wichtigsten Datenschutz- und Sicherheitsfunktionen von Office 365“.
Salesforce
(Salesforce, Security White Paper, 2013), Punkt „How You Can Encrypt Selected Data at Rest“: Verschlüsslung der Daten ist möglich (nach AES 128).
SAP Sales OnDemand
Ja. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.3 „Übertragungskontrolle“.
b. Werden Best Practices der Schlüsselverwaltung umgesetzt?
Dropbox
Es wurden keine Angaben dazu gefunden. Dropbox verwaltet die Schlüssel zentral, lässt aber zu, dass Kunden ihre Daten selbst verschlüsseln.
Fabasoft Folio Cloud

Es wurden keine Angaben dazu gefunden.
Google Apps
Es wurden keine Angaben dazu gefunden. Google nutzt Verschlüsselung allerdings auch nur für die Absicherung von Kommunikation.
Microsoft Office 365
Es wurden keine Angaben dazu gefunden.
Salesforce
(Salesforce, Security White Paper, 2013), Punkt „How You Can Encrypt Selected Data at Rest“: „It then uses key splitting to separate the keying material between application server and database so that no single salesforce.com administrator can recover both parts of the key.“
SAP Sales OnDemand
Es wurden keine Angaben dazu gefunden.

5.5.2.7 Identifikations- und Rechtemanagement

a. Ist eine Zwei-Faktor-Authentifizierung für Administratoren des Cloud-Service-Anbieters umgesetzt?
Dropbox
Dies ist technisch möglich. Soweit ersichtlich ist Zwei-Faktor-Authentifizierung aber kein zwingendes Feature für Administratoren. Ist das Feature allerdings durch den Administrator für Benutzer aktiviert worden, ist es obligatorisch (Dropbox, Dropbox Security Guide, 2013).
Fabasoft Folio Cloud
Ist technisch möglich. Wie weit dies genutzt wird, ist allerdings nicht erkenntlich (Fabasoft, Zwei-Faktor-Authentifizierung, 2013).
Google Apps
Ja, dies wird genutzt (Google, Google Apps Trust- Sicherheit, 2013), Punkt „Warum ist Google Apps sicher?“, Stichwort „Mitarbeiter“.
Microsoft Office 365
Ist technisch möglich, inwieweit dies intern genutzt wird, war nicht ersichtlich (Microsoft, Security in Office 365 White Paper, 2013), „Two-Factor Authentication“.
Salesforce
Keine Angaben dazu gefunden. Die Salesforce Website (Salesforce, Salesforce.com-Tools zur Unterstützung der Datenschutzeinhaltung, 2013) nennt nichts dergleichen.
SAP Sales OnDemand
Technisch möglich. Aber inwieweit dies für Administratoren umgesetzt ist, war aus den Unterlagen nicht ersichtlich (SAP, Multi-factor authentication, why not?, 2013).
b. Existiert eine rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte?
Dropbox
Dropbox trennt zwischen Administratoren und Nutzern, wobei unter den Nutzern weitere Account Level existieren (Dropbox, Dropbox Security Guide, 2013), Punkt „You are in control of your dropbox- As an Admin“.
Fabasoft Folio Cloud
Ja, solche Maßnahmen sind implementiert (Fabasoft, Cloud Assurance, 2013), Punkt „Identitäts- und Zugriffsmanagement“.
Google Apps

Ja, solche Maßnahmen sind implementiert (Google, IT Security White Paper, 2013), Punkt „Access Controls“.
Microsoft Office 365
Rollenbasierte Zugriffskontrolle ist implementiert und Audits der Rollenzuteilung sind vorgesehen. (Microsoft, Managing Access to the Exchange Online Service, 2013) (Microsoft, Unablässige Sicherheit, 2013).
Salesforce
Die Salesforce Website nennt nichts dergleichen (Salesforce, Unterstützung der Datenschutzeinhaltung, 2013), allerdings sollte die Einhaltung solcher Maßnahmen durch das ISO 27001 Zertifikat gesichert sein.
SAP Sales OnDemand
Ja, laut der SAP-Presentation sind derartige Maßnahmen vorgesehen (SAP, NAVIGATOR (SAP-Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Confidentiality and Integrity“.
c. Wird das „least privilege“-Modell umgesetzt (nur unbedingt erforderliche Rechte zur Durchführung der definierten Tätigkeiten werden gewährt)?
Dropbox
Es wurden keine Angaben gefunden.
Fabasoft Folio Cloud
Es wurden keine Angaben gefunden, allerdings sollte das durch ISO 27001 A11.2.2 geregelt sein.
Google Apps
Ja. (Google, IT Security White Paper, 2013), Punkt „Authorization Controls“.
Microsoft Office 365
Ja. (Microsoft, Managing Access to the Exchange Online Service, 2013).
Salesforce
Ja. (Salesforce, Security White Paper, 2013).
SAP Sales OnDemand
Es wurden keine Angaben gefunden; allerdings sollte das durch ISO 27001 A11.2.2 geregelt sein.

5.5.2.8 Monitoring und Security Incident Management

a. Existiert eine 24/7-Überwachung der Cloud-Dienste, und sind zeitnahe Reaktionen bei Angriffen und Sicherheitsvorfällen gewährleistet?
Dropbox
Amazon bietet 24x7x365 Incident Response (Amazon Overview of Security Processes- WhitePaper, 2013).
Fabasoft Folio Cloud
Ja.
Google Apps
Ja. Google implementiert derartige Maßnahmen (Google, IT Security White Paper, 2013), Punkt „Incident management“.
Microsoft Office 365
Ja. Microsoft implementiert Maßnahmen zur zeitnahen Reaktion auf Angriffe und Vorfälle (Microsoft, Unablässige Sicherheit, 2013), Punkt „Integrierte Sicherheit“ und (Microsoft, Dienstkontinuität,

2013).
Salesforce
Ja, die Salesforce-Website nennt Incident Management (Salesforce, Sicherheitsüberblick, 2013), Punkt „Zugriffssteuerung und technische Sicherheit“.
SAP Sales OnDemand
Ja, die SAP Präsentation nennt derartige Überwachung und Reaktion auf Vorfälle (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Network Security“.
b. Ist sichergestellt, dass relevante Datenquellen erfasst und ausgewertet werden können (System-status, fehlgeschlagene Anmeldeversuche etc.)?
Dropbox
Administratoren können Aktivitäten wie Logins einsehen und Berichte erstellen (Dropbox, Dropbox Security Guide, 2013), Punkt „View activity and monitor security“.
Fabasoft Folio Cloud
Logging-Daten sind vorhanden. Inwieweit sie dem Kunden zur Verfügung gestellt werden können, ist nicht klar.
Google Apps
Ja, allerdings sind diese nur vom Google-Sicherheitsteam im Anlassfall einsehbar (Google, IT Security White Paper, 2013), Punkt „Access Control“.
Microsoft Office 365
Ja, Microsoft stellt ein Tool bereit, um dem Kunden Logs zugänglich zu machen (Microsoft, The Microsoft Online Services Diagnostics and Logging (MOSDAL) Support Toolkit, 2013).
Salesforce
Der Systemstatus der Salesforce-Plattform ist jederzeit einsehbar (Salesforce, Salesforce System Status, 2013), ebenso wie Berichte über Data Modifikationen (Salesforce, Security White Paper, 2013), Punkt „How You Can Audit Data Modifications“.
SAP Sales OnDemand
Ja, SAP verfügt über derartige Datenquellen, ob diese dem Kunden überlassen werden, ist nicht klar (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Confidentiality and Integrity“.
c. Können relevante Logdaten in geeigneter Form durch den Auftragnehmer zur Verfügung gestellt werden?
Dropbox
Ja. (Dropbox, Dropbox Security Guide, 2013), Punkt „View Activity and Monitor Security.
Fabasoft Folio Cloud
Ja, ein Audit-Log für Objekte kann erstellt werden (Fabasoft, Audit Log Configuration in the Object Class, 2013).
Google Apps
Log-Daten sind vorhanden (Google, IT Security White Paper, 2013), Punkt „Access Control“. Inwieweit sie zur Verfügung gestellt werden können, ist nicht klar.
Microsoft Office 365
Office 365 bietet Audit-Reports als Feature, sofern SharePoint Teil des Abonnements ist. (Microsoft, Configure audit settings, 2013).
Salesforce
Ja. (Salesforce, Administrative Reports, 2013).

SAP Sales OnDemand
Ja. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.3 bzw. 2.7.
d. Werden die Aktivitäten von Administratoren aufgezeichnet und überwacht?
Dropbox
Ja. (Dropbox, Official Blog of Dropbox for Business, 2013), Punkt „Increased Visibility“.
Fabasoft Folio Cloud
Solche Maßnahmen müssen laut ISO 27001 A.10.10.4 implementiert sein.
Google Apps
Ja, Administratoren werden überwacht (Google, IT Security White Paper, 2013), Punkt „Information Access“und „Access Control/Accounting“.
Microsoft Office 365
Handlungen können eindeutig auf Akteure zurückgeführt werden („[…] through a set of system controls, including the use of unique user names, data access controls, and auditing […]“) (Microsoft, Administrative Access, 2013); sollten auch Teil der Audit-Logs sein.
Salesforce
Ja, auch Administratoren werden überwacht (Salesforce, Monitoring Setup Changes, 2013).
SAP Sales OnDemand
Ja, solche Maßnahmen werden zur Verfügung gestellt (SAP, NAVIGATOR (SAP- Partner) - Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Confidentiality and Integrity“, Stichwort; Activity Logging.

5.5.2.9 Notfallmanagement

a. Welche Notfallmaßnahmen sind im Falle eines Dienstausfalles vorgesehen?
Dropbox
Seitens Dropbox wurden keine Angaben dazu gemacht. Amazon garantiert in der SLA (Amazon, Amazon SLA, 2013), dass der Dienst verfügbar ist; die entsprechenden Maßnahmen werden nicht erwähnt.
Fabasoft Folio Cloud
Es wurden keine Angaben zum Notfallmanagement gefunden.
Google Apps
Google hat ein Notfallmanagement-System in Anlehnung an NIST-SP800-61 implementiert (Google, IT Security White Paper, 2013), Punkt „Incident Management“.
Microsoft Office 365
(Microsoft, Microsoft Dynamics CRM Online Security and Service Continuity, 2013), Punkt „Responsibilities during a Service Outage“. Die Verantwortlichkeiten seitens Microsoft sind folglich definiert, allerdings nicht die Notfall-Maßnahmen.
Salesforce
Es wurden keine Angaben dazu gefunden.
SAP Sales OnDemand
Die SAP-Website (SAP, Protecting your data – and your business securely with SAP, 2013) verweist auf Krisenmanagement, allerdings werden keine Details genannt.

5.5.2.10 Portabilität und Interoperabilität

a. Werden Daten bei Vertragsbeendigung in einem vereinbarten Format unter Beibehaltung der logischen Relation zur Verfügung gestellt?
Dropbox
Auch nach Ablauf des Abonnements können Daten exportiert werden (möglicherweise ist dies mit entsprechenden Gebühren verbunden). (Dropbox, Vereinbarung für „Dropbox für Unternehmen“, 2013), Punkt 10.e.
Fabasoft Folio Cloud
Ja, Daten können exportiert werden. (Fabasoft, Cloud Assurance, 2013), Punkt „Data and Services Portability“.
Google Apps
Ja, die Daten sind exportierbar (Google, Online Agreement, 2013), Punkt 11.1ii. Auch das Format sollte wählbar sein (Data Liberation Front, 2013).
Microsoft Office 365
Ja, die Daten können exportiert werden (Microsoft, Es sind ihre Daten, 2013).
Salesforce
Ja. Daten können innerhalb von 30 Tagen nach Ablauf des Abonnements exportiert werden. (Salesforce, Master Subscription Agreement, 2013), Punkt 12.5. Das Format dürfte .csv sein (Salesforce, Data Export, 2013).
SAP Sales OnDemand
Ja, die Daten können exportiert werden. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 2.8.
b. Existieren standardisierte oder offen gelegte Schnittstellen zum Auftragnehmer?
Dropbox
Dropbox hat seine APIs für Entwickler bereitgestellt. (Dropbox, Dropbox Developer, 2013).
Fabasoft Folio Cloud
Ja, offene und standardisierte Schnittstellen werden bereitgestellt (Fabasoft, API, 2013).
Google Apps
Ja, die Google-APIs sind frei zugänglich (Google, Google Apps Platform, 2013).
Microsoft Office 365
Ja, die APIs von Microsoft Office sind zugänglich können eingesehen werden. (Microsoft, Office for developers, 2013).
Salesforce
Ja, Force.com APIs sind zugänglich (Salesforce, Developer Site, 2013).
SAP Sales OnDemand
Ja. SAP stellt Schnittstellen bereit (SAP, Business Application Programming Interfaces, 2013).

5.5.2.11 Sicherheitsprüfung und -nachweis

a. Wie wird die Einhaltung der Datenschutzbestimmungen nachgewiesen?
Dropbox
Dropbox ist Safe-Harbor- bzw. eTrust-zertifiziert. Amazon hat ISO 27001 und ebenfalls Safe-Harbor-Zertifikate (Amazon, AWS privacy note, 2013).
Fabasoft Folio Cloud
Fabasoft unterliegt europäischen Datenschutzgesetzen und verfügt über entsprechende Zertifikate: • Audits von externen Firmen: ISO 27001, ISO 20000, ISO 9001, ISAE 3402 Type 2, Audit-proof archiving – Archive 2010. • Directive 95/46/EC, Directive 2002/58/EC bzw. Federal Data Protection Law (BDSG) und Austrian Data Protection Commission (Fabasoft, Performance Characteristics of Data Security, 2013).
Google Apps
SAS70 Zertifikat und Safe-Harbor-Abkommen (Google, Google Apps Trust- Sicherheit, 2013).
Microsoft Office 365
ISO 27001, DPA, HIPAA, FISMA, FERPA (Microsoft, Unabhängig geprüft, 2013).
Salesforce
Zertifikate und Audits externer Überprüfer (Salesforce, Unterstützung der Datenschutzeinhaltung, 2013).
SAP Sales OnDemand
Laut der SAP Geschäftsbedingungen wird die Einhaltung von Datenschutzbestimmungen gewährleistet (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 4, Stichwort: Kontrollrechte.
b. Werden unabhängige Zertifizierungen oder Audits beim Auftragnehmer hinsichtlich Datenschutz und Datensicherheit durchgeführt (SAS70, Trust Services, ISO27001)? Welche Bereiche werden zertifiziert?
Dropbox
Nein. (Dropbox, Is Dropbox HIPAA, FERPA, SAS 70, Safe Harbor, ISO 9001, ISO 27001,or PCI compliant?, 2013).
Fabasoft Folio Cloud
Ja. Informationssicherheit, Datenschutz, Organisatorisches (Fabasoft, Sicherheit und Datenschutz , 2013)
Google Apps
Google ist SAS70 zertifiziert. (Google, Certification & data privacy, 2013), dies deckt folgende Bereiche ab: „[...] all messaging and collaboration services as well as Message security […]“.
Microsoft Office 365
Ja, Microsoft ist konform mit IS027001, FISMA, HIPAA, ADVs/DPAs, EU-Standardvertragsklauseln, Safe Harbor, FERPA, SSAE 16, PIPEDA und GLBA. (Microsoft, Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit , 2013), Punkt: „Die zehn wichtigsten Verträge, Zertifizierungen, Standards und Bestimmungen, die die Einhaltung von behördlichen Vorschriften sicherstellen“, Stichworte: Datenschutz und IT- Security.
Salesforce
Salesforce hält ein ISO 27001 Zertifikat und hat weiters das SAS 70 Type II Auditing erfolgreich absolviert.
SAP Sales OnDemand
Ja, SAP verfügt über diverse Zertifikate: ISAE No. 3402 Type B und (SSAE) No. 16 (SAP, NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update, 2013), Punkt „Standards and Certificates“.

c. Werden regelmäßige Penetrationstests durchgeführt?
Dropbox
Ja. (Dropbox, Dropbox Security Guide, 2013), Punkt „We've got you (and your Data) covered".
Fabasoft Folio Cloud
In der Dokumentation konnte dazu nichts Ausdrückliches gefunden werden.,
Google Apps
Ja, laut Googles Whitepaper werden solche Tests durchgeführt (Google, IT Security White Paper, 2013), Punkt „Vulnerability Management".
Microsoft Office 365
Ja, laut Audit, werden solche Tests durchgeführt (Microsoft, Security Audit, 2013).
Salesforce
Ja, Penetrationstests werden durchgeführt (Salesforce, Secure, private, and trustworthy: enterprise cloud computing with Force.com, 2013), Punkt „Cloud-Computing and information security governance".
SAP Sales OnDemand
In der (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013) und in anderen allgemein zugänglichen SAP-Informationsquellen ist nichts dazu zu finden.
d. Werden regelmäßige Penetrationstests bei Subauftragnehmern durchgeführt?
Dropbox
Ja, laut Amazons Whitepaper führt Amazon als Dropbox-Subauftragnehmer Penetrationstests durch (Amazon Overview of Security Processes- WhitePaper, 2013), Punkt „Secure Design Principle".
Fabasoft Folio Cloud
Laut Fabasoft (Fabasoft, Sicherheit und Datenschutz , 2013) betreibt Fabasoft weitgehend eigene Wertschöpfung, nutzt folglich keine Subauftragnehmer, die für Penetrationstests infrage kommen würden.
Google Apps
Keinerlei Angaben wurden dazu gefunden.
Microsoft Office 365
Keinerlei Angaben wurden dazu gefunden.
Salesforce
Keinerlei Angaben wurden dazu gefunden.
SAP Sales OnDemand
Keinerlei Angaben wurden dazu gefunden. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013).

5.5.2.12 Personalanforderungen

a. Wird Personal nur nach positiver Überprüfung deren Hintergrunds eingestellt?
Dropbox
Dropbox macht keine Angaben dazu. Bei Amazon ebenfalls nichts gefunden, allerdings sollte dieser Punkt durch ISO 27001 abgedeckt sein.

Fabasoft Folio Cloud
Ja, Fabasoft überprüft seine Mitarbeiter (Fabasoft, Cloud Assurance, 2013), Punkt „Personnel Security“.
Google Apps
Ja, Google überprüft seine Mitarbeiter (Google, IT Security White Paper, 2013), Punkt „Personnel Security“.
Microsoft Office 365
Keine direkten Angaben dazu gefunden, allerdings sollte ISO27001 A.8.1.2 das abdecken.
Salesforce
Ja, Salesforce überprüft seine Mitarbeiter (Salesforce, Secure, private, and trustworthy: enterprise cloud computing with Force.com, 2013), Punkt „Force.com cloud platform security“.
SAP Sales OnDemand
Ja, derartige Überprüfung muss nach ISO 27001 A.8.1.2 gegeben sein.
b. Wurden relevante Mitarbeiter des Auftragnehmers zur Einhaltung des Datengeheimnisses nach § 15 DSG verpflichtet?
Dropbox
Ja, laut (Dropbox, Wie sicher ist Dropbox?, 2013): „Dropbox-Mitarbeitern ist es untersagt, den Inhalt der Dateien, die Sie in Ihrem Konto speichern, einzusehen.“ (abgesehen von Support u.ä.). Die Policy ist nicht einsehbar.
Fabasoft Folio Cloud
Ja. (Fabasoft, Cloud Assurance, 2013), Punkt „Personnel Security“.
Google Apps
Ja. (Google, IT Security White Paper, 2013), Punkt „Personnel Security“.
Microsoft Office 365
ISO27001 A.8.1.3 sollte Sensibilisierung hinsichtlich Informationssicherheit fördern. Inwieweit damit zu Stillschweigen verpflichtet wird, ist nicht bekannt.
Salesforce
Salesforce verpflichtet seine Mitarbeiter, vertrauliche Informationen (Kundendaten wie Mitarbeiterdaten) zu schützen. (Salesforce, Unterstützung der Datenschutzeinhaltung, 2013), Punkt „Vorgehensweise“ bzw. (Salesforce, Security White Paper, 2013), Punkt „How We Operate Internally“.
SAP Sales OnDemand
Ja. (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 5.
c. Wird relevantes Personal regelmäßig geschult?
Dropbox
Dropbox macht dazu keine Angaben.
Fabasoft Folio Cloud
Ja, Fabasoft-Personal wird geschult (Fabasoft, Cloud Assurance, 2013), Punkt „Personnel Security“.
Google Apps
Ja, Google-Mitarbeiter werden regelmäßig geschult (Google, IT Security White Paper, 2013), Punkt „Personnel Security“.
Microsoft Office 365
Microsoft macht keine Angaben dazu, allerdings muss dies laut ISO27001 A.8.2.2 für die Zertifizierung gegeben sein.
Salesforce

Ja, Salesforce schult seine Mitarbeiter (Salesforce, Security White Paper, 2013), Punkt „How We Operate Internally“.
SAP Sales OnDemand
Ja, SAP schult seine Mitarbeiter regelmäßig. Dieser Punkt ist vertraglich zugesichert (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 5.
d. Wird das Personal hinsichtlich Informationssicherheit und Datenschutz sensibilisiert?
Dropbox
Es wurden dazu keine Angaben gefunden.
Fabasoft Folio Cloud
Ja, eine derartige Sensibilisierung erfolgt (Fabasoft, Cloud Assurance, 2013), Punkt „Personnel Security“.
Google Apps
Ja, eine derartige Sensibilisierung erfolgt laut dem Whitepaper (Google, IT Security White Paper, 2013), Punkte „Personnel Security“ und auf Basis der Mitarbeiter-Verhaltensrichtlinien (Google, Code of Conduct, 2013), Punkt 3.
Microsoft Office 365
Es wurden keine Angaben dazu gefunden, allerdings muss eine derartige Sensibilisierung laut ISO27001 A.8.2.2 erfolgen.
Salesforce
Ja, eine derartige Sensibilisierung erfolgt laut dem Salesforce Whitepaper (Salesforce, Security White Paper, 2013), Punkt „How We Operate Internally“.
SAP Sales OnDemand
Ja, eine derartige Sensibilisierung erfolgt laut den SAP-AGBs (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 5.
e. Verpflichten sich die Mitarbeiter der Informationssicherheit, dem Datenschutz und dem angemessenen Umgang mit Kundendaten?
Dropbox
Es wurden keine Angaben dazu gefunden.
Fabasoft Folio Cloud
Ja, laut der Fabasoft-Website wird dies zugesichert (Fabasoft, Cloud Assurance, 2013), Punkt „Personnel Security“.
Google Apps
Ja, laut den Verhaltensrichtlinien von Google verpflichten sich Mitarbeiter dazu (Google, Code of Conduct, 2013), Punkt 3.
Microsoft Office 365
Es wurden keine Angaben von Microsoft gefunden.
Salesforce
Ja, Salesforce Whitepaper spricht derartige Punkte an (Salesforce, Security White Paper, 2013), Punkt „How We Operate Internally“.
SAP Sales OnDemand
Ja, laut den SAP-AGBs werden dem Kunden diese Punkte zugesichert (SAP, Allgemeine Geschäftsbedingungen für SAP Cloud Services der SAP Österreich GmbH, 2013), Anlage 2, Punkt 5.

Fazit

Die Analyse hat gezeigt, dass die betrachteten Cloud-Service-Anbieter hinsichtlich der Datensicherheits- und Datenschutzmaßnahmen um Transparenz bemüht sind, zumal diese auch wichtige Marketingmaßnahmen darstellen. Die analysierten österreichischen und deutschen Anbieter versuchen, durch verstärkte Transparenz und europäische Standorte beim datenschutzaffinen Kunden zusätzlich zu punkten.

Die Analyse hat auch gezeigt, dass die Bearbeitung der einzelnen Analysefragen und die damit verbundenen Recherchen in White Papers, AGB, Websites, Standardverträgen, Marketingunterlagen etc. sehr zeitaufwändig und für den Konsumenten nicht zumutbar sind. Unabhängige Gütesiegel oder Zertifikate anerkannter und seriöser Organisationen (z.B. staatlicher Natur oder ähnlich dem TÜV) könnten hier im Sinne des Konsumenten Transparenz und Übersichtlichkeit schaffen. Durch regelmäßige Re-Zertifizierungen wird sichergestellt, dass ein Fragenkatalog wie der obige in festgesetzten zeitlichen Abständen überarbeitet und der Erfüllungsgrad an die aktuellen Gegebenheiten angepasst wird. Das auszustellende Zertifikat sollte daher an eine Gültigkeitsdauer geknüpft sein (z.B. 12 Monate).

6 RISIKOANALYSE CLOUD-NUTZUNG

In diesem Kapitel werden in einem ersten Schritt mögliche Datenmissbrauchsszenarien im Zusammenhang mit der Nutzung von Cloud-Diensten definiert und abgegrenzt. Mögliche rechtliche, technische, soziale und finanzielle Folgen werden darauf aufbauend abgeschätzt und Strategien zur Risikominimierung definiert.

Obwohl Cloud-Computing durch Professionalisierung und Dezentralisierung des IT-Infrastrukturbetriebs höhere Betriebssicherheit verspricht, gab es in jüngster Vergangenheit einige Vorfälle, welche eine Vielzahl von Cloud-Computing-Kunden betrafen:

- Im August 2011 und im Juni 2012 störten heftige Gewitter das Amazon EC2 Rechenzentrum nahe Dublin. Der Ausfall beeinträchtigte die darauf gehosteten Websites wie zum Beispiel Instagram oder Netflix und deren Millionen User[73] [70].
- Am 28. Februar 2012 ging Microsoft Azure in mehreren Teilen der Welt aufgrund eines Schaltjahrproblems offline[74] [71]. Die Wiederherstellung der Services nahm 24 Stunden in Anspruch. Betroffen war unter anderen auch der britische G-Gov CloudStore.
- Im März 2009 verloren 7.500 Carbonite Kunden ihre Backups. Nach 24 Stunden war es allen außer 54 Kunden möglich, ihre Backups wiederherzustellen[75] [72].
- Im Oktober 2009 verloren 1 Million Kunden von T-Mobile-Sidekick ihre Kontakte, Kalendereinträge, To-do-Listen und Fotos wegen eines Servicefehlers bei einem von Microsofts Subauftragnehmern[76] [73].
- Im Juli 2010 verloren 6.323 Evernote-Kunden aufgrund eines Hardwarefehlers ihren Evernote Datenbestand[77] [74].
- Im Februar 2011 verloren 35.000 Kunden von Google-Mail und -Apps all ihre dort gespeicherten Daten. Google benötigte vier Tage, um die Daten von alten Bandkopien wiederherzustellen[78] [75].

[73] Lighting in Dublin knocks Amazon and Microsoft data centers offline, abrufbar unter: http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/ (letzter Zugriff: 24.03.2014)

[74] Windows Azure Service disruption Update, abrufbar unter: https://blogs.msdn.com/b/windowsazure/archive/2012/03/01/windows-azure-service-disruption-update.aspx (letzter Zugriff: 24.03.2014)

[75] Online backup company Carbonite loses customers data and sues suppliers, abrufbar unter: http://techcrunch.com/2009/03/23/online-backup-company-carbonite-loses-customers-data-blames-and-sues-suppliers/ (letzter Zugriff: 24.03.2014)

[76] T-Mobile Sidekick disaster, abrufbar unter: http://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/ (letzter Zugriff: 24.03.2014)

[77] Evernote's July 1st server problem, abrufbar unter: http://blog.evernote.com/2010/08/09/july1/ (letzter Zugriff: 24.03.2014)

[78] Google Gmail Outage, abrufbar unter: http://www.huffingtonpost.com/2011/03/03/google-gmail-outage_n_830229.html (letzter Zugriff: 24.03.2014)

6.1 Definition und Abgrenzung von Datenmissbrauchsszenarien (Angriffsvektoren)

6.1.1 Verletzung der Datenvertraulichkeit

Dieses Szenario ist eines der meistgefürchteten in Zusammenhang mit der Nutzung von Cloud-Computing[79] [76]: Die beim Cloud-Anbieter gespeicherten internen/sensibler Daten sind Dritten ohne Zustimmung des Dateninhabers zugänglich. Zwar existiert diese Bedrohung auch innerhalb der unternehmenseigenen IT-Infrastruktur, doch durch die gemeinsame Nutzung von IT-Infrastruktur bei Public-Cloud-Angeboten steigt die Wahrscheinlichkeit der ungewollten Offenlegung von Daten (vgl. PRISM-Programm der NSA).

6.1.2 Verletzung der Integrität

Ein System gewährleistet Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Die Integrität von Daten, Nachrichten und Informationen bezeichnet deren Unverfälschtheit bzw. Vertrauenswürdigkeit[80]. In Cloud-Umgebungen sind neben Datenintegrität auch Softwareintegrität (Software verhält sich gemäß Spezifikation und weist keine Hintertüren oder ähnliche Mechanismen auf), Konfigurationsintegrität (Konfiguration kann nur durch autorisierte Personen geändert werden) und Nachrichtenintegrität (inklusive Verwaltungs- und Steuerungsinformation) von Bedeutung.

6.1.3 Beeinträchtigung der Verfügbarkeit

Wie bei jedem IT-Service ist auch bei Cloud-Angeboten die ununterbrochene Verfügbarkeit von Daten und Diensten ein wesentliches Qualitäts- und Sicherheitskriterium. Im Gegensatz zu selbst betriebenen IT-Infrastrukturen bilden bei Cloud-Computing SLAs und das generelle Vertrauen in den Anbieter die Grundlage zuverlässiger Dienste. Die gemeinsame Nutzung von IT-Infrastruktur durch mehrere Kunden kann die Wahrscheinlichkeit einer Verfügbarkeitsunterbrechung erhöhen (beispielsweise durch Probleme/Angriffe welche im Bereich anderer Kunden verursacht werden, sich aber durch die geteilte Verwendung auch auf die eigenen Cloud-Dienste auswirken).

6.1.4 Datenverlust

Wie auch in traditionellen IT-Infrastrukturen besteht bei Cloud-Computing das Risiko des Datenverlusts durch bewusste/unbewusste Löschung, Angriffe, physische Einwirkungen (Naturkatastrophen) oder technische Defekte. Redundante Datenspeicherung und Backups können diesem Risiko sowohl auf Anbieter- als auch auf Kundenseite entgegenwirken.

---

[79] CSA – The Notorious Nine: Cloud Computing Top Threats in 2013

[80] BKA Positionspapier, Kapitel 7 [12]

6.1.5 Übernahme des Accounts oder des Datenverkehrs

Angriffsmethoden wie Phishing, Spear Phishing, Betrug oder die Ausnützung von Softwareschwachstellen können dazu führen, dass Dritte den Cloud-Computing-Account oder den Datenverkehr zwischen Anbieter und Kunden übernehmen können. So erlaubte zum Beispiel eine Lücke im Cross-Site-Scripting (XSS) Angreifern im April 2010, Zugangsdaten von Amazon-Kunden zu stehlen[81] [77]. 2009 wurden darüber hinaus einige Amazon-Systeme als Zeus-Botnet-Knoten missbraucht[82] [78]. Sollte ein Angreifer in Besitz der Cloud-Service-Zugangsdaten kommen, so hat dies weitreichende Konsequenzen für den Kunden:

- Die gesamte Kommunikation (Aktivitäten, Transaktionen etc.) zwischen Anbieter und Kunden kann abgehört werden.
- Daten, welche bei Cloud-Anbieter gespeichert sind, können vom Angreifer ohne das Wissen des Kunden manipuliert werden.
- Datenanfragen können falsch beantwortet werden. So könnten beispielsweise wichtige Kalendereinträge aus dem SaaS-Service gelöscht werden, um die Geschäftstätigkeit empfindlich zu stören.
- Kunden könnten auf Websites mit bösartigem Inhalt weitergeleitet werden (beispielsweise falsche Webshops, um Zahlungsströme umzuleiten).
- Angreifer können die Reputation des Kunden verwenden, um ausgehend von dessen Systemen Angriffe zu starten.

6.1.6 Unsichere Schnittstellen und APIs

Eine Vielzahl von Cloud-Diensten bieten Schnittstellen und APIs, um deren Integration in weitere Dienste und Anwendungen zu ermöglichen. Sowohl Verwaltung, Monitoring, Zusammenstellung mit anderen Cloud-Angeboten als auch die eigentliche Dienstausführung können über programmatische Schnittstellen durchgeführt werden. Somit ist auch die gesamte Sicherheit des Cloud-Services von der Sicherheit und der fehlerfreien Implementierung der Schnittstellen abhängig und sollte aus diesem Grund nicht vernachlässigt werden.

6.1.7 Denial of Service

„Denial of Service“-Attacken (d.h. Angriffe, welche bewusst Überlastungen im Zielsystem erzeugen, um dieses für legitimierte Nutzer unbrauchbar zu machen) in Zusammenhang mit Cloud-Diensten haben im Gegensatz zu gleichartigen Angriffen auf unternehmenseigene Infrastruktur zwei Besonderheiten:

- Einerseits ermöglicht die gemeinsame Verwendung von IT-Ressourcen mehrerer Kunden die Überlastung des Cloud-Services durch einen einzelnen, legitimierten Kunden und dessen

[81] Amazon website treat, abrufbar unter: http://www.theregister.co.uk/2010/04/20/amazon_website_treat/ (letzter Zugriff: 24.03.2014)

[82] Amazon EC2 bot control channel, abrufbar unter: http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/ (letzter Zugriff: 24.03.2014)

übermäßige Inanspruchnahme von Ressourcen (Rechenleistung, Speicher etc.). Dies kann durch den Kunden selbst oder durch Angreifer mithilfe gestohlener Zugangsdaten erfolgen.

- Andererseits können wirtschaftliche DoS-Attacken auf Basis des häufig angewandten „pay-per-use"-Modells erfolgen. Dabei führt der Angreifer mithilfe gestohlener Zugangsdaten vermehrt kostenpflichtige Operationen (generelle Nutzung des Dienstes, Rechenoperationen etc.) auf Kosten des angegriffenen Unternehmens durch. Der Dienst funktioniert in diesem Szenario von technischer Seite nach wie vor einwandfrei, doch wird der Kunde durch immer stärker steigende Kosten zum Abschalten des Dienstes gezwungen.

6.1.8 Malicious Insider

Risiken, welche von legimitierten Nutzern (Administratoren, Geschäftspartner, Mitarbeitern, Vertragspartnern etc.) ausgehen, sind sowohl in traditionellen als auch Cloud-basierten Umgebungen zu bewerten und zu adressieren[83] [79]. Während in traditionellen Umgebungen potenzielle Malicious Insider bekannt sind, so ist dies bei Cloud-Computing nicht der Fall. Daten und Anwendungen werden über weit verteilte geographische Bereiche verstreut und das administrierende Personal ist in der Regel nicht bekannt. Gegenmaßnahmen wie Verschlüsselung sollten aus diesem Grund implementiert und die dazugehörigen Schlüssel dem Cloud-Service-Anbieter nicht bekannt gegeben werden.

6.1.9 Missbrauch von Cloud-Services

Die kostengünstige Verfügbarkeit von hohen Bandbreiten und Rechenkapazität ermöglicht es Angreifern, Cloud-Infrastrukturen für kriminelle Zwecke zu missbrauchen (DoS-Attacken, Entschlüsselungsoperationen etc.). In diesem Szenario sind vor allem die Cloud-Service-Anbieter gefordert, um solch missbräuchliche Verwendungen zu erkennen und zu unterbinden. Die Auswirkungen des Missbrauchs sind dreifach: (i) Rufschädigung des Anbieters, (ii) Schaden des eigentlichen Angriffsopfers und (iii) Schaden jener Kunden, welche die Cloud-Infrastruktur mit dem Angreifer teilen (beispielsweise durch verminderte Leistung oder Blacklisting der IP-Adressen durch andere Anbieter).

6.1.10 Unzureichende Due Diligence

Cloud-Computing wird von den Marketingabteilungen der Anbieter als kostengünstige und effiziente Methode zum Betrieb von IT-Services angeboten. Geleitet von beworbenen Kosteneinsparungen lagern Organisationen IT-Infrastrukturen aus, ohne die Auswirkungen und damit verbundenen Verantwortungen (Incident Response, Verschlüsselung, Security Monitoring etc.) im Vorfeld zu prüfen. Speziell die Auslagerung von IT-Funktionen, welche von internen Sicherheitseinrichtungen abhängig sind, können schwerwiegende Probleme nach sich ziehen. Eine tiefergehende Risikoanalyse für jedes auszulagernde Service ist deshalb vor der Auslagerung unbedingt erforderlich.

[83] Insider threats to cloud computing, abrufbar unter: http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/ (letzter Zugriff: 24.03.2014)

6.1.11 Gemeinsame Nutzung der Cloud-Infrastruktur

Die gemeinsame Nutzung von IT-Infrastruktur durch mehrere Cloud-Kunden birgt zahlreiche Risiken: Schwachstellen in Hypervisoren, geteilte Software-Bibliotheken oder Plattformkomponenten betreffen nicht nur einen, sondern alle Kunden, welche sich die verwundbare Ressource teilen.

6.1.12 Hardware Security

Um die einfache Kommunikation zwischen verschiedensten Systemen zu gewährleisten, wurde das OSI-Schichtenmodell (Zimmermann, 1980) [80] entwickelt. Die Grundidee basiert darauf, klar definierte und abgegrenzte Aufgaben auf einzelne Schichten aufzuteilen und zwischen den aufeinanderfolgenden Schichten nur Schnittstellen verfügbar zu machen. Auf diese Weise sind verschiedenste Schichtimplementierungen möglich, die ausgetauscht werden können. Das Modell zählt sieben Schichten:

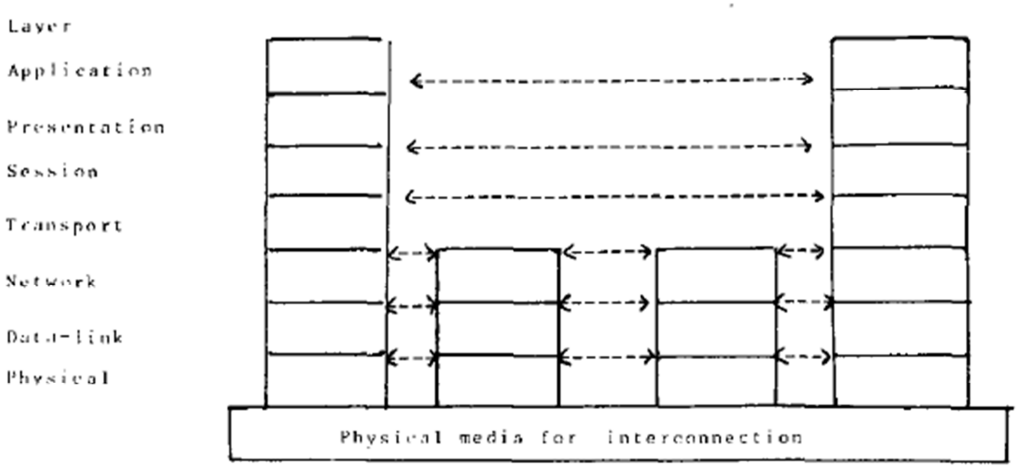

Abbildung 6: OSI-Schichtenmodell (Zimmermann, 1980) [80]

Bitübertragungsschicht (Physical Layer): Hier werden mechanische, elektrische oder anderweitig funktionale Hilfsmittel bereitgestellt, um physische Verbindungen zu öffnen, zu schließen und Bits zu übertragen.

Sicherungsschicht (Data-Link Layer): Aufgabe dieser Schicht ist, eine weitgehend fehlerfreie Übertragung zu gewährleisten, beispielsweise durch Prüfsummen für Bit-Blöcke.

Vermittlungsschicht (Transport Layer): Sorgt für das Schalten von Verbindungen beziehungsweise das Weiterleiten von Paketen (auch *Routing* genannt).

Transportschicht (Network Layer): Behandelt neben der Segmentierung des Datenstroms auch die Kontrolle zwischen den Endpunkten von Kommunikationskanälen.

Sitzungsschicht (Session Layer): Ist für die Prozesskommunikation zwischen verschiedenen Systemen zuständig.

Darstellungsschicht (Presentation Layer): Stellt Hilfsmittel bereit um, übertragene Daten zu interpretieren, beispielsweise um Formate anzugleichen (auch die Verschlüsselung ist hier angesiedelt).

Anwendungsschicht (Application Layer): Diese oberste Schicht stellt die Verbindung zu den darunter liegenden Schichten her und somit deren Funktionen zur Verfügung.

Bei einer Übertragung werden Daten von Schicht zu Schicht gereicht und um weitere Daten (Header bzw. Trailer) ergänzt. Während des Routings müssen an den Knoten nur die unteren drei Schichten durchlaufen werden, um den tatsächlichen Empfänger zu bestimmen. Im Zielsystem können die Daten wieder zusammengesetzt und gegebenenfalls dem lokalen System angepasst werden.

Da aktuell sämtliche Kommunikation in Netzwerken auf dem oben beschriebenen OSI-Modell aufsetzt und Protokolle innerhalb einer Schicht beliebig austauschbar sind, bestimmt die Sicherheitsstufe einer Implementierung auch jene der darunterliegenden Schichten.

Vor allem tiefer liegende Schichten werden aufgrund höherer Performanceanforderungen durch Hardware-Implementierungen abgedeckt und entsprechen nicht immer den erforderlichen Standards bzgl. Informationssicherheit. Man beachte beispielsweise das Abhören des Datenverkehrs von unverschlüsselten WLAN-Netzen. Hier lässt etwa eine verabsäumte Konfiguration der Übertragungsschicht zu, dass – sofern nicht in höheren Schichten eine Verschlüsselung stattgefunden hat (HTTPS, TLS etc.) – ohne weiteres Daten ausgelesen werden können.

6.2 Folgenabschätzung

Basierend auf der Risikoanalyse in Kapitel 5.5.2 gibt dieser Abschnitt eine Übersicht über die rechtliche, technische, soziale und finanzielle Folgen für KMUs und kleine Behörden.

6.2.1 Szenario „Verletzung der Datenvertraulichkeit“

Rechtliche Folgen

Für den Fall, dass bei einer Verletzung der Datenvertraulichkeit sensible Daten offengelegt werden, besteht je nach Art und rechtlicher Grundlage die Daten betreffend die Möglichkeit, gegen bestehende Datenschutzbestimmungen zu verstoßen, wodurch in weiterer Folge mit rechtlichen Schritten gerechnet werden muss. Rechtliche Schritte können von Betroffenen, aber auch Behörden eingeleitet werden. Neben Verfahrenskosten sowie Geld- und Haftstrafen ist Berufsverbot eine mögliche Folge.

Technische Folgen

Erneute Absicherung der offengelegte Datensätze beispielsweise durch Migration auf neue Systeme, Verschlüsselung, Ausgabe neuer Passwörter etc. War eine technische Schwachstelle für die Verletzung der Datenvertraulichkeit verantwortlich, so ist diese umgehend durch geeignete Maßnahmen zu schließen.

Soziale Folgen

Solche Vorfälle ziehen je nach Umfang der Verletzung zum Teil gravierende Rufschädigungen für die Betroffenen nach sich. Weiters kann auch die Wettbewerbsfähigkeit eingeschränkt werden. Ist die

Verletzung der Datenvertraulichkeit auf das Fehlverhalten eines Mitarbeiters zurückzuführen, so sind sofort geeignete Maßnahmen zu treffen, um ähnliche Schadensfälle in Zukunft zu vermeiden.

Finanzielle Folgen

Durch Verlust der Datenvertraulichkeit bzw. durch Verletzung des Datenschutzes können Zahlungen an Betroffene oder Behörden nötig werden. Rufschädigung kann sich direkt oder indirekt auf den Geschäftserfolg des Unternehmens auswirken.

6.2.2 Szenario „Verletzung der Integrität“

Rechtliche Folgen

Falls die Integrität von Geschäftsdokumenten nach §§ 132 Absatz 2 Bundesabgabeordnung – BAO nicht gegeben ist, hat dies rechtliche Konsequenzen mit Strafbestand der Steuerhinterziehung bzw. Urkundenunterdrückung zur Folge.

Technische Folgen

Ist die Datenintegrität alleinig durch den Cloud-Dienst nicht gegeben, müssen geschäftsrelevante Unterlagen noch in weiterer Form gespeichert werden, um bei Prüfungen vorgelegt werden zu können.

Soziale Folgen

Kann die Integrität und Unversehrtheit von Daten nicht garantiert werden, besteht für das betroffene Unternehmen durchaus das Risiko von Rufschädigung im Falle der Veröffentlichung dieser Schwachstellen. Dies kann sich in weiterer Folge auch als schadhaft für die Wettbewerbsfähigkeit herausstellen.

Finanzielle Folgen

Durch fehlende Integrität von Daten, beispielsweise Rechnungsdokumente oder Datensätze, die für die Buchhaltung relevant sind, kann es zu fehlerhaften Abrechnungen kommen.

6.2.3 Szenario „Beeinträchtigung der Verfügbarkeit“

Rechtliche Folgen

Durch eine Beeinträchtigung der Verfügbarkeit von angebotenen Diensten kann der Umstand auftreten, dass vertraglich geregelte Vereinbarungen mit Kunden nicht eingehalten werden können.

Technische Folgen

Durch den Ausfall von Diensten und dem erneuten Starten dieser Dienste kann es zwischenzeitlich zu Inkonsistenzen von Daten kommen, beispielsweise wenn Transaktionen vor dem Ausfall nicht abgeschlossen werden konnten und durch den Vorfall in einen „illegal state“ geraten.

Soziale Folgen

Betrifft der Ausfall wichtige Dienste, ist damit Verunsicherung bei Kunden und Rufschädigung des Dienstes zu erwarten. Ein nicht erreichbarer Dienst wird vermutlich als nicht vertrauenswürdig und unzuverlässig eingestuft werden.

Finanzielle Folgen

Stehen geschäftskritische Unterlagen nicht zur Verfügung, beziehungsweise sind Unterlagen und Dienste für die Erfüllung von Tätigkeiten nicht verfügbar, können durch den Ausfall hohe Schadenssummen entstehen. Beispielsweise wurde der Blackberry-Hersteller RIM nach mehrtägigen Ausfall seines Dienstes auf mehrere Millionen Dollar verklagt.[84] [81] Ähnliches widerfuhr Microsoft nach Ausfall des Xbox-Life-Dienstes[85] [82].

6.2.4 Szenario „Datenverlust“

Rechtliche Folgen

Datenverlust im Fall von Geschäftsunterlagen kann zu einem Verstoß gegen die Aufbewahrungsplicht führen (§§ 131, 132 Bundesabgabeordnung – BAO), wobei je nach Rechtslage Steuerhinterziehung sowie Urkundenunterdrückung als Straftatbestand in Betracht gezogen werden können. Darüber hinaus können im Falle von Datenverlust vertraglich geregelte Ansprüche von Kunden geltend gemacht werden.

Technische Folgen

Wiederherstellung verlorener Daten kann sich als schwierig erweisen. Beispielsweise kann das Einspielen von Backups in das laufende System Probleme verursachen oder gar das System zwischenzeitlich unbrauchbar machen.

Soziale Folgen

Verliert ein Dienst Daten, erweckt dies keinesfalls den Eindruck von Verlässlichkeit und Vertraulichkeit. Neben der Verunsicherung des Kunden tragen solche Vorfälle auch erheblich zum Imageverlust des Unternehmens bzw. der Behörde bei.[86] [83]

Finanzielle Folgen

Wurde eine vertraglich geregelte Gewährleistung von Datenverfügbarkeit verletzt, besteht die Möglichkeit auf Schadenersatzforderungen seitens der Betroffenen. Wird durch den Datenverlust Arbeitsausfall beziehungsweise Geschäftsentgang verursacht[87] [84], besteht ebenfalls Anspruch auf Ersatzzahlungen, auch wenn dies möglicherweise mit juristischem Aufwand verbunden ist.

---

[84] First an outage, abrufbar unter: http://betanews.com/2011/10/27/first-an-outage-now-a-lawsuit-us-canadian-blackberry-users-want-compensation/ (letzter Zugriff: 24.03.2014)

[85] Class action lawsuit targets Microsoft, abrufbar unter: http://arstechnica.com/gaming/2008/01/class-action-lawsuit-targets-microsoft-for-xbox-live-outages/ (letzter Zugriff: 24.03.2014)

[86] Blackberry services return, abrufbar unter: http://betanews.com/2011/10/13/blackberry-services-return-after-historical-global-outage/ (letzter Zugriff: 24.03.2014)

[87] Urteil 16.000 Euro Schadenersatz, abrufbar unter: http://www.zdnet.de/41558761/urteil-16-000-euro-schadenersatz-fuer-datenverlust-durch-stromausfall/ (letzter Zugriff: 24.03.2014)

6.2.5 Szenario „Übernahme des Accounts oder des Datenverkehrs“

Rechtliche Folgen

Durch die Übernahme des Accounts beziehungsweise des Datenverkehrs können die Grundwerte der Informationssicherheit nicht mehr gewährleistet werden: Vertraulichkeit, Verfügbarkeit und Integrität.[88] [85] Werden durch die Übernahme des Benutzerkontos Geschäfte unter fremdem Namen getätigt, sind diese im Nachhinein anzweifelbar (entsprechende Rechtsgrundlagen und Beweislage vorausgesetzt); dies bedarf allerdings mitunter eines erheblichen rechtlichen Aufwands.[89] [86]

Technische Folgen

Wird die Übernahme eines Benutzerkontos oder von Datenverkehr entdeckt, muss sichergestellt werden, dass dies in Zukunft unterbunden wird. Dies wird einerseits durch das Schließen der Sicherheitslücken, die die erfolgreiche Übernahme überhaupt verursacht hat, und weiters mit der Änderung aller Zugangsdaten erledigt.

Soziale Folgen

Die Übernahme eines Accounts zieht kritische Konsequenzen nach sich, beispielsweise können durch die Übernahme einerseits geschäftskritische Unterlagen und Daten offengelegt werden (Einschränkung der Wettbewerbsfähigkeit), andererseits ist Rufschädigung eine wahrscheinliche Folge eines solchen Angriffs.

Finanzielle Folgen

Werden Geschäfte unter falschem Namen getätigt, kann der Geschädigte die Echtheit der Verträge anzweifeln – sofern die Beweislage solche Schritte zulässt – was allerdings mit erheblichem rechtlichem Aufwand und hohen Kosten verbunden sein kann. Können Vertragsabschlüsse nicht angefochten werden, so sind diese auch einzuhalten.

Werden durch die Übernahme von Accounts oder des Datenverkehrs sensible Daten entwendet und an Dritte weitergegeben, beispielsweise im Fall von Industriespionage, so kann dem Betroffenen hoher Schaden entstehen. Ein Beispiel aus der jüngeren Vergangenheit ist etwa der Diebstahl von Daten eines geheimen US-Militärprojektes.[90] [87]

6.2.6 Szenario „Unsichere Schnittstellen“

Rechtliche Folgen

---

[88] Grundwerte Informationssicherheit, abrufbar unter:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (letzter Zugriff: 24.03.2014)

[89] LA Bonn Urteil, abrufbar unter: http://openjur.de/u/454361.html (letzter Zugriff: 24.03.2014)

[90] F35 JSF aircraft program, abrufbar unter: http://spectrum.ieee.org/riskfactor/computing/it/f_35_jsf_aircraft_program_pene (letzter Zugriff: 24.03.2014)

Unsichere Schnittstellen zu Cloud-Diensten können die unbeabsichtigte Offenlegung von Daten nach sich ziehen, wodurch weiters die Datenintegrität nicht mehr gewährleistet werden kann. In Verbindung damit können einerseits vertraglich zugesicherte Sicherheitsleistungen nicht länger gewährleistet werden, was rechtliche Schritte zur Folge haben kann, andererseits können durch die Schnittstellen sensible Daten offengelegt werden oder geschäftswichtige Daten verloren gehen, wodurch wiederum Ansprüche Dritter geltend gemacht werden können.

Technische Folgen

Werden unsichere Schnittstellen identifiziert, so muss sichergestellt werden, dass diese entweder durch Neukonfiguration oder Patching an Sicherheitsstandards angepasst oder durch sichere Alternativen ersetzt werden.

Soziale Folgen

Das Bekanntwerden von unsicheren Schnittstellen geht mit einer Schädigung des Rufes von Anbietern einher. Das Vertrauen der Kunden in den Dienst wird durch die Verwendung solcher Technologien nachhaltig geschwächt.

Finanzielle Folgen

Die konkreten finanziellen Folgen sind davon abhängig, wie schwerwiegend einerseits die Schwachstelle in der Schnittstelle und andererseits die Geschäftsrelevanz der Schnittstelle sind. Legt die Schnittstelle mehr Funktionalität als eigentlich beabsichtigt offen, ist die Integrität und Vertraulichkeit des Dienstes nicht länger gegeben. In weiterer Folge können Forderungen Dritter entstehen, deren Daten offengelegt wurden; oder sensible Interna geraten in falsche Hände, was wiederum Einbußen durch geminderte Wettbewerbsfähigkeit nach sich zieht.

Beispielsweise erlaubte eine Version des Dropbox-Clients theoretisch Zugriff auf gespeicherte Daten über eine unverschlüsselte lokale Datenbank[91] [88], was nach bisheriger Erkenntnis allerdings nicht geahndet wurde. Anders hingegen erlaubte ein Update beim Login zum Webservice jedwedes Passwort zu akzeptieren, woraufhin sich Dropbox mit einer Klage aufgrund von Fahrlässigkeit und Eingriff in die Privatsphäre konfrontiert sah.[92] [93] [94] [89], [90], [91]

6.2.7 Szenario „Denial of Service“

Rechtliche Folgen

Falls vertraglich geregelt, kann der Service-Anbieter sich das Recht vorbehalten (i) die Anzahl der Aufrufe von einem Account aus zu limitieren, um DoS zu verhindern und (ii) den Account vorläufig zu sperren, falls er auffällig viele Anfragen sendet.

---

[91] Dropbox authentication, abrufbar unter: http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/ (letzter Zugriff: 24.03.2014)

[92] Cloud site Dropbox drops the ball, abrufbar unter: http://www.consumeraffairs.com/news04/2011/06/cloud-site-dropbox-drops-the-ball.html (letzter Zugriff: 24.03.2014)

[93] Dropbox facing class action lawsuit, abrufbar unter: http://www.geek.com/news/dropbox-facing-class-action-lawsuit-over-any-password-worked-glitch-1396291/ (letzter Zugriff: 24.03.2014)

[94] Cloud storage Dropbox lawsuit, abrufbar unter: http://www.tomsguide.com/us/Cloud-storage-dropbox-lawsuit-Arash-Ferdowski-Cristina-Wong,news-11673.html (letzter Zugriff: 24.03.2014)

Durch einen herbeigeführten Ausfall kann beispielsweise vertraglich geregelten Verpflichtungen nicht nachgekommen werden, womit in weiterer Folge Schadensersatzzahlungen verbunden sein können.

Technische Folgen

Ist der Kunde selbst für die hohe Anzahl der Service-Aufrufe verantwortlich, bietet sich möglicherweise eine Neuvereinbarung des Vertrags mit dem Anbieter bzw. die Übersiedelung zu anderen Anbietern an.

Wenn der DoS-Angriff nicht vom legitimierten Kunden, aber mit dessen Account ausgelöst wurde, legt dieser Umstand nahe, dass der Account kompromittiert wurde, was entweder eine Infektion der lokalen IT-Infrastruktur mit bösartigen Code als Quelle haben kann oder eine anderweitige Offenlegung von Account-Details.

Soziale Folgen

Wird der DoS-Angriff über ein infiziertes Benutzerkonto ausgeführt, kann dies zur Folge haben, dass der Dienstbetreiber eben diesen sperrt, um weitere Angriffe zu verhindern. In diesem Fall erleidet der Kunde eine Art Rufschädigung, da der Betreiber ihn nicht länger als vertrauenswürdig einstuft und ihm den Zugriff auf den Dienst entzieht.

Finanzielle Folgen

Abhängig von der Nutzungsart bzw. im Fall von „pay-per-use“-Abrechnung können hohe Schäden entstehen. Andererseits können durch den resultierenden Ausfall des Dienstes und der dadurch nicht gewährleisteten Verfügbarkeit ebenso nicht bezifferbare Schäden entstehen. Ein Beispiel dafür ist die Internet-Werbeindustrie und ihre Einbußen durch Bot-Netze[95] [92].

6.2.8 Szenario „Malicious Insider“

Rechtliche Folgen

Integrität und Vertrauen sind durch einen bösartigen Insider nicht mehr gegeben, was sich je nach Branche als geschäftsstörend bis existenzvernichtend auswirken kann, wenn geheime Interna durch den Insider nach außen getragen werden. Durch eine solche Veröffentlichung von Daten können vertraglich geregelte Zugeständnisse an die Datensicherheit nicht mehr gewährleistet werden, wodurch rechtliche Schritte bzgl. Vertragsbruchs möglich sind.

Technische Folgen

Die Identifizierung eines Malicious Insiders kann sich durch die dezentrale und verteilte Natur der Cloud als äußerst schwierig erweisen. Jede Sicherheitsänderung ist auch dem Insider bekannt. Einzig Sicherheitsmaßnahmen wie die Verschlüsselung von Dokumenten seitens des Kunden kann Sicherheit gewährleisten.

Soziale Folgen

[95] Chameleon click fraud, abrufbar unter: http://www.infosecurity-magazine.com/view/31389/chameleon-click-fraud-botnet-costs-advertisers-6m-per-month/ (letzter Zugriff: 24.03.2014)

Es kommt zu einer schwerwiegenden Rufschädigung des Service-Anbieters. Werden Daten durch den Insider offengelegt, betrifft dies auch das Unternehmen sowie die Kunden.

Finanzielle Folgen

Durch Offenlegungen des Insiders können dem Unternehmen einerseits Schadensersatzforderungen von Dritten entstehen, andererseits besteht die Möglichkeit des Geschäftsentganges, sollte der Insider Geheimnisse zu Konkurrenten transferieren.

6.2.9 Szenario „Missbrauch von Cloud-Services“

Rechtliche Folgen

Werden die Kapazitäten eines Cloud-Services über kompromittierte Benutzerkonten für kriminelle Zwecke missbraucht, können einerseits gegen den Besitzer des Kontos rechtliche Schritte im Sinne von Beihilfe eingeleitet werden, andererseits kann ein Verstoß gegen die Benutzerrichtlinien des Dienstes, welcher mit Schadensersatzforderungen Dritter verbunden ist, vom Anbieter auf den Kunden abgewälzt werden.

Technische Folgen

Zunächst gilt es, die Quelle des Missbrauchs zu finden, diese zu schließen und sicherzustellen, dass dieser in solcher Art nicht mehr vorkommen kann. Dazu zählt einerseits die Veröffentlichung der Vorgehensweise des Angreifers, andererseits angepasste Richtlinien und Prozesse. Wird ein Benutzerkonto als Angriffsverktor genutzt, muss sichergestellt werden, dass die Zugangsdaten geändert werden.

Soziale Folgen

Werden Cloud-Dienste für kriminelle Tätigkeiten missbraucht, gerät der Dienst bei Aufdeckung dieser in Verruf. Gleiches gilt für involvierte Benutzerkonten, die vom Anbieter für die weitere Nutzung gesperrt werden können.

Finanzielle Folgen

Wird der Account des Kunden für den Missbrauch benutzt und besteht ein „pay per use“-Abkommen mit dem Anbieter, können durch den Missbrauch des Dienstes dem Kunden ungewollte Operationen in Rechnung gestellt werden.

6.2.10 Szenario „Unzureichende Due Diligence“

Rechtliche Folgen

Diesem Szenario liegt Fahrlässigkeit zugrunde, und auch der Grundsatz: „Unwissenheit schützt nicht vor Strafe“ gilt, wenn vertraglich geregelte Maßnahmen nicht erfüllt werden können. Dies betrifft insbesondere Verstöße gegen Datenschutzbestimmungen, wenn dadurch Daten offengelegt werden und im weiteren Sinne Verletzungen der Sorgfaltspflicht und des Verbandsverantwortlichkeitsgesetzes vorliegen.

Technische Folgen

Durch Vorfälle dieser Art kann die Verfügbarkeit, die Integrität und die Vertraulichkeit von verarbeiteten Daten nicht länger gewährleistet werden. Um diese wieder bereitzustellen, bedarf es der Neuregelgungen der Verantwortlichkeiten oder erweiterter Mitarbeiterschulungen, um diese in solchen Belangen zu sensibilisieren.

Soziale Folgen

Unzureichende Due Diligence seitens eines Mitarbeiters in führender Position wirft allgemein ein schlechtes Licht auf das Unternehmen und den Dienst und schwächt gleichzeitig das Vertrauen von Kunden.

Finanzielle Folgen

Durch unbedachtes Auslagern und nötigenfalls Nachrüsten oder Anpassen von Lösungen können dem Unternehmen nicht zu unterschätzende Kosten entstehen. Weiters können Forderungen von Strafzahlungen im Sinne des Verbandsverantwortlichkeitsgesetzes geltend gemacht werden.

6.2.11 Szenario „Gemeinsame Nutzung“

Rechtliche Folgen

Durch die gemeinsame Nutzung von Ressourcen sind Integrität und Vertraulichkeit von verarbeiteten Daten nicht mehr automatisch gegeben. Werden dadurch Daten offengelegt, besteht einerseits die Möglichkeit, gegen bestehende Datenschutzbestimmungen zu verstoßen, andererseits können betroffene Kunden Forderungen geltend machen. Ähnliches gilt, werden vertragliche zugesicherte Sicherheitsleistungen dadurch nicht erfüllt.

Technische Folgen

Sicherheitsmaßnahmen wie Verschlüsselung der Daten bevor sie in die Cloud geraten, können Abhilfe schaffen. Im Fall von Software-Ressourcen sollte der Service-Anbieter Änderungen vornehmen.

Soziale Folgen

Durch die Offenlegung von Daten aufgrund von gemeinsamer Nutzung von Ressourcen besteht ein Grund, die Vertraulichkeit des Dienstes anzuzweifeln, was sich im weiteren Verlauf zu Rufschädigung entwickelt. Weiters können auch die durch die Offenlegung betroffenen Kunden zu Schaden kommen.

Finanzielle Folgen

Schadensersatzforderungen seitens betroffener Kunden sind möglich. Werden geschäftsrelevante Daten offengelegt, kann dadurch die Wettbewerbsfähigkeit von Unternehmen gefährdet sein bzw. Geschäftsentgang drohen.

6.2.12 Szenario „Hardware Security“

Rechtliche Folgen

Kommt sicherheitstechnisch fehlerhafte Hardware zum Einsatz und können dadurch vertraglich geregelte Sicherheitsmaßnahmen nicht gewährleistet werden, besteht die Möglichkeit, dass Schadensersatzforderungen geltend gemacht werden.

Technische Folgen

Ist Hardware kompromittiert beziehungsweise ist die Sicherheitsstufe, die seitens der Hardware geboten wird nicht ausreichend, bleibt nur, diese durch Alternativen zu ersetzen. Je nach Anwendungsgebiet ist es unterschiedlich schwer, passende Alternativen zu finden.

Soziale Folgen

Mangelnde Sicherheitsleistungen schaden in jedem Fall dem Ruf und der Wettbewerbsfähigkeit des Anbieters, da der Eindruck entsteht, man wolle sich nicht um die sichere Verwahrung und kontrollierten Zugriff auf Daten der Kunden kümmern.

Finanzielle Folgen

Einerseits können Schadensersatzforderungen durch verabsäumte Lieferung von vertraglich geregelten Sicherheitsmaßnahmen entstehen, andererseits Kosten durch die Neubeschaffung oder die Neukonfiguration der Hardware.

6.3 Risikominimierungsmaßnahmen

In diesem Kapitel werden Maßnahmen vorgestellt, die im Fall der vorgestellten Szenarien die Risiken senken können.

6.3.1 Szenario „Verletzung der Datenvertraulichkeit“

Das Risiko, dass ungewollt sensible Daten durch Dritte offengelegt werden, kann durch mehrere Ansätze minimiert werden. Dabei muss zwischen Ansätzen, welche vom Cloud-Dienst-Betreiber zur Verfügung gestellt werden und solchen, die der Benutzer heranzieht, unterschieden werden.

Vom Betreiber ausgehend besteht einerseits die Möglichkeit, Zugriffsrechte und Benutzer-Rollen-Management zu verwenden, um den unbeabsichtigten oder auch bösartig beabsichtigen Zugriff auf Daten zu unterbinden. Verstärkte Sicherheit und zusätzliche Risikominimierung bietet die Verschlüsselungstechnologie, um das Lesen der Daten im Fall einer Offenlegung unmöglich zu machen, gesetzt den Fall, dass die verwendeten Schlüssel sicher verwahrt wurden. Folglich ist die Verwendung einer sicheren und vertrauenswürdigen Schlüsselverwaltung ein unbedingtes Kriterium für den Diensteanbieter, um von dessen Seite Datenvertraulichkeit zu gewährleisten.

Wird Verschlüsselung vom Cloud-Dienst-Betreiber nicht verwendet oder bereitgestellt, sollte der Benutzer Daten von sich aus verschlüsseln, bevor diese dem Dienst übergeben werden. Durch dieses Vorgehen kann das Risiko einer Offenlegung auf ein sehr niedriges Level abgeschwächt werden. Selbst im Fall, dass der Betreiber nicht sicher ist beziehungsweise Hintertüren befürchten muss (vgl.

u.a. PRISM), sind die Daten immer noch relativ gut gegen Offenlegung geschützt. Abhängig von den verwendeten Algorithmen und der Länge der Schlüssel können verschlüsselte Daten nur mit sehr hohem Rechenaufwand wieder lesbar gemacht werden. Zwei konkrete Tools zur zuverlässigen Datenverschlüsselung sind:

TrueCrypt[96] [93] ist eine Open-Source–Verschlüsselungssoftware, welche es erlaubt, verschlüsselte Container zu erstellen. Innerhalb dieser Container können Dateien in verschlüsselter Form abgelegt werden. Da der Container aus nur einer Datei besteht, eignet sich TrueCrypt besonders gut, um eigene Daten auf Filesharing-Plattformen wie Dropbox zu verschlüsseln. Dabei wird nur der Container zum Cloud-Service hochgeladen und vom Nutzer unter Verwendung seines persönlichen Schlüssels geöffnet. Sowohl die gespeicherten als auch die zwischen Cloud-Service-Anbieter und -Nutzer transferierten Daten sind dabei verschlüsselt und können nur vom Nutzer selbst, aber nicht vom Cloud-Service-Anbieter eingesehen werden.

TAVUU[97] [94] ist eine von Xylem Technologies (Unternehmensstandort: Wien) entwickelte Verschlüsselungs- und Verteilungssoftware, welche es ermöglicht, persönliche Daten verschlüsselt und auf mehrere Cloud-Service-Anbieter verteilt abzuspeichern. Im Gegensatz zu TrueCrypt arbeitet der Nutzer wie gewohnt auf seinem Rechner und TAVUU verschlüsselt, verteilt und synchronisiert im Hintergrund die Daten in die Cloud. Durch die verteilte Speicherung ist es dem Cloud-Service-Anbieter oder einem Angreifer selbst bei Kenntnis des Schlüssels nicht möglich, die Daten des Nutzers zu rekonstruieren.

Um die Vertraulichkeit des Anbieters von Cloud-Diensten zu erhöhen, bietet es sich zudem an, angebotene Leistungen auf vertraglicher Basis zu regeln. Selbiges gilt auch für den dem Kunden zugesicherten Datenschutz seitens des Anbieters. Neben den erwähnten Zusicherungen können nationale oder international anerkannte Zertifikate und Standards von externen Stellen überprüft werden. Derartig normierte Standards bieten einfach zugängliche Information über interne Organisationsstrukturen, Datenhandhabung und Sicherheit, ohne gleichzeitig zu viel über die konkrete Implementierung und potenziell mögliche Angriffsvektoren auf die Dienste zu verraten.

6.3.2 Szenario „Verletzung der Integrität“

Datenintegrität beschreibt die Fähigkeit sicherzustellen, dass Daten erstens gespeichert werden, wie es ursprünglich vom Besitzer beabsichtigt wurde, und zweitens dass Daten, auf die zugegriffen wird, auch tatsächlich in dem Zustand sind, in dem sie abgelegt wurden. Folglich ist jede unbeabsichtigte Änderung durch Speicher-, Zugriff- oder Rechenoperationen ebenso wie Hardwarefehler, menschliches Versagen oder böswilliges Handeln ein Bruch mit der Integrität von Daten. Falls unerwünschte Abänderungen von Daten oder Inhalten nicht verhindert werden können, muss zumindest sichergestellt werden, dass die Manipulation erkannt wird.

Neben den technischen Voraussetzungen, welche im Fall von Cloud-Diensten vom Dienstbetreiber bereitzustellen sind, bedarf es auch von Seiten des Dienst-Benutzers Maßnahmen, um die Wahrschein-

[96] TrueCrypt, abrufbar unter: www.truecrypt.org/ (letzter Zugriff: 24.03.2014)
[97] TAVUU, abrufbar unter: www.tavuu.com/ (letzter Zugriff: 24.03.2014)

lichkeit einer Verletzung der Datenintegrität zu verringern. Schließlich ist letzten Endes der Datenbesitzer selbst für seine Daten verantwortlich. Dieser Behauptung folgend kann auch ein technisch bestens geschützter Diensteanbieter nicht verhindern, dass durch Unachtsamkeit oder Unbedarftheit seiner Benutzer Sicherheitsmechanismen kompromittieren, wodurch die Integrität von Daten nicht mehr gewährleistet werden kann.

Seitens des Dienstbenutzers ist zu erwarten, dass (i) jeder Subbenutzer, der Zugriff auf den Dienst benötigt, dafür ein eigenes Benutzerkonto heranzieht, (ii) jeder Subbenutzer seine Kontodaten geheim hält und nicht weitergibt, (iii) jede Datenmanipulation auf ein Benutzerkonto zurückzuführen ist, (iv) jedes Benutzerkonto auf eine existente und gleichfalls dafür autorisierte Person zurückzuführen ist, (v) Benutzer gegenüber Cloud und speziell Datenintegrität sensibilisiert sind und (vi) organisatorische Maßnahmen oder Richtlinien bestehen, um grundsätzlich das Risiko von menschliches Versagen zu minimieren.

Letzteres kann beispielsweise durch Mitarbeiterschulung und spezielles Training erreicht werden, wie auch durch das Bereitstellen von Leitlinien und Anlaufstellen im Fall von Unklarheiten beim Umgang mit Cloud-Diensten.

6.3.3 Szenario „Beeinträchtigung der Verfügbarkeit“

Die Verfügbarkeit von Daten bildet gemeinsam mit der Vertraulichkeit und der Integrität die Grundpfeiler der Informationssicherheit. Der Begriff der Verfügbarkeit umfasst zwar nicht alleinig die Bereitstellung von Dienst und Daten, sondern auch beispielsweise Maßnahmen im Fall von Insolvenz des Anbieters und den damit verbundenen Unklarheiten über das Fortbestehen von Daten und Dienst.

Zur Risikoverminderung im Fall eines Verfügbarkeitsverlustes ist bei seriösen Anbietern gängige Praxis, sogenannte *Service Level Agreements* (kurz SLAs) anzubieten, welche dem Kunden die Verfügbarkeit von Daten und Diensten auf vertraglicher Basis gewährleisten. Falls keine spezifizierte *SLA* angeboten wird, können vertragliche Regelungen zwischen Betreiber und Kunden formuliert werden, um selbiges zu erreichen. Auf Basis der im Vertrag zugesicherten Maßnahmen zur Erhaltung der Verfügbarkeit kann der Kunde sich auf Maßnahmen seinerseits einstellen, respektive erleichtert dies die Risikoabschätzung im Fall der Fälle beträchtlich.

SLAs bieten auch technisch weniger versierten Benutzern einen relativ einfachen Zugang, um Dienste miteinander zu vergleichen und nach eigenen Kriterien auszuwählen.

Geht es um Datenverfügbarkeit, müssen auch Sicherungskopien von Daten besprochen werden. Hier mag die Lösung mit lokalen, vom Benutzer selbst gemachten Sicherungen verlockend klingen, allerdings kann dies zu erhöhtem Aufwand an Hardware und Speichermedien führen. Ein weiterer Nachteil ist, dass bei lokalen Sicherungskopien nicht zwingend die Datenverfügbarkeit gegeben ist, die unter Umständen benötigt wird, um etablierten Organisationsstrukturen und Geschäftsprozessen gerecht zu werden.

Abhängig vom genutzten Cloud-Betreiber und dem Umfang des angebotenen Servicepakets werden oftmals seitens der Betreiber Sicherungen von Kundendaten gemacht, um Datenverfügbarkeit zu ge-

währleisten. Problematisch kann sich hier der Zugriff von außerhalb erweisen, wenn diese nicht vom Benutzer vorgesehen sind oder die Zeitpunkte der Sicherung nicht transparent gestaltet wurden.

Abhilfe kann hier das vom Wiener Unternehmen Xylem Technologies entwickelte Tool **TAVUU** schaffen (siehe Abschnitt 6.3.1). TAVUU bietet die Möglichkeit, die in der Cloud gespeicherten Daten nicht nur zu verschlüsseln, sondern auch auf mehrere Cloud Service-Anbieter zu verteilen. Somit stehen die Daten auch bei fehlender Verfügbarkeit eines einzelnen Anbieters für den Kunden zur Verfügung. Die Verwaltung der Datenspeicherung erfolgt zwar vollautomatisiert im Hintergrund, ist aber dennoch für den Nutzer transparent.

6.3.4 Szenario „Datenverlust“

Der Verlust von Daten ist ein bedrohliches Szenario für alle Benutzergruppen von Cloud-Diensten. Auch wenn konkreten Daten meist kein materieller Wert beigemessen werden kann, so kann dennoch das Abhandenkommen von Datensammlungen oder von Dokumenten, die auf dem Cloud-Dienst abgelegt wurden, den Besitzer schwer treffen. Hier kann Verlust von ideellen Werten (beispielsweise Urlaubsfotos) oder materiellen Werten im Fall von Geschäftsunterlagen, Kundendaten o.ä. entstehen.

Indirekt können durch Datenverlust noch weitere materielle Schäden verschuldet werden, etwa die Verzögerung vertraglich geregelter Vereinbarungen oder gänzlicher Geschäftsentgang.

Um sich gegen Datenverlust zu wappnen empfiehlt es sich, Maßnahmen zur regelmäßigen Datensicherung zu implementieren, um die damit verbundenen Risiken abzuschwächen. Dies stellt, nach dem Stand der aktuellen Erkenntnis, die einzig effektive Methode dar, um die entsprechenden Risiken auf ein akzeptables Niveau zu senken.

Cloud-Betreiber sorgen teilweise für Redundanz von Kundendaten, um Verlust vorzubeugen, allerdings sind diese Vorgänge für den Kunden meist nicht transparent gestaltet und laufen automatisiert ab, wobei der Kunden die direkte Kontrolle über seine Daten verlieren kann. Dies kann beispielsweise problematisch sein, wenn vertrauliche Daten die vorgesehenen Örtlichkeiten als Sicherungskopie verlassen und diese an dritten Standorten mit geringeren Datenschutzstandards oder Sicherheitsvorkehrungen abgelegt werden.

Neben dem Kontrollverlust für Daten, der mit der Benutzung von Cloud-Diensten einhergeht, und der fehlenden Transparenz für Kunden ist meist der Zeitpunkt der automatisierten Sicherung ebenso wenig transparent bzw. auch nicht frei wählbar. Die Löschung bzw. Rückgabe von Daten und deren Sicherungskopien kann sich weiter als kompliziert erweisen, sofern vom Cloud-Betreiber keine Gewährleistungen in dieser Richtung gegeben sind.

Um oben beschriebene Risiken zu minimieren, hat der Cloud-Benutzer die Möglichkeit, lokale Sicherungskopien zu nutzen, womit prinzipiell allerdings einer der Grundgedanke der Cloud, nämlich die Einsparung von benötigter Hardware, ad absurdum geführt wird. Dahingegen können vertraglich vereinbarte Maßnahmen zur Datensicherung, wie beispielsweise in einer SLA dem Kunden Sicherheit garantieren und möglicherweise auch den Sicherungsvorgang transparenter machen, oder aber dem Kunden mehr Möglichkeiten und Kontrolle zum Prozess der Datensicherung anbieten.

Abhilfe kann hier das vom Wiener Unternehmen Xylem Technologies entwickelte Tool **TAVUU** schaffen (siehe Abschnitt 6.3.1). TAVUU bietet die Möglichkeit, die in der Cloud gespeicherten Daten nicht nur zu verschlüsseln, sondern auch auf mehrere Cloud-Service-Anbieter zu verteilen. Idealerweise werden Cloud-Service-Anbieter aus unterschiedlichen geografischen Regionen gewählt. Somit stehen die Daten auch bei völligem Ausfall eines einzelnen Anbieters für den Kunden zur Verfügung. Die Verwaltung der Datenspeicherung erfolgt vollautomatisiert im Hintergrund und ist für den Nutzer transparent.

6.3.5 Szenario „Übernahme des Accounts oder des Datenverkehrs“

Die Übernahme von Benutzerkonten durch Angreifer stellt ein schwer zu überwindendes Risiko dar, da einerseits aus Sicht der Systemsicherheit kein Angriff passiert, denn schließlich wird ein legitimierter Account für Zugriffe benutzt, und andererseits die Kontrolle über Benutzer und deren Umgang mit Zugangsdaten schon allein rein rechtlich gesehen ihre Grenzen hat. Folglich bleibt hier meist die Schwachstelle Mensch übrig, wenn technische Vorkehrungen nicht ohne Aufwand oder Risiko überwunden werden können. Ein Beispiel sind hier Spearphishing-Attacken, die die übliche Phishing-Methodik mit auf den Empfänger zugeschnittenem Inhalt kombinieren, um Zugangsdaten offen zu legen. Neben Phishing-Attacken werden außerdem technisch ausgereifte Malware-Tools genutzt, um Zugangsdaten offenzulegen. Für diese gestohlenen Daten besteht teilweise ein Schwarzmarkt, was es auch technisch unbedarften, aber hoch motivierten Angreifern erlaubt, mit mäßigem Aufwand an Zugangsdaten zur Übernahme des Accounts zu gelangen. Die Verwendung einer einzigen Kombination von Zugangsdaten für mehrere Dienste stellt beispielsweise ein hohes Risiko für die Konten aller damit verwendeter Dienste dar, denn wird einmal der Datensatz offengelegt, sind potenziell alle Dienste gefährdet. Selbiges gilt bei der Verwendung von „unsicheren“ Passwörtern, etwa vom Betreiber standardmäßig definierte Werte oder zu kurze Passwörter, die ein Erraten durch Brute-Force-Methoden erlauben. Maßnahmen zum Schutz vor Malware beinhalten das regelmäßige Aktualisieren von Betriebssystemen, Software und Software-Firewall-Lösungen (Virenprogramme u.ä.) sowie beispielsweise „Blacklisting“, um Zugriffe auf Webseite und -dienste zu verhindern, die für die Verbreitung von Malware bekannt sind.

Die Sensibilisierung von Benutzern gegenüber Malware und Phishing kann zumindest das entsprechende Verständnis fördern, erhöhte Sicherheit bietet jedoch nur das Verwenden von sicheren Passwörtern, einem vertrauenswürdigen Computersystem und einer Politik des regelmäßigen Änderns von benutzten Passwörtern. Die Autorisierung des Benutzers via der klassischen Kombination aus Benutzernamen und Passwort kann durch einen weiteren Faktor ergänzt werden. Dieses zusätzliche Feature kann verschiedenartiger Natur sein, wie biometrische Merkmale (Fingerabdrücke oder Retina), Hardware-Tokens, die digitale Schlüssel in sich tragen oder der Verbund mit einer Identifikation über weiteren Dienste oder Geräte, z.B. durch die Zusendung eines generierten Codes an ein Mobiltelefon oder eine E-Mail-Adresse.

Neben den direkten Angriffen auf Benutzerkonten werden allgemein auch passive Vorgehensweisen zur Offenlegung von Zugangsdaten verwendet, wie etwa das Abfangen und Belauschen des Datenverkehrs. So können beispielsweise Benutzernamen und Passwörter sehr einfach ausgelesen werden,

wenn diese über unverschlüsselte Verbindungen übertragen werden. Selbiges gilt natürlich auch für jedwede Kommunikation, die über derlei Kanäle abgewickelt wird.

6.3.6 Szenario „Unsichere Schnittstellen“

Cloud-Dienste sind komplexe verteilte Systeme, die auf verschiedensten Kombinationen aus einzelnen Hardware- und Software-Komponenten aufbauen. Es muss gewährleistet sein, dass diese effektiv miteinander kommunizieren können. Da über die Systemschnittstelle die dahinterliegende Komponente ansprechbar ist, definiert sich das Sicherheitsniveau der Komponente auch über das Niveau der Schnittstelle.

In der Regel hat der Kunde kaum Einblick und schon gar keine Kontrolle über die im Cloud-Dienst verwendeten Schnittstellen. Es obliegt alleine dem Anbieter, für sichere Schnittstellen zu sorgen, wobei hier Best-Practice-Ansätze und Standards das Vorgehen unterstützen. Der Erwerb von Zertifikaten, die die oben genannten Punkte abdecken, beziehungsweise die Verwendung von allgemein anerkannten und als sicher eingestuften Technologien kann für eine breitere Akzeptanz der Kunden sorgen und erlaubt es, technisch wenig versierte Benutzer für die Nutzung des Dienstes zu gewinnen.

Für Benutzer von Cloud-Diensten stellt sich die Aufgabe, Anbieter auf die verwendeten Schnittstellen beziehungsweise intern benutzten Sicherheits-Modelle zu überprüfen. Da dies meist nicht direkt möglich ist, muss sich der Kunde auf Angaben und Zusicherungen des Diensteanbieters verlassen, die nach Möglichkeit auch vertraglich geregelt sein sollten. Zertifikate über verwendete Informationstechnologien erlauben dem Kunden, das Sicherheitsniveau abzuschätzen.

6.3.7 Szenario „Denial of Service“

Im vorigen Kapitel wurde im Zusammenhang mit DoS-Attacken einerseits auf die Überlastung von Diensten (wobei hier nicht zwischen absichtlicher und unabsichtlicher Verursachung unterschieden werden muss) und andererseits auf wirtschaftliche Angriffe, welche auf die Bezahlmodelle zwischen Kunden und Betreiber abzielen, eingegangen.

Erstgenannte Angriffe treffen hauptsächlich den Dienst selbst, allerdings kann dem Kunden durch die Störung der Verfügbarkeit von Daten und Anwendungen wirtschaftlicher Schaden entstehen. Hier sind Maßnahmen auf Seiten des Dienstbetreibers gefragt, um derlei Angriffe zu erkennen und zu unterbinden. Falls es dennoch zu Ausfällen kommt, können vertragliche Regelungen, wie etwa ein SLA, das Risiko für den Kunden kalkulierbarer machen. Lokale Sicherungskopien von Daten können natürlich im Fall eines Dienstausfalles für verminderte Unannehmlichkeiten sorgen, allerdings ist fraglich, ob der damit verbunden Arbeits- und Hardwareaufwand gerechtfertigt ist. Auch in Fall eines DoS-Angriffs können Tools wie **TAVUU** den weiteren Zugriff auf die gespeicherten Daten durch die verteilte Speicherung bei mehreren Cloud-Service-Anbieter ermöglichen. In diesem Szenario empfiehlt es sich, bei der Anbieterauswahl darauf zu achten, dass diese nicht von einer gemeinsamen Infrastruktur abhängig sind (z.B. Anbieter, welche die Amazon-Infrastruktur nutzen).

Aus Sicht der Dienste-Anbieter bietet ein „pay per use“-Bezahlmodell einen gewissen Schutz gegen klassische DoS-Attacken. Werden jedoch gestohlene Kundendaten für den Gebrauch von Cloud-Diensten benutzt, welche ein derartiges Bezahlmodell implementiert haben, werden die illegalen Zu-

griffe selbstverständlich dem legalen Besitzer des Kontos in Rechnung gestellt. Die entstandenen, nicht kontrollierbaren Kosten können diesen wiederum zwingen, die Benutzung des Dienstes (wie bereits erwähnt) gänzlich einzustellen, da das nun offengelegte Konto nur sehr schwer wieder abgesichert werden kann. In diesem Fall sollte sichergestellt werden, dass Daten nach Terminierung des Vertrages für einen gewissen Zeitraum für einen Export zur Verfügung stehen und diese Daten auch gegebenenfalls unter akzeptablem wirtschaftlichem Aufwand auf andere Cloud-Dienste migriert werden können.

6.3.8 Szenario „Malicious Insider“

Der Bedrohung durch als vertrauenswürdig angesehene Personen, die vollen Zugriff auf Dienste haben und deren Benutzung böswillig oder durch Nachlässigkeit empfindlich stören, ist allein mit technischen Mitteln nur schwer beizukommen. Zum einen sind aus Sicht des Systems jegliche Schritte völlig legitim, sofern der Benutzer dafür autorisiert ist, zum anderen verfügen Insider über genaues Wissen bzgl. Sicherheitsvorkehrungen, wie diese überwindbar und die Spuren von Angriffen verwischbar sind. Des Weiteren sind die unterschiedlichen Motivationen des Angriffes von technischer Seite schwer beschreibbar. Ergänzend erleichtern Sicherheitsmaßnahmen, welche nur externe Bedrohungen berücksichtigen, den internen Angriff.

Folglich sind technische Maßnahmen erforderlich, die auch nach innen restriktiv wirken, wie beispielsweise strenge Benutzer- und Rechtemanagementsysteme, konsequente Verwaltung von analogen wie digitalen Gütern und das Erfassen von Zugriffen auf diese. Bei kritischen Vorgängen empfiehlt sich generell die Vorgehensweise des Vier-Augen-Prinzips. Ergänzend dazu bieten sich organisatorische Maßnahmen im Rahmen des Personalmanagements, wie Hintergrundüberprüfung bei Einstellung von Personal, an die Tätigkeit entsprechend angepasste Rechte und sofortiger Entzug dieser bei Ausscheiden aus der Organisation. Andere organisatorische Regelungen umfassen beispielsweise das Sensibilisieren von Mitarbeitern gegenüber der Thematik von Insider-Angriffen, damit verbundene auffällige Verhaltensmuster des Angreifers und Einrichten einer Anlaufstelle, um eminente Beobachtungen mitzuteilen.

Werden sensible Tätigkeiten oder der Umgang mit sensiblen Daten an dritte Parteien ausgelagert, sollte sichergestellt werden, dass diese ebenso ihre Mitarbeiter gegenüber Datenschutz sensibilisieren, gegebenenfalls zur Geheimhaltung verpflichten und, je nach Umgang mit klassifizierten Daten oder Zugang zu solchen, ebenfalls Hintergrundüberprüfungen der Person durchführen.

Das Risiko durch Insider kann nie völlig ausgeschlossen werden, da derartige Vorfälle meist schon durch unbewusstes Fehlverhalten von Mitarbeitern ausgelöst werden können. Wird Fehlverhalten durch umfangreiche Schulung minimiert, bleibt noch das Restrisiko durch Mitarbeiter, die tatsächlich illegale Absichten haben.

6.3.9 Szenario „Missbrauch von Cloud-Services“

Dieses Szenario beschreibt hauptsächlich die Nutzung der kostengünstigen Kapazitäten von Cloud-Diensten für kriminelle Zwecke. Wie bereits erwähnt, sind hauptsächlich die Anbieter selbst gefragt, dies nach Möglichkeit zu erkennen und zu unterbinden. Für den Cloud-Nutzer hingegen bietet es sich

ebenfalls an, Maßnahmen zur Absicherung seines Kontos zu treffen, um dieses nicht für kriminelle Machenschaften seitens unbekannter Dritter verfügbar zu machen. Hierfür bieten sich Schritte an, wie sie auch in den Abschnitten „Szenario Übernahme des Accounts oder des Datenverkehrs“ oder „Szenario unsichere Schnittstellen“ erwähnt wurden.

Ansonsten gilt sicherzustellen, dass nur Mitarbeiter Zugang zum Dienst erhalten, die dies auch unbedingt zur Ausführung ihrer Tätigkeiten benötigen, um schon allein die Anzahl der genutzten Benutzerkonten überschaubar zu halten.

6.3.10 Szenario „Unzureichende Due Diligence“

Die Problematiken, die in diesem Szenario auftreten beziehungsweise dieses im Grunde verursachen, haben ihren Ursprung in dem unzureichenden Befassen mit benutzten Technologien, den damit verbundenen Konzepten und den daraus resultierenden Sicherheitsanforderungen. Cloud-Technologie wird oftmals von Management-Entitäten – den Versprechungen von Hardware-Einsparungen und erhöhter Verfügbarkeit folgend – ohne ausreichende Prüfung auf die internen Anforderungen in der Organisation eingeführt und des Weiteren als selbstregulierend, folglich ohne Verwaltungsaufwand, betrachtet.

Um die Folgen derartiger Vorgehensweisen zu minimieren, ist es notwendig, zuallererst die Technologie mit den Anforderungen der Organisation abzugleichen, alle involvierten Benutzer für die Verwendung und Sicherheitsrisiken von Cloud-Diensten zu sensibilisieren und gegebenenfalls für diese verpflichtende Workshops und Trainingseinheiten anzubieten.

6.3.11 Szenario „Gemeinsame Nutzung“

Durch die mangelnde Transparenz von Cloud-Diensten gegenüber den Benutzern im Sinne von Speicherort und des verwendeten Ressourcenmanagements, besteht die Möglichkeit, dass Daten irrtümlich oder bewusst offengelegt werden können.

Maßnahmen, um beschriebene Risiken von Offenlegung durch gemeinsame Nutzung von Ressourcen zu minimieren, sind einerseits erneut die Verschlüsselung von gespeicherten Daten durch den Benutzer, sofern diese nicht bereits vom Betreiber des Dienstes angeboten wurde. Zudem gilt es sicherzustellen, dass der Dienste-Anbieter eine Trennung von Ressourcen für jedes Benutzerkonto vornimmt, wie es beispielsweise durch virtuelle Maschinen oder logische Trennung von Speicherbereichen üblich ist. Auf diese Art und Weise sollte das Risiko der Offenlegung von Kundendaten durch andere Kunden spürbar minimiert werden.

6.3.12 Szenario „Hardware Security“

Zunächst gilt sicherzustellen – sofern dies dem Kunden möglich ist – dass die beim Cloud-Anbieter verwendete Hardwarelösungen den eigenen Anforderungen genügen. Bei fehlendem Kontrollrecht können vertraglich zugesicherte Sicherheitsmaßnahmen oder Zertifikate Abhilfe schaffen.

Ferner sollten die lokal auf Seiten des Kunden für den Zugriff auf den Cloud-Dienst benutzte Hardware wie Netzwerk-Geräte, Rechner und mobile Geräte ebenso überprüft und somit sichergestellt

werden, dass beispielsweise die Kommunikation selbst bereits in verschlüsselter Form stattfindet, wodurch das Abfangen von Informationen nur noch mit erhöhtem Aufwand möglich ist. Werden drahtlose Netzwerke genutzt, sollte auch hier darauf geachtet werden, dass eine ausreichende Verschlüsselung verwendet wird.

6.4 Zusammenfassung der wichtigsten Maßnahmen

Basierend auf den in den letzten Kapiteln dargestellten Bedrohungen können folgende Maßnahmen als die Grundpfeiler für sicheres Cloud-Computing zusammengefasst werden:

- konkrete, nachvollziehbare Service Level Agreements mit angemessenen Konsequenzen bei Nichteinhaltung
- explizite vertragliche Regelung datenschutzrechtlicher Erfordernisse, abgestimmt auf den eigenen Kundenkreis
- Verschlüsselung des Datenverkehrs vom/zum Cloud-Computing-Anbieter und Verschlüsselung der beim Cloud-Computing gespeicherten Daten mit eigenem (dem Anbieter nicht bekannten) Schlüssel (Einsatz von Tools wie zum Beispiel TrueCrypt oder TAVUU)
- wirksames und effizientes Schlüsselmanagement, um die verschlüsselten Daten berechtigten externen Partnern und internen Mitarbeitern verfügbar zu machen
- Klare vertragliche Regelung von Exit-Strategien: diese sollten sowohl die rechtliche (z.B. Konkursfall des Cloud-Computing-Anbieters) als auch die technische Seite (z.B. Portieren der Daten zu einem anderen Anbieter) umfassen.
- Externe Zertifizierungen der Cloud-Computing-Anbieter geben zusätzliche Sicherheit bzgl. der korrekten Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen.

7 LEITFÄDEN FÜR BEHÖRDEN UND KMUS

Dieses Kapitel beschreibt zielgruppenspezifische Leitfäden zur sicheren Cloud-Nutzung in Behörden und KMUs. Abgeleitet von den vorangegangenen Kapiteln werden Nutzungsmodelle, rechtliche Rahmenbedingungen und Schutzbedarfskategorien definiert sowie Entscheidungsbäume und Checklisten zur einfachen praktischen Umsetzung erstellt.

7.1 Mögliche Nutzungsmodelle

Mögliche Nutzungen von in der Public Cloud bereitgestellten SaaS-Cloud-Diensten umfassen für E-PU, KMU und kleine/mittlere Behörden in erster Linie Anwendungen zwecks Kommunikation, Textverarbeitung, Tabellenkalkulation, Datenspeicherung und Kollaboration mit internen und externen Akteuren. Die folgende Tabelle zeigt die identifizierten Cloud-Dienste, deren Relevanz für EPU, KMU und Behörden sowie beispielhafte Produkte.

Tabelle 3: Cloud-Dienste

Cloud-Dienst	beispielhafte Produkte	EPU	KMU und Behörden
E-Mail	Google Mail	X	X
Instant Messaging	hosted.IM		X
Video- und Audio-Conferencing	BlueJeans	X	X
geteilte Kalender	Google Calendar		X
geteilter Speicherplatz	Dropbox		X
Datensicherung/Datenarchivierung	Wuala, ARQ	X	X
Textverarbeitung und Tabellenkalkulation	Office365, Google Docs	X	X
Abrechnung, Rechnungserstellung	Billomat	X	X
Projektmanagement	Easy-PM	X	X
CRM (Customer Relationship Management)	Mircosoft Dynamics CRM	X	X

CMS (Content Management Systeme)	Osmek		X
Zeiterfassungssysteme	TimeTac, Time&Bill	X	X
Personalgeschäftsprozesse	Utilitas		X
ERP (Enterprise Resource Planning)	NetSuite ERP		X
Dokumentenmanagementsysteme (DMS)	Folio Cloud	X	X
Softwareentwicklungswerkzeuge	GitHub	X	X
Produktivitätswerkzeuge (To-do-Listen, Notizanwendungen etc.)	Remember the Milk, Evernote	X	X
virtuelle Server	VMware	X	X
Sicherheitsdienstleistungen (E-Mail-Filter, SPAM-Abwehr, Verschlüsselung etc.)	Proofpoint	X	X

Für die wichtigsten Cloud-Dienst-Kategorien werden in der folgenden Tabelle beispielhafte, am österreichischen Markt angebotene Produkte vorgestellt. Die angegebenen Preis- und Produktinformationen erheben keinen Anspruch auf Vollständigkeit und Korrektheit (alle Preise zzgl. der gesetzlichen Mehrwertsteuer).

Tabelle 4: Produkt- und Preisinformation Textverarbeitung, Tabellenkalkulation und Kommunikation

Textverarbeitung, Tabellenkalkulation und Kommunikation			
Produkt	**Beschreibung**	**Preis**	**Anbieter**
Microsoft Office 365 for Small Business (max. 25 Nutzer)	online Textverarbeitung, Tabellenkalkulation, Präsentationserstellung, E-Mail-Kommunikation etc.		
		4,90 € pro Nutzer und Monat	Microsoft Österreich GmbH **Betrieben in Niederlanden und Irland**

		4,75 € pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Niederlanden und Irland**
Microsoft Office 365 for Midsize Business (max. 300 Nutzer)	online Textverarbeitung, Tabellenkalkulation, Präsentationserstellung, E-Mail-Kommunikation etc.		
		12,30 € pro Nutzer und Monat	Microsoft Österreich GmbH **Betrieben in Niederlanden und Irland**
		11,95€ pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Niederlanden und Irland**
Microsoft Exchange Online® 2010	E-Mails, Kalender und Kontaktverwaltung	**3,25 €** pro Nutzer und Monat	Telekom Deutschland GmbH **Betrieben in Deutschland**
		3,90 € - 8,90 € pro Nutzer und Monat	A1 Telekom Austria AG **Betrieben in Österreich**

		2,90 € - 15,90 € pro Nutzer und Monat	GPN - Global Private Network Telecommunication GmbH **Betrieben in Österreich**
		5,75 € pro Nutzer und Monat	Hutchison Drei Austria GmbH **Betrieben in Österreich**
Google Apps for Business	E-Mail, Kalender, Kontaktverwaltung, Kollaboration, Textverarbeitung, Tabellenkalkulation	**4,00 € / 8,00 € (mit Vault)** pro Nutzer und Monat	Google Inc **Betrieben in USA**
ContactOffice Regular	E-Mail, Kontakte, Meetings, Dokumente, Aufgaben etc.	**5,00 € (Light) – 20 € (Advanced)** pro Nutzer und Monat	ContactOffice Group SA **Betrieben in EU**

Tabelle 5: Produkt- und Preisinformation CRM

CUSTOMER RELATIONSHIP MANAGEMENT (CRM)			
Produkt	**Beschreibung**	**Preis**	**Anbieter**
TecArt-CRM	CRM, Groupware und Kontaktmanagement	**9,95 € (Easy) – 39,95 € (Plus)** pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Deutschland**
	ausschließlich CRM	**29,95 € (CRM) – 79,95 € (CRM**	

WICE Cloud Based CRM		**Premium)** pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Deutschland**
weclapp CRM	ausschließlich CRM	**9,95 € (Basic) – 19,95 € (Pro)** pro Nutzer und Monat	Deutsche Telekom AG [130] **Betrieben in Deutschland**
Salesforce Sales Cloud Enterprise	CRM, Social Network Tool, Analysis Tool	**4 € (Contact Manager) – 315 € (Performance)** pro Nutzer und Monat	salesforce.com Germany GmbH **Betrieben in Deutschland**
VTC CRM Cloud	CRM, Social Network Tool, Analysis Tool	**25 € (Basic)** pro Monat - **5250 € (On Premise)** pro Jahr	Different Solutions GmbH **Betrieben in Deutschland**

Tabelle 6: Produkt- und Preisinformation Online Storage und Backup

ONLINE STORAGE UND BACKUP			
Dienst	**Beschreibung**	**Preis**	**Anbieter**
Box Business/Enterprise	Backup- und Filesharing-Plattform	**12,00 € (Business) / 30,00 € (Enterprise)** pro Nutzer und Monat	Box **Betrieb erfolgt ausserhalb**

			der EU
HiDrive Pro 100 GB **HiDrive Pro**	Backup- und Filesharing-Plattform	**5,95 € (100 GB) – 139,95 € (5000 GB)** pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Deutschland**
Fabasoft STORE LOCALLY • SHARE GLOBALLY **Fabasoft Cloud Professional**	Backup- und Filesharing-Plattform	**85,00 €** pro Monat	Fabasoft Fabasoft AG **Betrieben in Österreich, Deutschland und Schweiz**
Dropbox for Business	Backup- und Filesharing-Plattform	**15 US$** pro Nutzer und Monat	Dropbox Dropbox Inc. **Betrieben in USA**
3CloudBackup	Backup- und Filesharing-Plattform	**5,75 € (10 GB) - 50 € (250 GB)** pro Nutzer und Monat	Hutchison Drei Austria GmbH **Betrieben in Österreich**

Tabelle 7: Produkt- und Preisinformation Projektmanagement

Projektmanagement			
Produkt	**Beschreibung**	**Preis**	**Anbieter**
Projecterus	Projektmanagement und Projektplanerstellung	**39,95 € (Basic) - 399,95 € (Enterprise)** pro Nutzer und Monat	Deutsche Telekom AG **Betrieben in Deutschland**
Projectfacts	Monitoring und Planung von Projekten	**12,64 €** pro Nutzer und Monat (fallend mit steigender Anzahl der Nutzer)	5 POINT AG **Betrieben in Deutschland**

Tabelle 8: Produkt- und Preisinformation Rechnungserstellung und Rechnungsverwaltung

Rechnungserstellung und Rechnungsverwaltung			
Produkt	**Beschreibung**	**Preis**	**Anbieter**
Scopevisio AB-RECHNUNG Smart	Rechnungserstellung und Monitoring	**9,95 € (1 Nutzer) - 69,95 € (10 Nutzer)** pro Monat	Deutsche Telekom AG **Betrieben in Deutschland**
Billomat	Rechnungserstellung und Monitoring	**6,00 € (S+) - 48,00 € (XL)** pro Monat	Billomat GmbH & Co. KG **Betrieben in Deutschland**

Vor Abschluss eines Cloud-Service-Vertrages sollten die rechtlichen Rahmenbedingungen, der Schutzbedarf der eigenen Daten sowie Details der Vertragsgestaltung beachtet werden. In den folgenden Abschnitten werden diese Punkte zusammenfassend dargestellt.

7.2 Rechtliche Rahmenbedingungen

Die Ausführungen aus Kapitel 4.2 zusammenfassend, zeigt dieser Abschnitt die grundlegensten rechtlichen Rahmenbedingungen bzgl. des Cloud-Computing-Einsatzes für kleine und mittlere Unternehmen und Behörden.

- Die Verantwortung für Informationssicherheit liegt grundsätzlich bei der Unternehmensführung (siehe UGB und GmbH-Gesetz).
- Die Auslagerung von IT-Diensten an Cloud-Computing-Anbieter befreit die Unternehmensführung nicht von ihrer Verantwortung gegenüber deren Kunden (siehe ABGB und DSG).
- Beauftragte Cloud-Computing-Anbieter müssen auf sichere und rechtmäßige Datenverarbeitung überprüft werden; organisatorische und technische Schutzmaßnahmen müssen angemessen umgesetzt sein (siehe DSG).
- Genehmigungsfrei dürfen personenbezogene Daten nur innerhalb des EWR-Raums und nach Andorra, Argentinien, Australien, Kanada, Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, USA (Safe-Harbor-Abkommen und Flugpassagierdaten), Neuseeland und Uruguay übermittelt werden.
- Die Rückgabe oder Vernichtung der Daten bei Beendigung des Vertragsverhältnisses zwischen Cloud-Computing-Anbieter und Auftraggeber muss vertraglich geregelt sein (siehe §11 DSG).
- Potenzielle Verletzungen von Berufsgeheimnissen durch Berufsgeheimnisträger wie Ärzte oder Therapeuten sind in §121 Strafgesetzbuch geregelt. Eine Verlagerung von betroffenen Daten in die Cloud ist auch aufgrund der Sensibilität der Daten im Einzelfall genau zu prüfen.

7.3 Schutzbedarfskategorien

Zum einfacheren Bestimmung, welche Daten in der Cloud gespeichert und verarbeitet werden können, wurden auf Basis des österreichischen Datenschutzgesetzes (§6-§9 DSG) die in diesem Abschnitt beschriebenen Schutzbedarfskategorien entwickelt.

Sensible, d.h. besonders schutzwürdige Daten umfassen nach § 4 Z 2 DSG Daten natürlicher Personen über deren rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben; dies ist besonders relevant für Gesundheits- und Rechtssektor.

Personenbezogene Daten umfassen nach § 4 Z 1 DSG all jene Daten, welche ausreichen, um die Identität einer Person zu bestimmen; relevant für alle Branchen (z.B. im Sinne von Rechnungen, Angeboten, Schriftverkehr etc.).

Archivierungspflichte Daten im Sinne der BAO (z.B. Bücher, Rechnungen etc.); relevant für alle Branchen.

Sonstige schutzwürdige Daten im Kontext der Unternehmensaktivität; relevant für alle Branchen (Geschäftsgeheimnisse, Konstruktionspläne, Forschungs- und Entwicklungsergebnisse). Unterneh-

mensinterne Datenklassifikation bzgl. Vertraulichkeit, Verfügbarkeit und Integrität (z.B. hoch, mittel, niedrig). Die Klassifikation der einzelnen Datenarten kann nach folgendem Schema erfolgen:

- **Niedrig:** Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat keine oder kaum Auswirkungen auf das Unternehmen bzw. auf die Behörde.
    - Beispiele: öffentlich verfügbare Marketingmaterialien (Flyer, Produktbroschüren etc.)
- **Mittel:** Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat empfindliche finanzielle, rechtliche oder rufschädigende Wirkung auf das Unternehmen bzw. auf die Behörde.
    - Beispiele: personenbezogene Daten

- **Hoch:** Die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit hat existenzbedrohende finanzielle, rechtliche oder rufschädigende Wirkung auf das Unternehmen bzw. auf die Behörde.
    - Beispiele: Geschäftsgeheimnisse, sensible Kundendaten

Tabelle 9: Datenklassifikation und Schutzbedarf

Klassifikation/Schutzbedarf	Niedrig	Mittel	Hoch
sensible Daten im Sinne des DSG			
personenbezogene Daten im Sinne des DSG			
Daten mit bestimmte Archivierungspflichten (BAO)			
sonstige Daten – niedrige Vertraulichkeit			
sonstige Daten – mittlere Vertraulichkeit			
sonstige Daten – hohe Vertraulichkeit			
sonstige Daten – niedrige Verfügbarkeit			
sonstige Daten – mittlere Verfügbarkeit			
sonstige Daten – hohe Verfügbarkeit			
sonstige Daten – niedrige Integrität			
sonstige Daten – mittlere Integrität			
sonstige Daten – hohe Integrität			

7.4 Leitfäden zur sicheren Cloud-Nutzung

In diesem Abschnitt werden basierend auf zwei Fallbeispielen (Ein-Personen-Unternehmen und kleines Unternehmen mit zwei Standorten) typische Beispielszenarien inkl. der in Anspruch genommenen Dienste und Sicherheitsvorkehrungen beschrieben und Leifäden zur sicheren Cloud-Nutzung gegeben.

Ein-Personen-Unternehmen (EPU)

Das in diesem Szenario beschriebene EPU ist ein Handwerksbetrieb mit nur einem IT-Nutzer und Rechner. Der Rechner wird vom Geschäftsführer des Unternehmens für die Abwicklung der gesamten Geschäftstätigkeit (Rechnungen, Angebote, Berichte etc.) verwendet. Folgende Softwarepakete werden lokal verwendet:

- Textverarbeitung (Angebote, Berichte etc.)
- Tabellenkalkulation (Rechnungen, Planung etc.)
- E-Mail-Client (Kommunikation mit Kunden und Lieferanten, Terminkalender)
- branchenspezifische Software (CAD und Planungsprogramme)

Der Wechsel zu Cloud-Diensten wird aus Gründen der Kosteneffizienz (Lizenzen für Office-Software), Sicherheit (kein ausreichend gesichertes Backup) und Aktualität (nur veraltete Software-Versionen vorhanden) angestrebt. In jeder Kategorie soll einer der folgenden Cloud-Dienste verwendet werden (die gelisteten Produkte verstehen sich als Beispiele):

- Textverarbeitung und Tabellenkalkulation
    - Microsoft Office 365
    - Google Docs

- E-Mail-Kommunikation und Terminkalender
    - Google Mail
    - Contact Office

- Datenbackup
    - Dropbox for Business
    - Fabasoft Cloud

Kleines Unternehmen mit verteilten Standorten

Das in diesem Szenario beschriebene Unternehmen ist ein Produktionsbetrieb mit zwei geografisch getrennten Standorten. Der Betrieb beschäftigt 27 Mitarbeiter, wovon 7 Mitarbeiter die IT des Unternehmens für administrative und planerische Aufgaben nutzen. Folgende Softwarepakete werden lokal verwendet und sollen durch einen der gelisteten Cloud-Dienste ersetzt werden:

- Textverarbeitung (Angebote, Berichte, Planungsdokumente etc.)
    - Microsoft Office 365
    - Google Docs

- Tabellenkalkulation (Rechnungen, Planung, Zeiterfassung etc.)
  - Microsoft Office 365
  - Google Docs

- E-Mail-Client (Kommunikation mit Kunden und Lieferanten, Terminkalender)
  - Microsoft Exchange Online 2010
  - Google Mail

- CRM System
  - TecArt-CRM
  - Salesforce Sales Cloud

In beiden Szenarien planen die Unternehmen personenbezogene (nicht sensible) Daten in öffentlichen Clouds zu speichern und zu verarbeiten. Gemäß §10 Datenschutzgesetz dürfen die Unternehmen Dienstleister für die Verarbeitung der Daten in Anspruch nehmen, müssen sich aber von der rechtmäßigen und sicheren Datenverwendung (inkl. der tatsächlich getroffenen Schutzmaßnahmen) überzeugen. Gemäß §11 und §14 Datenschutzgesetz darf der Cloud-Service-Anbieter die Daten nur im Rahmen der Aufträge des Auftraggebers und unter Einhaltung angemessener Sicherheitsvorkehrungen verarbeiten. Nach Beendigung des Vertragsverhältnisses müssen die Daten an den Auftraggeber zurückgegeben und vernichtet werden.

Unabhängig von den nachfolgenden vertraglichen Bestimmungen sollten folgende technische Maßnahme zur Erhöhung der Datensicherheit seitens des Kunden getroffen werden:

- **Einsatz von Verschlüsselungssoftware**
  So weit wie möglich sollten die in der Cloud gespeicherten Daten verschlüsselt werden. Der Schlüssel darf dabei nur dem Kunden, nicht aber dem Cloud-Service-Anbieter oder Dritten bekannt sein. Während die Verschlüsselung in manchen Bereichen nur schwer zu bewerkstelligen ist (z.B. Textverarbeitung) kann Verschlüsselung im Bereich des Cloud-basierten Daten-Backups leicht umgesetzt werden. Mögliche Tools umfassen TrueCrypt zur reinen Verschlüsselung (truecrypt.org) oder TAVUU zur Verschlüsselung und verteilten Speicherung (tavuu.com).

- **Verteilte Speicherung der Daten**
  Besonders bei unternehmenskritischen Daten empfiehlt es sich, trotz Service Level Agreements nicht auf einen einzelnen Anbieter zu vertrauen, sondern die Daten bei mehreren Anbietern in unterschiedlichen geografischen, politischen und wirtschaftlichen Räumen zu hinterlegen. Somit ist sichergestellt, dass selbst bei Ausfall bzw. Sperre eines Anbieters die Unternehmensdaten zugänglich bleiben. Tools wie das vom Wiener Unternehmen Xylem Technologies entwickelte TAVUU ermöglichen die transparente, automatisierte, verteilte und ver-

schlüsselte Speicherung von Unternehmensdaten in der Cloud. Dabei arbeitet der Nutzer wie gewohnt am Rechner, während das Tool im Hintergrund die Daten verschlüsselt und zu vorher definierten Cloud-Service-Anbietern synchronisiert. Darüber hinaus besteht auch die Möglichkeit, die Daten verteilt zu speichern. D.h. selbst bei Verletzung der Vertraulichkeit des Schlüssels könnte kein Cloud-Service-Anbieter die Daten rekonstruieren, da diese von TA-VUU beim Upload-Prozess zerteilt und nur in Fragmenten zu den einzelnen Anbietern hochgeladen werden.

- **Sichere Speicherung der Passwörter**
  Jedes Cloud-Service erfordert Nutzernamen und Passwörter zur Verwendung der Dienste. Es empfiehlt sich, Passwortmanagementwerkzeuge wie KeyPass zu verwenden, um die Zugangsdaten in verschlüsselter Weise auf dem lokalen Rechner zu speichern und so vor Ausspähangriffen zu schützen.

Neben den technischen Maßnahmen sollten folgende Fragen[98] vor Abschluss eines Cloud-Service-Vertrags geklärt werden, sofern personenbezogene Daten in der Cloud verarbeitet oder gespeichert werden sollen. Meistens finden sich Teile der Antworten in den AGB und Einzelvertragsbestimmungen der Anbieter. Sollte die eine oder andere Frage nicht beantwortbar sein, sollte der Anbieter kontaktiert und die dementsprechende Bestimmung vertraglich geregelt werden.

Vertragsgestaltung

Frage	**Erfüllt?**
1. Besteht die Möglichkeit des Abschlusses eines schriftlichen Vertrages oder kann dieser nur online abgeschlossen werden?	☐
2. Bestehen für Subauftragnehmer dieselben Verpflichtungen wie für den Auftragnehmer? Ist dieser Umstand vertraglich geregelt?	☐
3. Wird der Kunde über Einsatz bzw. Wechsel von Subauftragnehmern informiert und ist dessen Zustimmung erforderlich (§10 DSG)?	☐
4. Sind Regelungen vorgesehen, welche im Falle einer Insolvenz des Auftragnehmers die Daten des Kunden schützen und die Verfügbarkeit seiner Anwendungen sicherstellen?	☐
5. Besteht im Falle einer Insolvenz das Recht auf Herausgabe der jüngsten Datensicherungskopien an den Kunden?	☐
6. Wie wird bei Speicherung aufbewahrungspflichtiger Daten (z.B. Rechnungen,	☐

[98] Die Fragen wurden aus Quellen der österreichischen Wirtschaftskammer, dem deutschen BSI und EuroCloud sowie eigenen Ergänzungen zusammengestellt.

Bücher im Kontext von BAO, UGB) die Einhaltung der Aufbewahrungsfristen (z.B. sieben Jahre) gewährleistet?	
7. Existieren Regelungen für Rückgabe und Löschung der Daten nach Vertragsende (§11 DSG)?	☐
8. Ist im Fall von Streitigkeiten zur Leistungserbringung oder bei Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?	☐
9. Werden Änderungen des technischen und organisatorischen Schutzmaßnahmenkonzepts an den Kunden kommuniziert und muss dieser zustimmen?	☐
10. Besteht für den Kunden oder für einen von ihm beauftragten Dritten ein Kontrollrecht hinsichtlich der Umsetzung der vereinbarten technischen und organisatorischen Schutzmaßnahmen?	☐
11. Sind Sicherheitsleistungen im Vertrag definiert und durch Sicherheits-SLA oder SLA weiter spezifiziert?	☐

Datenschutz

Frage	**Erfüllt?**
1. Existiert ein definierter Datenschutzbeauftragter als Ansprechpartner für den Kunden?	☐
2. Existieren Regeln für die Benachrichtigung, Auskunft und Löschung von personenbezogenen Daten auf Anfrage von Betroffenen?	☐
3. Wo werden die Daten gespeichert und verarbeitet? • ausschließlich in Österreich • ausschließlich im EU-/EWR-Raum • ausschließlich in Staaten mit angemessenen Datenschutzniveau lt. Definition der EU-Kommission (Schweiz, Australien etc.) • international	☐
4. Werden die Daten außerhalb des EU-/EWR-Raums verarbeitet und gespeichert? • Wenn ja, ist ein angemessenes Datenschutzniveau sichergestellt (Safe–Harbor-Abkommen etc.)? • Besteht die Möglichkeit, die Datenhaltung auf Österreich oder den EU-/EWR-Raum einzugrenzen?	☐
5. Sind die Verantwortlichkeiten des Auftragnehmers hinsichtlich der Umsetzung von Weisungen und technischen Schutzmaßnahmen gemäß DSG exakt definiert?	☐

6. Sind der Umfang, die Art und der Zweck der Verarbeitung und Speicherung von Daten und der Kreis der Betroffenen definiert?	☐
7. Wie lange und wo werden Daten, welche sich auf die eigentlichen Nutzerdaten beziehen (Verkehrs- und Metadaten) gehalten?	☐
8. Sind jene Fälle, welche den Schutz personenbezogener Daten verletzen, exakt definiert, sodass der Kunde Betroffene gemäß DSG benachrichtigen kann?	☐
9. Sind technische und organisatorische Schutzmaßnahmen gemäß §14 DSG ausreichend dokumentiert und dem Kunden zugänglich?	☐
10. Wie wird der Kunde im Falle eines Datenverlustes oder einer Verletzung der Datenvertraulichkeit informiert?	☐

Sicherheitsmaßnahmen

Frage	**Erfüllt?**
1. Sind alle wichtigen Versorgungskomponenten (Strom, Klimatisierung des Rechenzentrums, Verkabelung etc.) redundant ausgelegt?	☐
2. Werden Zutritte zum Rechenzentrum durch Zutrittskontrollsysteme, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal und Alarmsysteme angemessen überwacht und geregelt?	☐
3. Wird der Zutritt zum Rechenzentrum durch Zwei-Faktor-Authentifizierung geregelt?	☐
4. Sind Maßnahmen zur Brandbekämpfung und -vermeidung angemessen umgesetzt (Brandmeldeanlagen, Branderkennung, Löschanlagen, Brandschutzübungen etc.)?	☐
5. Ist die bauliche Infrastruktur robust genug ausgeführt, um Elementarschäden und Eindringversuchen entgegenzuwirken?	☐
6. Sind die Rechenzentren redundant ausgelegt und so weit voneinander entfernt, dass Schadenereignisse nicht beide Rechenzentren gleichzeitig treffen können, um den Betrieb im Falle des Ausfalls eines Rechenzentrums aufrechterhalten zu können?	☐
7. Sind technische Maßnahmen zum Schutz der Server angemessen implementiert (Firewalls, regelmäßige Integritätsüberprüfungen, host-based intrusion detection systems etc.)?	☐
8. Besitzen die Server eine sichere Grundkonfiguration (Deaktivierung unnötiger Dienste, gehärtete Betriebssysteme etc.)?	☐
9. Sind Sicherheitsmaßnahmen gegen Malware angemessen implementiert (Vi-	☐

renschutz, Firewall etc.)?	
10. Sind Sicherheitsmaßnahmen gegen netzbasierte Angriffe angemessen implementiert (IPS/IDS-Systeme, Firewalls, Gateways etc.)?	☐
11. Sind Maßnahmen zur DDoS-Angriffsabwehr implementiert?	☐
12. Existiert eine geeignete Netzsegmentierung (Managementnetz vs. Datennetz)?	☐
13. Sind alle Komponenten der Cloud-Architektur sicher konfiguriert?	☐
14. Ist sichergestellt, dass die Fernadministration nur über einen sicheren Kommunikationskanal (SSH, IPSec, VPN etc.) erfolgen kann?	☐
15. Erfolgt die Verschlüsselung zwischen den Cloud-Standorten mit ausreichend sicherer Verschlüsselung?	☐
16. Erfolgt die Verschlüsselung mit Subauftragnehmern mit ausreichend sicherer Verschlüsselung?	☐
17. Wie wird der Zugriffsschutz auf die gespeicherten Daten insbesondere in Hinsicht auf internes Personal gewährleistet?	☐

Anwendungssicherheit

Frage	**Erfüllt?**
1. Ist Sicherheit Bestandteil des Software Development Life Cycle Prozesses (Reviews, automatisierte Tests, Vulnerability Tests etc.)	☐
2. Werden Sicherheits-Mindeststandards der zu Verfügung gestellten Web-Anwendungen eingehalten (z.B. OWASP)?	☐
3. Existiert ein definiertes Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service-Packs)?	☐
4. Werden Patches vor dem Einspielen auf Produktivsystemen in Testumgebungen getestet?	☐

Datensicherheit

Frage	**Erfüllt?**
1. Werden Kundendaten durch Maßnahmen wie zum Beispiel virtuelle Speicherbereiche sicher voneinander isoliert?	☐
2. Werden regelmäßige Datensicherungen durchgeführt und sind deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte, Speicherdauer)	☐

für den Kunden nachvollziehbar?	
3. Ist die technische Umsetzung der Löschung von Daten genau definiert und ihre tatsächliche nachweisliche Lösung gewährleistet (welche Policy, Löschverfahren, Umgang mit Backup-Medien, Wiederverwendung der Datenträger)?	☐

Verschlüsselung und Schlüsselmanagement

Frage	**Erfüllt?**
1. Werden alle Daten des Kunden verschlüsselt gespeichert?	☐
2. Werden Best Practices der Schlüsselverwaltung umgesetzt?	☐

Identifikations- und Rechtemanagement

Frage	**Erfüllt?**
1. Ist eine Zwei-Faktor-Authentifizierung für Administratoren des Cloud-Service-Anbieters umgesetzt?	☐
2. Existiert eine rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte?	☐
3. Wird das „least privilege"-Modell umgesetzt (nur unbedingt erforderliche Rechte zur Durchführung der definierten Tätigkeiten werden gewährt)?	☐

Monitoring und Security Incident Management

Frage	**Erfüllt?**
1. Existiert eine 24/7-Überwachung der Cloud-Dienste und sind zeitnahe Reaktionen bei Angriffen und Sicherheitsvorfällen gewährleistet?	☐
2. Ist sichergestellt, dass relevante Datenquellen erfasst und ausgewertet werden können (Systemstatus, fehlgeschlagene Anmeldeversuche etc.)?	☐
3. Können relevante Logdaten in geeigneter Form durch den Auftragnehmer zur Verfügung gestellt werden?	☐
4. Werden die Aktivitäten von Administratoren aufgezeichnet und überwacht?	☐

Notfallmanagement

Frage	Erfüllt?
1. Welche Notfallmaßnahmen sind im Falle eines Dienstausfalles vorgesehen?	☐

Portabilität und Interoperabilität

Frage	Erfüllt?
1. Werden Daten bei Vertragsbeendigung in einem vereinbarten Format unter Beibehaltung der logischen Relation zur Verfügung gestellt?	☐
2. Existieren standardisierte oder offen gelegte Schnittstellen zum Auftragnehmer?	☐

Sicherheitsprüfung und -nachweis

Frage	Erfüllt?
1. Wie wird die Einhaltung der Datenschutzbestimmungen nachgewiesen?	☐
2. Werden unabhängige Zertifizierungen oder Audits beim Auftragnehmer hinsichtlich Datenschutz und Datensicherheit durchgeführt (SAS70, Trust Services, ISO27001)? Welche Bereiche werden zertifiziert?	☐
3. Werden regelmäßige Penetrationstests durchgeführt?	☐
4. Werden regelmäßige Penetrationstests bei Subauftragnehmern durchgeführt?	☐

Personalanforderungen

Frage	Erfüllt?
1. Wird Personal nur nach positiver Überprüfung deren Hintergrunds eingestellt?	☐
2. Wurden relevante Mitarbeiter des Auftragnehmers zur Einhaltung des Datengeheimnisses nach § 15 DSG verpflichtet?	☐
3. Wird relevantes Personal regelmäßig geschult?	☐
4. Wird das Personal hinsichtlich Informationssicherheit und Datenschutz sensibilisiert?	☐
5. Verpflichten sich die Mitarbeiter der Informationssicherheit, dem Datenschutz und dem angemessenen Umgang mit Kundendaten?	☐

7.5 Entwicklung eines Cloud-Sicherheitsmodells

Das in diesem Abschnitt beschriebene Cloud-Sicherheitsmodell wurde aus der Sicht von KMU und kleinen/mittleren Behörden als Service-Konsumenten entwickelt und soll bei der sicheren Integration von Cloud-Services in die Organisation unterstützen.[99]

Sicherheitsmanagement spielt im Bereich Cloud-Computing eine wichtige Rolle; bereits bei der Anbieterauswahl soll darauf geachtet werden, dass die eigenen Anforderungen, die im Sicherheitskonzept definiert werden, durch den Anbieter erfüllt sind oder ob gegebenenfalls das Konzept angepasst werden muss. Diesbezüglich ist speziell die Risikoanalyse erneut zu betrachten und die Cloud-spezifischen Änderungen umzusetzen.

Besteht in dem Unternehmen noch keine Risikoanalyse, so ist empfehlenswert, diese nach einem bestehenden Leitfaden (z.B. nach dem Risiko-Assessmentprozess der ENISA) vorzunehmen. Dies hat den Vorteil, dass in diesem Dokument bereits Risiken, Schwachstellen, Unternehmenswerte und Empfehlungen bezüglich Cloud-Sicherheit berücksichtigt wurden. Die Risikoanalyse der klassischen (in-house) Lösung ist der Risikoanalyse der Cloud-Lösung gegenüberzustellen und zu bewerten.

Im Zuge der Vorbereitungsarbeit sind eine Datenanalyse und eine Analyse der bestehenden Systeme durchzuführen. Es gilt es zu hinterfragen, welche Daten in welcher Anwendung verarbeitet werden. Darüber hinaus ist die Frage zu klären, ob eine besondere Schutzbedürftigkeit der Daten oder Anwendungen gegeben und zu berücksichtigen ist.

Vor der Entscheidung für einen Anbieter sind vorab Anforderungen zu definieren, die später als Auswahlkriterien dienen. Weiters ist eine Wirtschaftlichkeitsbeurteilung des Projektes durchzuführen und Anforderungen an die Cloud und die Sicherheit zu definieren. Für die Wirtschaftlichkeitsbeurteilung ist es notwendig, die internen Kosten zu ermitteln, um diese mit den Kosten der Cloud-Lösung vergleichen zu können. Es gilt sicherzustellen, dass der Übergang aus zeitlicher und organisatorischer Sicht geordnet und nachhaltig vonstattengehen kann.

7.5.1 Phase 1: Cloud-Sourcing-Strategie

Die erste Phase dient zur Festlegung der Cloud-Sourcing-Strategie, die im Rahmen eines IT-Servicemanagements Teil der Service-Strategie ist. Für bestehende IT-Prozesse können, wenn bereits ein Sicherheitskonzept vorliegt, die Business Impacts sowie die Anforderungen an die Sicherheitsmaßnahmen aus den bestehenden Dokumenten abgeleitet werden. Weiters können aus einem bestehenden Konzept auch Anhaltspunkte für den Vergleich der bestehenden Lösung mit einer möglichen Cloud-Lösung entwickelt werden. Sind die IT-Prozesse noch nicht definiert, so können bis dahin bekannte Fakten (z.B. aus Compliance-Anforderungen und Business Impacts) Anhaltspunkte für die strategische Bewertung und Festlegungen in Bezug auf Informations- und IT-Sicherheit als grobes

[99] Dieser Abschnitt basiert auf Vorarbeiten, welche von Sonja Haslinger an der Universität Wien durchgeführt wurden.

Sicherheitskonzept darstellen. Folgende Fragen sollten in dieser Phase beantwortet werden und in die Strategie einfließen[100] [95]:

- Sind Servicestrategie, Architekturplanung und die Sourcing-Strategien mit Cloud-Services vereinbar?
- Für welche Geschäftsprozesse soll Cloud-Computing eingesetzt werden und welche Ziele werden mit diesen Geschäftsprozessen hauptsächlich verfolgt?
- Welche Anforderungen bestehen für die in Frage kommenden Geschäftsprozesse im Hinblick auf Governance, Compliance, Leistung sowie Sicherheit?
- Welche Service-Modelle und Cloud-Arten kommen für die Services in Frage, und wie sehen die Anforderungen an die Cloud-charakteristischen Merkmale aus?
- Welche Daten und Informationen dürfen NICHT in Cloud-Systemen gespeichert werden?
- Welche Vorteile werden durch das Cloud-Sourcing erwartet?
- Welche Nachteile können akzeptiert werden, welche Nachteile schließen den Umstieg aus?
- Besteht für die relevanten Prozesse ein Sicherheitskonzept mit den wichtigsten Sicherheitsanforderungen und Business Impacts?

Es wird empfohlen die Cloud-spezifischen Gefährdungen zu analysieren und passende Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Es soll eine Risikoanalyse sowie eine Schutzbedarfsanalyse durchgeführt und es müssen Schutzniveaus für die jeweiligen Daten bzw. Anwendungen festgelegt werden. Die Schutzbedarfsniveaus und daraus resultierenden Schutzbedarfskategorien bilden die Basis für die Angebots- und Vertragsphase. Weiters sind Schnittstellen von IT-Systemen, Datenbeständen und Anwendungen zu identifizieren. In der Cloud-Sourcing-Strategie ist ebenso abzuklären, ob die Daten bereits auf Seiten des Unternehmens verschlüsselt werden sollen.

Der Einsatz von Cloud-Services kann sich auch auf die Unternehmensstrategie sowie -struktur auswirken, es kann zu einer Umverteilung von Rollen, Verantwortungen und zu Veränderungen in den Prozessen kommen, dies muss in der Strategieentwicklungsphase mitbedacht werden. Auch ist bereits in der Planungsphase eine Exit-Strategie zu entwickeln und ein grober Zeit- und Ressourcenplan zu erstellen.

Für die Vorbereitung der Evaluierungs- und Auswahlphase müssen Schutzziele, Datenschutzrichtlinien sowie rechtliche Aspekte für die Themen Informationsschutz in der Verarbeitung, Speicherung und Übertragung von Informationen festgelegt werden.

Ergebnisse dieser Phase:

- Cloud-Sourcing-Strategie, abgestimmt auf Unternehmens- und IT-Strategie, welche die Aspekte der Sicherheit, IT Governance und Compliance berücksichtigt
- Gegenüberstellung der Ergebnisse der klassischen Risikoanalyse zu den Ergebnissen der Risikoanalyse Cloud
- Business-Impact-Analyse
- Sicherheitskonzept inklusive:

[100] Königs H.P., 2013, S. 388 (Königs Hans Peter, 2013, IT-Risikomanagement mit System Praxisorientiertes Management von Informationssicherheits- und IT-Risiken, 4. Auflage, Springer Vieweg, Springer Fachmedien Wiesbaden)

  - Schutzziele
  - Cloud-spezifische Risiken
  - Cloud-spezifische Gefährdungsanalyse
  - Schutzbedarfsniveaus und -kategorien
  - adäquate Sicherheitsmaßnahmen
- Zeit- und Ressourcengrobplanung
- Exitstrategie

7.5.2 Phase 2: Evaluierung und Auswahl

Auf Basis der Ergebnisse der Strategiephase wird zu Beginn der zweiten Phase ein Pflichtenheft erstellt, welches die Ziele und Anforderungen, die an das Service bzw. den Anbieter gestellt werden beinhaltet. Hier kann eine Einteilung in die Kategorien „Muss-Anforderungen“, „Wunsch-Anforderungen“ und „Nicht-Anforderungen“ vorgenommen werden. Weiters sollten funktionale, nicht-funktionale, technische sowie wirtschaftliche Anforderungen beinhaltet sein. Wird das Einhalten von Normen und Standards vorausgesetzt, so sind diese Anforderungen auch in das Pflichtenheft zu integrieren.

Die zweite Phase beinhaltet die Evaluation und die Auswahl von Cloud-Services bzw. -Anbietern. Es gibt ein breites Spektrum an verschiedenen Kunden-Lieferanten-Beziehungen und so ist auch die Möglichkeit und Verhandelbarkeit der verschiedenen Leistungsangebote bzw. Nutzungsbedingungen und Richtlinien unterschiedlich gestaltet. Standardisierte Angebote setzen oft die Akzeptanz einseitiger, nicht verhandelbarer Nutzungsbedingungen und Sicherheitsrichtlinien voraus, die bei Anmeldung automatisch akzeptiert werden müssen. Ein Beispiel dafür ist der Cloud-Dienst Dropbox. In den Nutzungsbedingungen werden Verantwortlichkeiten sowie Haftungsgründe seitens des Anbieters abgelehnt und darauf verwiesen, dass die Nutzung des Services durch den Anbieter jederzeit eingestellt und das Service zeitweilig oder endgültig auch ohne Benachrichtigung beendet werden kann. In der Phase der Evaluierung müssen Angebote auf Kompatibilität mit den Strategie-Anforderungen geprüft werden, dafür eignen sich u.a. folgende Fragen[101]:

- Beinhaltet die Einladung zur Angebotslegung (RFP – Request for Proposal) die wichtigsten, aus dem IT-Sicherheitskonzept resultierenden, Sicherheitsanforderungen und Business Impacts?
- Gehen aus dem IT-Sicherheitskonzept nicht nur die Sicherheitsanforderungen des Kunden, sondern auch die des Endbenutzers hervor, z.B. geheime Personendaten?
- Sind die Anforderungen aus Sicht der Geschäftsprozesse in klaren, unmissverständlichen SLAs formuliert und quantifiziert?
- Sind die Anforderungen an das Change Management, Service Asset Management und Configuration Management abgedeckt?

101 Königs H.P., 2013, S. 390

- Entsprechen die angebotenen Serviceleistungen des Anbieters den Anforderungen der Ausschreibung?
- Hält der Anbieter eine Zertifizierung für das Informationssicherheits-Management seines Angebots?
- Bietet der Anbieter vertraglich festgelegte Zusagen?
- Ist ein Anbieter aus der Liste der möglichen Lieferanten zu streichen, da er vorab definierter Muss-Kriterien nicht erfüllen kann? (z.B. wichtige Compliance-Anforderungen zum Datenschutz)
- Kann die Anbieter-Auswahl mittels Nutzwert-Analyse getroffen werden?

Bei der Einholung von Angeboten können darüber hinaus auch folgende Fragen herangezogen werden, um die Sicherheitsmaßnahmen des Anbieters zu evaluieren. Weiters können sie als Basis dienen, um vom ausgewählten Anbieter in der folgenden Vertragsphase Sicherheit und dementsprechende Maßnahmen einzufordern. Dabei spielen die folgenden Themengebiete eine Rolle:

- **Standort des Anbieters, der Infrastruktur, der Daten:** In welchem Land hat der Cloud-Anbieter seinen Sitz, wo ist die Infrastruktur des Anbieters lokalisiert? Welche Maßnahmen hinsichtlich physischer Sicherheit werden an den Standorten geboten? Sind diese an Standards wie z.B. ISO27001 ausgerichtet? Wo werden die Daten physisch gespeichert? Bietet der Anbieter Informationen und volle Steuerung über den aktuellen physischen Standort der Daten?

- **Subunternehmen:** Wird ein Teil des Services an ein Subunternehmen überantwortet oder ausgelagert? Werden – und wenn ja, wie oft – Outsourcing- bzw. Subunternehmen einem Audit unterzogen? Wie wird sichergestellt und garantiert, dass Service Levels durch Dritt-Dienstleister erfüllt und eingehalten werden? Sind die Sicherheitspolicies und -steuerung vertraglich zwischen Anbieter und Drittanbietern vereinbart? Besteht eine Definition der ausgelagerten Services, vor allem jener, die essenziell für die Sicherheit und Erreichbarkeit der Betriebsabläufe sind?

- **Datentransport, Speicherung und Löschung:** Wie werden die Daten des Kunden und der Kunden des Kunden gesammelt, verarbeitet und transportiert? Wie werden Daten von Speichern (Storage und Memory) gelöscht und Datenspuren bereinigt, bevor die Ressourcen neu zugeordnet werden? (Im Falle, dass physische Ressourcen nicht mit anderen Kunden geteilt werden.) Was passiert mit Daten nach Vertragsende? Bestehen Prozesse, um Daten – falls notwendig – von alte Medien oder Systeme zu löschen? Werden die Daten überschrieben oder physisch zerstört?

- **Ressourcenmanagement, Separierung und Skalierung:** Wie wird bei Ressourcenüberlastung informiert? Wie viel Einfluss hat der Kunde auf die Skalierung (Vergrößerung) der Ressourcen? Bietet der Anbieter Garantien für den Bezug eines Maximums an Ressourcen innerhalb eines Mindestzeitraumes? Gibt es eine Garantie auf zusätzlich verfügbare Ressourcen in-

nerhalb eines Mindestzeitraumes? Welche Prozesse sind vorgesehen, um Skalierungstrends im Bereich des Ressourcenverbrauchs, z.B. aufgrund von saisonalen Effekten, zu behandeln? Welche Garantien bietet der Anbieter, dass die Ressourcen des Kunden vollständig isoliert werden? Besteht eine genaue Beschreibung der Prozesse, die es Dritten ermöglichen, sicher auf die physische oder logische Infrastruktur zugreifen?

- **Standards und Normen:** Ist der Anbieter ISO 27001/2 zertifiziert? Sind die vom Anbieter verwendeten Produkte nach Common Criteria zertifiziert? Besteht ein kontinuierlicher Evaluierungsprozess?

- **Service Management und Organisation:** Bestehen detaillierte und festgelegte Change-Prozesse und -Policies, inklusive Re-Assessment der Risiken nach Änderungen? Bestehen Policies und Prozesse für Backups, Prozesse für das Management von Wechseldatenträgern und das sichere Zerstören von nicht länger benötigten Datenträgern etc.?

- **Change Management und Configuration Management:** Wie werden neue Releases auf Einsatzfähigkeit und Risikos geprüft? Welche Prozesse werden angewandt, um Anwendungen abzusichern? Werden bei einem Software-Release Penetration-Tests durchgeführt, um sicherzustellen, dass die Software keine Schwachstellen enthält? Wie sehen Prozesse aus, um gefundene Schwachstellen zu beheben? Besteht eine Darstellung der Patch-Management-Prozesse? Kann sichergestellt werden, dass die Patch-Management-Prozesse alle Schichten der Cloud-Liefertechnologie berücksichtigen (z.B. Netzwerk, Server-Betriebssysteme, Virtualisierungssoftware, Anwendungen und Sicherheitssysteme)?

- **Netzwerk und Sicherheit:** Wie erfolgt die Steuerung der Netzwerk-Architektur, besteht eine Überwachung um DDoS-Angriffe zu erkennen und abzuwehren, eine Definition der Isolationslevel und setzt der Anbieter eine virtuelle Netzwerkinfrastruktur ein? Stellt der Anbieter sicher, dass das virtuelle Image standardmäßig gehärtet ist? Sind diese vor unautorisiertem Zugriff geschützt?

- **SaaS – Applikationssicherheit:** Wie sieht die Administrationssteuerung aus? Ist ein Rechtemanagement von anderen Benutzern durch die Steuerung möglich? Ist die Zugriffskontrolle fein graduiert, kann eine Anpassung an die Organisations-Policies vorgenommen werden?

- **Authentifizierung:** Unterstützt oder ordnet der Anbieter technische, Token-basierte, Zwei-Faktor-Authentifikationen für den Client-Zugriff an?

- **Autorisierung:** Gibt es Accounts mit systemweiten Rechten, und wenn ja für welche Operationen (lesen/schreiben/löschen)? Wie werden die Accounts mit den höchsten Berechtigungsstufen abgesichert und verwaltet? Wie werden die kritischsten Entscheidungen autorisiert? Werden verschiedene Rollen mit hohen Berechtigungen von einer Person gehalten? Werden rollenbasierte Zugriffsberechtigungen verteilt, wird das „least privilege“-Modell angewandt?

- **Identitätsbereitstellung:** Welche Prüfungen werden bei einer Registrierung eines Benutzer-Accounts vorgenommen (Identitätsprüfung; Standards?) Gibt es verschiedene Stufen von Identitätsprüfungen? Welche Prozesse bestehen für De-Provisionierungen? Erfolgen (De)-Provisionierungen innerhalb des Cloud-Systems zeitgleich oder aufgrund von geografisch weitverteilten Standorte zeitversetzt?
- **Personenbezogene Daten:** Wie sehen Policies und Prozesse im HR-Management aus, werden z.B. Zuverlässigkeitsprüfung, Beschäftigungsbiographie, Leumund der Angestellten von Mitarbeitern gefordert? Welche Sicherheitsausbildung wird dem Personal geboten? Wie wird die Steuerung der Datenspeicherung und Sicherheit des Benutzerverzeichnisses und des Zugriffs auf das Verzeichnis geregelt? Ist das Benutzerverzeichnis in einem standardisierten Format exportierbar? Wird seitens des Anbieters das Need-to-know-Prinzip auf den Zugriff auf Kundendaten angewandt?

- **Verschlüsselung – Schlüsselmanagement:** Bestehen Sicherheitsregelungen für das Lesen und Schreiben der Schlüssel, z.B. Passwort-Policies, Speicherung der Schlüssel in einem separaten System, Hardware-Security-Module für Root-Zertifikat-Schlüssel, Authentifizierung durch Smartcards etc.? Gibt es Sicherheitsregeln für die Verwendung der Schlüssel zur Signierung und zur Datenverschlüsselung? Ist die Sperrung des Schlüssels simultan für verschiedene Standorte möglich? Werden Images des Kundensystems geschützt oder verschlüsselt? Wo wird Verschlüsselung angewandt (für Datentransport, Daten während der Speicherung, Daten bei der Verarbeitung oder im Speicher)? Werden Usernamen und Passwörter verschlüsselt? Wird in einer Policy geregelt, was verschlüsselt werden soll und was nicht? Wer verwaltet die Zugriffsschlüssel, wie werden diese geschützt?

- **Identitätsmanagement – Authentifizierung:** Welche Formen der Authentifizierung werden für Operationen mit hohem Sicherheitsbedarf verwendet? Wird eine Zwei-Faktor-Authentifizierung verwendet, um kritische Komponenten innerhalb der Infrastruktur zu verwalten?

- **Diebstahl oder Kompromittierung der Berechtigungsdaten:** Werden Systeme zur Erkennung von Anomalitäten angewandt? Welche Vorkehrungen bestehen, wenn es zu einem Diebstahl der Berechtigungsdaten des Kunden kommt?

- **Identitätsmanagementframeworks:** Ist das Identitätsmanagement des Cloud-Anbieters interoperabel mit Drittanbietern im Bereich Identitätsmanagement? Gibt es eine Möglichkeit, um Single-Sign-On zu integrieren?

- **Zugriffssteuerung:** Ermöglicht das Client-Berechtigungssystem eine Separierung von Rollen und Verantwortlichkeiten für verschiedene Bereiche? Wie wird der Zugriff zu Kundensystemimages verwaltet und sichergestellt, dass Authentifizierungs- und kryptografische Schlüssel nicht darin enthalten sind?

- **Daten und Service-Portabilität:** Bestehen dokumentierte Prozesse und APIs, um Daten aus der Cloud zu exportieren? Bietet der Anbieter interoperable Exportformate für alle in der Cloud gespeicherten Daten an?

- **Incident Management und -Response:** Besteht seitens des Anbieters ein formaler Prozess, um Incidents zu erkennen, identifizieren, analysieren und darauf zu reagieren? Ist dieser Prozess erprobt und wird die Effektivität der Incident-Handling-Prozesse getestet? Sind sich die handelnden Personen ihrer Rollen während des Prozesses bewusst? Wie sind die Erkennungsmöglichkeiten strukturiert (Meldung von Anomalitäten durch Kunden, Echtzeit-Sicherheitsmonitoring)? Werden periodische Reports über Sicherheitsvorfälle erstellt? Wie erfolgt die Aufbewahrung und der Zugriff auf Sicherheitslogs? Wie sind die Eskalationsprozesse definiert? Wie sieht die Incident- und Beweisdokumentation aus? Wie oft testet der Anbieter die Disaster-Recovery- und Business-Continuity-Pläne?

- **Business Continuity Management:** Dokumentiert der Anbieter den Einfluss einer Unterbrechung detailliert, z.B. Recovery Point Objective und Recovery Time Objective für Services? Sind die Sicherheitsaktivitäten im Wiederherstellungsprozess passend adressiert? Bestehen für den Unterbrechungsfall definierte Kommunikationswege zum Endkunden? Sind Rollen und Verantwortungen im Unterbrechungsfall klar identifiziert und definiert? Bestehen seitens des Anbieters Recovery-Prioritätsklassen und decken sich diese mit den Prioritäten des Kunden? Welche relevanten Abhängigkeiten bestehen im Wiederherstellungsprozess?

- **Service Level Management:** Misst der Anbieter die Zufriedenheit bzw. die Erreichung der SLAs? Führt der Anbieter Help-Desk-Tests durch, z.B. Social Engineering Tests? Führt der Anbieter Penetration Tests durch? Wenn ja, wie oft? Was wird getestet? Führt der Anbieter Vulnerability-Tests durch? Wenn ja, wie oft? Wie sieht der Prozess zur Schwachstellen-Verbesserung aus (Hot Fixes, Re-Konfiguration etc.)?

- **Sonstige Fragen bezüglich der Sicherheit des Datencenters:** Wer – neben dem autorisierten IT-Personal – hat unbeaufsichtigten Zutritt zu IT-Infrastruktur, z.B. Reinigungspersonal, Manager, Verkäufer etc.? Wie oft werden die Zutrittsrechte überprüft, wie schnell können Rechte widerrufen werden? Wird Personal mit Zutritt zu den Sicherheitsbereichen überwacht? Wie sehen die Policies und Prozesse für das Montieren, Demontieren und Installieren von neuem Equipment aus? Werden regelmäßige Untersuchungen durchgeführt, um nicht autorisiertes Equipment zu entdecken? Verwendet das Personal, das Zutritt zum Datencenter hat, mobile Geräte wie z.B. Laptops oder Smartphones? Wenn ja, wie wird dies geschützt? Welche Maßnahmen werden getroffen, um Zutrittskarten zu überprüfen? Wie sehen die Genehmigungsprozesse aus, wenn Ausrüstungen von einem Standort zu einem anderen Standort transportiert werden soll? Wie oft werden Inventuren durchgeführt, um eine unautorisierte Entfernungen von Equipment zu überwachen? Wie oft werden Überprüfungen durchgeführt, um festzustellen, dass die Umgebung mit den notwendigen rechtlichen und regulatorischen Anforderungen

konform ist? Welche Prozesse oder Policies sind definiert, um sicherzustellen, dass Umgebungseinflüsse keine Serviceunterbrechung hervorrufen können? Welche Methoden werden verwendet, um Schaden aufgrund von Umwelteinflüssen zu verhindern?

Datenschutzrelevante Themen, die nach dem österreichischen Informationshandbuch in ein Auswahlverfahren miteinfließen sollen sind: Datenzugriff, die Gewährleistung der rechtlichen Vorgaben zur Einsichtnahme und Löschung personenbezogener Daten, der Speicherort der Daten, der Verbleib von Daten hinsichtlich der Frage, welche Daten wie lange gespeichert werden (z.B. Verkehrs- oder Metadaten), die Vernichtung von Daten, Datenschutzbestimmungen in Abstimmung mit der Compliance des Unternehmens, Audit und Monitoring sowie der Umgang mit Datenschutzverletzungen. Für österreichische Organisationen stellt sich die Frage, ob die rechtlichen Vorgaben des DSG 2000 eingehalten werden können. Diese Frage ist bereits in der Strategieentwicklung abzuklären.

Die Anbieter-Entscheidung sollte auf den Ergebnissen der Risikoanalyse, der Einflussidentifizierung und einem Kosten/Nutzen-Vergleich basieren, die auch die Kosten der Migration mitberücksichtigen.

Ergebnisse dieser Phase:

- **Pflichtenheft**
  - Muss-Anforderungen
  - Wunsch-Anforderungen
  - Nicht-Anforderungen

- **Funktionale Anforderungen**
  - nichtfunktionale Anforderungen
  - technische Anforderungen
  - wirtschaftliche Anforderungen
  - Standards und Normen

- **Basis für Nutzwert-Analyse inkl. Gewichtung nach Anforderungen aus dem Pflichtenheft; Relevante Themenbereiche:**
  - Niederlassung des Anbieters, Standort der Infrastruktur und der Daten sowie Datentransport
  - Subunternehmen
  - Ressourcen-Separierung
  - Authentifizierung
  - Standards, Normen und Zertifizierungen
  - Service Management und Organisation
  - Patch- und Change-Management, Configuration Management
  - Rechenzentrum, Netzwerk und Sicherheit
  - SaaS – Applikationssicherheit
  - Authentifizierung, Autorisierung und Identitätsbereitstellung
  - Verschlüsselung

  - Identitäts- und Berechtigungsmanagement
  - personenbezogene Daten
  - Daten und Service Portabilität
  - Incident Management und Response
  - Service Level Management, inkl. Wiederanlaufklassen
  - Sicherheitsmaßnahmen im Standardumfang
  - Sicherheitsarchitektur, Kryptokonzept, Datensicherungskonzept
  - Monitoring und Reporting
  - Notfallmanagement, Notfallhandbuch und Notfallkonzept
  - regelmäßige Überprüfung bestehender Maßnahmen, Reviews
  - Datenschutz

- **Einladung zur Angebotslegung (RFP – Request for Proposal)**

- **Angebote der Anbieter**

- **Reihung der Anbieter nach Nutzwertanalyse**

Die Reihung der Anbieter erfolgt nach der Gewichtung der Anforderungen und der durchgeführten Nutzwertanalyse. Der Anbieter, der auf der Liste an erster Stelle gereiht ist, wird in der folgenden Phase zu Vertragsverhandlungen eingeladen.

7.5.3 Phase 3: Vertragsentwicklung

In der dritten Phase[102], während der Vertragsentwicklung, sind mit dem ausgewählten Anbieter möglichst viele Prozesse abzustimmen und zu definieren. Dies sollte möglichst in Anlehnung an einen Standard für Servicemanagement z.B. ITIL oder ISO/IES2000 erfolgen. Ziel ist ein durchgängiges Servicemanagement. Die folgenden Prozesse sind abzustimmen, zu definieren und zu vereinbaren:

- Incident Management
- Change Management
- Availability Management
- IT Service Continuity Management
- Informations Security Management
- Service Desk

Aus diesen Vereinbarungen resultiert ein definiertes, für den zukünftigen Betrieb abgestimmtes, IT-Sicherheitskonzept. In dieser Phase der Vertragsgestaltung werden folgende Fragen miteinbezogen[103]:

- Sind die Anbieter- und kundenseitigen Servicemanagement-Prozesse und Sicherheits-Management-Prozesse definiert und aufeinander abgestimmt?

[102] Königs H.P., 2013, S. 391f
[103] Königs H.P., 2013, S. 391f

- Sind Protokolle und Interfaces, die eingehalten werden müssen, bestimmt?
- Besteht eine Vereinbarung bzw. ein Konzept für zusätzlich notwendige Systemkomponenten und -funktionen?
- Sind die Leistungen und Leistungsniveaus z.B. in SLAs entsprechend der Erwartungen vereinbart und quantifiziert?
- Ist ein Kosten- und Zeitplan festgehalten und abgestimmt?
- Sind die aus dem IT-Sicherheitskonzept resultierenden Anforderungen mit den gegenseitigen Pflichten abgestimmt und vereinbart?
- Werden zukünftige Anforderungen, neue Risiken sowie der kontinuierliche Verbesserungsprozess auf beiden Seiten berücksichtigt?

Wird diese Phase abgeschlossen, so resultiert daraus der Vertrag, auf dem das nachfolgende Cloud-Sourcing-Management aufbaut. In der Vertragsphase sollten auch die Inhalte der Service Level Agreements definiert werden. Diese sollten folgende Themenbereiche so detailliert wie nötig und möglich umfassen, um in der Betriebsphase auch als Steuerungs- und Controlling-Instrument dienen zu können:

- Kerninhalte und zentrale Vereinbarungen des Vertrags
- Spezifizierung von Rollen und Verantwortlichkeiten
- Service Level Targets, Performance-Ziele
- Dokumentation der SLA
- Prozesse zur Berücksichtigung und Einarbeitung unvorhersehbarer zukünftiger Anforderungen bzw. Innovationen
- Prozesse zur Vorgangsweise von vorhersehbarer Ereignisse
- effiziente Feedback- und Vertragsanpassungsprozesse
- Kennzahlendefinition, KPIs, Schwellenwerte für Ausfallzeiten von geschäftskritischen Anwendungen
- Regelungen zu Strafen und Pönalen
- Ausstiegsklauseln und Modalitäten zur Vertragsbeendigung
- Dokumentation von Kommunikationsprozesse
- Eskalierungs- und Schlichtungsprozesse

Der Vertrag soll laut BSI alle Nutzungsbedingungen des Cloud-Services genau und unmissverständlich spezifizieren und regeln. Dies betrifft insbesondere die Leistungsbeschreibung, Dienstgütevereinbarungen, Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistung, Gestaltung der Sicherheitsmaßnahmen, Datenschutz und Regelungen zur Weitergabe von Informationen an Dritte. Die SLAs, Verträge und AGB-Bestimmungen des Anbieters sollten transparent und nachvollziehbar offengelegt werden. Weiters müssen die Muss-Ziele bzw. die definierten Anforderungen vertraglich abgedeckt sein. Dazu zählen der regionale Standort der Infrastruktur, der Datenspeicher bzw. der Standort der Dienste sowie die dortige rechtliche Situation. Weiters sollte die Rechts- und Besitzverhältnisse des Anbieters klar und nachvollziehbar sein. Der Umgang mit personenbezogenen Daten und die datenschutzrechtliche Verantwortung sollte vertraglich vereinbart werden. Zuständigkeiten müssen

ausreichend und umfassend geregelt werden, für relevante Bereiche müssen genügend Ausfallkapazitäten vereinbart sein und vorliegen. Wiederanlaufklassen sind in den SLAs zu vereinbaren.

Ergebnisse dieser Phase:

- **vertragliche Vereinbarungen mit dem Anbieter**
- **Service Level Agreements**
- **abgestimmte Prozesse**

7.5.4 Phase 4: Projekt Migration

Die Migration der Anwendung, Daten bzw. die Durchführung für das Service notwendigen Änderungen werden in dieser vierten Phase in Form eines Projektes durchgeführt.

Dafür ist es notwendig, die Migration gemeinsam mit dem Cloud-Service-Anbieter und den betroffenen Abteilungen zu planen bzw. die Pläne aus der Strategiephase zu detaillieren. Es sind Prozesse, notwendige Vorbereitungs- und Umstellungsarbeiten festzulegen, ein Zeitplan für die Umsetzung der Auslagerung in die Cloud muss aufgesetzt werden. Während der Umstellung gilt es, die Übereinstimmung der technischen und fachlichen Anforderungen zu überprüfen. Weiters ist zu berücksichtigen, dass im Falle eines Scheiterns oder beim Auftreten von Komplikationen die Möglichkeit eines Rollbacks offen gehalten werden muss. Wichtig ist, dass die betroffenen Mitarbeiter miteinbezogen werden.

Bei der Implementierung soll darauf geachtet werden, dass das Thema Sicherheit ganzheitlich betrachtet und berücksichtigt wird. Erst nach erfolgreicher Testung des migrierten Umfanges kann dann der produktive Umstieg auf das neue System erfolgen. Im Zuge dieser Phase sind die Mitarbeiter, die zukünftig mit dem Cloud-System arbeiten, im Hinblick auf die Sicherheitsproblematiken in Cloud-Umgebungen zu schulen und zu sensibilisieren. Weiters sollte Wert auf eine umfassende Dokumentation gelegt werden.

Ergebnisse dieser Phase:

- **Ergebnisse der notwendigen Vorbereitungs- und Umstellungsarbeiten**
- **Testumgebung inkl. Tests**
- **Produktivsystem**
- **Dokumentation**

7.5.5 Phase 5: Cloud-Sourcing-Management

In der fünften Phase, der Phase des Cloud-Sourcing-Managements, können das Service- und Informationsmanagement ausgeführt werden. Dies betrifft die IT-Service-Organisation und kann sich auch auf den Aufbau, Betrieb und möglicherweise Ab- oder Umbau von IT-Prozessen auswirken. Diese Phase beinhaltet nach ITIL: „Operational Service Lifecycle“ und die Sub-Prozesse „Service Catalogue Management“, „Service Level Management“, „Availability Management“, „Capacity Management“, „Change Management“, „IT Service Continuity Management“, „Information Security Management“, „Access Management“ und „Incident Management“.

Ähnlich dem Outsourcing bedarf es auch beim Cloud-Sourcing einer Anlaufstelle auf beiden Seiten (Single Point of Contact). Der Kunde kann über die Anlaufstelle „Service Desk“ Störungen, Sicherheitsvorkommnisse, Wünsche und Fragen des Benutzers melden. Für den Service-Betrieb auf der Kundenseite bedarf es einer Etablierung der Prozesse „Event Management“, „Incident Management“, „Request Fulfilment“, „Problem Management“ und „Access Management“.

Im laufenden Betrieb sollte vor allem das Monitoring von Performance und auf Einhaltung von SLAs sowie etwaige Sicherheitsvorkommnisse betrieben werden. Hier ist darauf zu achten, dass die vereinbarten Reporting- und Logprozesse funktionieren. Für den Anwender sollte eine regelmäßig wiederkehrende Sensibilisierung hinsichtlich (Daten-)Sicherheits- und Datenschutzthematiken erfolgen. Weiters sollten, wenn vertraglich eingefordert, die Ergebnisse der regelmäßig (z.B. jährlich) durchzuführenden Audits bereitgestellt werden.

Ergebnisse dieser Phase:

- **Monitoring-Berichte**
- **Reporting- und Logs**
- **Audits**

8 SCHLUSSFOLGERUNGEN UND HANDLUNGSEMPFEHLUNGEN

Zusammenfassend kann festgehalten werden, dass der Trend zur Cloud-Migration in Unternehmen und Behörden ein unumkehrbarer ist und Sicherheitsaspekte neben potenziellen Kosteneinsparungen höchste Priorität haben. Die in diesem Kapitel dargestellten Schlussfolgerungen und Handlungsempfehlungen adressieren die Zielgruppen Konsumenten, Cloud-Service-Anbieter und Interessensvertreter der Konsumenten (beispielsweise die Wirtschaftskammer Österreich).

8.1 Handlungsempfehlungen für Konsumenten

Mit dem Begriff „Konsumenten“ werden im Kontext des Berichts EPU und KMU sowie kleine und mittlere Behörden zusammengefasst. Folgende Handlungsempfehlungen können für Konsumenten gegeben werden:

- **Prüfung der Wirtschaftlichkeit und Machbarkeit**
  - Welcher Nutzen wird beim Einsatz von Cloud-Service-Diensten erwartet (innerhalb und außerhalb der Organisation)?
  - Sind reelle Kosteneinsparungen zu erwarten, beispielsweise durch Reduktion von Kosten für bestehende IT-Lösungen und deren Wartung und Ausbau?
  - Kann durch den Einsatz von Cloud-Service-Diensten die Qualität der Dienste gesteigert werden? Zum Beispiel durch automatische Teilnahme an Softwareupdates oder durch gesteigerte Verfügbarkeit und Compliance?

- **Prüfung der Risiken**
  - Inwieweit lassen sich durch den Einsatz von Cloud-Service-Diensten Risiken wie Verfügbarkeitsausfälle und Datenverlust reduzieren?
  - Welche Risiken erhöhen sich? Beispielhaft können hier Lock-in-Effekte, Abhängigkeiten vom Cloud-Service-Anbieter, Kontrollverlust und datenschutzrechtliche Aspekte angeführt werden.
  - Die Verwendung personenbezogener und sensibler Daten innerhalb des Unternehmens muss geregelt sein. Organisatorische und technische Sicherheitmaßnahmen sind innerhalb des Unternehmens erforderlich. Während von der Auslagerung sensibler Daten in die Cloud vollständig abgesehen werden sollte, sollten personenbezogene Daten nur innerhalb der EU und nach Prüfung der Zuverlässigkeit des Anbieters dem Cloud-Service-Anbieter überlassen werden. Sollten sensible Daten dennoch in der Cloud gespeichert werden, so ist die ausdrückliche Zustimmung der Betroffenen erforderlich.

- **Prüfung der Kompatibilität mit der Unternehmensstruktur und -kultur**
  - Welche Prozesse sind überhaupt mit Cloud-Diensten bewältigbar? Zum Beispiel generische Prozesse im Kontext des Projektmanagements, der Personalverwaltung oder der Kommunikation?
  - Ist die Organisation auf Basis ihrer Historie, Verpflichtungen und Unternehmenskultur bereit, Daten an Dritte auszulagern und die Kontrolle zumindest teilweise abzugeben?

- **Prüfung der Verträge und damit verbundenen AGB**
  - Decken Verträge und damit verbundene AGB die rechtlichen und unternehmensinternen Anforderungen (z.B. Datenschutzgesetz) ab? Leitfäden für diese Prüfung wurden in Kapitel 7 bereitgestellt.
  - Sind Abläufe bzgl. Audits, Incident Management und Reporting vertraglich definiert?
  - Werden Details der Sicherheitsarchitektur und Verantwortlichkeiten für Datensicherheit definiert?
  - Ist es dem Konsumenten möglich und gestattet, sich selbst von der Umsetzung der Sicherheitsmaßnahmen zu überzeugen?
  - Sind die geografischen Standorte der Rechner und Speichersysteme vertraglich fixiert?

- **Prüfung von Zertifikaten**
  - Ist der Cloud-Service-Anbieter durch dritte vertrauenswürdige Stellen zertifiziert? Als ein Beispiel für eine solche Zertifizierungsstelle kann der TÜV Rheinland genannt werden.
  - Werden die Zertifikate in angemessenen Abständen erneuert bzw. passen sich diese an sich verändernde rechtliche Rahmenbedingungen an?

8.2 Handlungsempfehlungen für Anbieter

Cloud-Service-Anbieter können durch Transparenz, Regionalität und klare vertragliche Regelungen ihren Konsumenten Vertrauen und Kompetenz vermitteln. Folgende Handlungsempfehlungen werden in Richtung der Cloud-Service-Anbieter ausgesprochen:

- **Klare vertragliche Vereinbarungen**
  Neben den übertragenen technischen Pflichten (SLAs etc.) sollten Cloud-Service-Anbieter auch die rechtlichen Verpflichtungen (DSG etc.) ihrer Kunden erfüllen und diese zum Vertragsbestandteil machen. Da diese rechtlichen Erfordernisse österreichischer Unternehmen und Behörden unterschiedlich sein können, empfiehlt es sich, nicht einen Einheitsvertrag, sondern auf die Zielgruppen zugeschnittene Verträge anzubieten.

- **Vertrauen über Zertifikate Dritter schaffen**
  Speziell kleine, neue bzw. noch unbekannte Cloud-Service-Anbieter können ein Vertrauensproblem seitens des Konsumenten haben. Hier wird empfohlen, Vertrauen über Zertifikate zu

schaffen. Es ist jedoch darauf zu achten, dass die Zertifikate von vertrauenswürdigen und mit entsprechender Reputation ausgestatteten Dienstleistern wie beispielsweise TÜV Rheinland oder EuroCloud ausgestellt werden.

- **Datenhaltung innerhalb der Europäischen Union forcieren, Verzicht auf Dienste mit US-Bezug:** Nahezu jeder Cloud-Service-Anbieter, speziell im SaaS-Bereich, benötigt Cloud-Services Dritter (beispielsweise Speicher, Rechenkapazität oder Entwicklungsumgebungen), um sein Angebot zu betreiben. Die US-Überwachungsaktivitäten der vergangenen Monate haben den einfachen Zugriff der US-Behörden auf US-IT-Firmen demonstriert. Aus diesem Grund sind Cloud-Service-Anbieter angehalten, die Datenhaltung und Datenverarbeitung wenn möglich ausschließlich innerhalb der Europäischen Union durchzuführen. Im Idealfall haben zugekaufte dritte Leistungen auch keinen rechtlichen Bezug außerhalb des EU-Raums (z.B. US-Unternehmen, welche Dienste innerhalb der EU anbieten).
  Die Recherchen haben gezeigt, dass dies aufgrund der Dominanz der US-Cloud-Service-Angebote kein leichtes Unterfangen ist (speziell im IaaS-Bereich). Aus diesem Grund ist die europäische Cloud-Service-Industrie dazu aufgerufen, entsprechende Angebote bereitzustellen und Bewusstseinsbildung in diese Richtung zu betreiben.

8.3 Handlungsempfehlungen für Interessensvertreter

Als Interessensvertreter sind im Kontext dieses Berichts jene Organisationen angesprochen, welche die Interessen von EPU, KMU und kleinen wie mittleren Behörden in Österreich vertreten (z.B. Wirtschaftskammer Österreich). Folgende Handlungsempfehlungen können für Interessensvertreter ausgesprochen werden:

- **Aktive Kommunikation der wichtigsten rechtliche Bestimmungen an die Zielgruppen**
  Während bei der Nutzung von Cloud-Service-Angeboten die technischen Aspekte auf deren Wirtschaftlichkeit und Nutzenstiftung meist im Detail von den Kunden durchleuchtet werden, werden die rechtlichen Verpflichtungen nicht mit derselben Intensität beachtet. Aus diesem Grund empfehlen wir, rechtliche Bestimmungen im Kontext des Cloud-Computing in kurzer, aber ausdrücklicher Weise inklusive Nennung der Konsequenzen bei Nichteinhaltung an die Zielgruppen zu kommunizieren. Bei sich verändernden Bestimmungen wie der kommenden EU-Datenschutzverordnung sollten die Zielgruppen gesondert informiert werden.

- **Wiederkehrende Informationskampagnen**
  Informationskampagnen bzgl. der Chancen und Herausforderungen des Cloud-Computings sollten in wiederkehrenden Abständen (z.B. jährlich) durchgeführt werden. Wie auch in anderen Bereichen (z.B. Verkehrssicherheit) sind den Kunden die Gefahren prinzipiell bewusst, aber bei Vertragsabschluss eines Cloud-Computing-Angebots nicht unbedingt präsent. Darüber hinaus erfordern sich verändernde Bestimmungen und Situationen (US-Abhörskandal, EU-Datenschutzverordnung etc.) ohnehin gesonderte Informationskampagnen.

- **Information über zertifizierter Anbieter**
  Wie bei den „Handlungsempfehlungen für Anbieter“ ausgeführt, können Zertifikate zusätzliches Vertrauen zwischen Konsument und Cloud-Service-Anbieter schaffen. Auf Basis von anerkannten Zertifikaten sollten die Interessensvertretungen eine Liste dieser zertifizierten Anbieter zur Verfügung stellen, um ihren Zielgruppen die Auswahl eines geeigneten Cloud-Service-Anbieters zu erleichtern.

- **Monitoring der „Standardverträge“ ausgewählter Anbieter**
  Oftmals kommen bei Cloud-Service-Anbietern Standardverträge ohne Berücksichtigung individueller Kundenbedürfnisse zum Einsatz. Standardverträge ausgewählter, d.h. sehr häufig verwendeter, Cloud-Service-Anbieter können von den Interessensvertretungen auf Konformität hinsichtlich der geltenden gesetzlichen Bestimmungen geprüft werden (wie dies auch schon im Finanzbereich beispielsweise bei Versicherungsverträgen erfolgt). Die in den Verträgen gefundenen unklaren und/oder nicht gesetzeskonformen oder für den Konsumenten nachteiligen Formulierungen sollten zumindest an die Konsumenten kommuniziert werden. Im Idealfall kann dieses Monitoring der Standardverträge durch Kooperation mit den Cloud-Service-Anbietern zu für den Konsumenten verbesserten Standardverträgen führen.

8.4 Entwicklungen in naher Zukunft

In naher Zukunft zu erwartende Entwicklungen betreffen sowohl rechtliche als auch technologische Aspekte. Insbesondere ist davon auszugehen, dass Datenschutz im Kontext des Cloud-Computing zu intensiven Diskussion nicht nur innerhalb der EU, sondern auch mit den wichtigsten Wirtschaftspartnern der EU führen wird. Die zunehmende Globalisierung der IT-Infrastrukturen und die technische Möglichkeit, IT-Dienstleistungen weltweit anzubieten, erzeugen einen verstärkten wirtschaftlichen Druck auf Datenschutzinteressen. Dies kann sowohl zu Standortnachteilen als auch -vorteilen führen, je nachdem, ob es gelingt, ein hohes Datenschutzniveau als Wettbewerbsvorteil zu etablieren. Die Diskussionen zwischen der EU und den USA, verschärft durch die NSA-Enthüllungen des Jahres 2013, lassen bereits erahnen, wie schwierig sich die internationalen Diskussionen gestalten werden. Das Safe–Harbor-Abkommen bildet derzeit noch die zentrale Basis für den Austausch personenbezogener Daten zwischen EU und USA. Ob dieses Abkommen im Fall einer EU-Datenschutzverordnung aufrecht bleiben kann oder neu verhandelt werden muss, ist eine der wohl wichtigsten Fragen im Kontext des geplanten Freihandelsabkommens zwischen EU und USA.

Zurzeit ist dieses Abkommen die wichtigste datenschutzrechtliche Brücke zwischen den beiden Wirtschaftspartnern. Jene internationalen Schatten, die sich aufgrund der Krise in der Ukraine abzeichnen, werden ebenfalls ihre Auswirkungen auf das Hosting von Cloud-Dienstleistungen außerhalb der EU haben.

Da aufgrund der in den vergangenen Jahren kontinuierlich zunehmenden Bedeutung von Cloud-Computing davon ausgegangen werden kann, dass diese Technologie bald so wenig wegzudenken sein wird wie heute das Internet, ist auch davon damit zu rechnen, dass sichere und datenschutzkonforme Cloud-Technologie innerhalb der EU eine hohe Priorität erhalten wird.

GLOSSAR

Account: Benutzerkonto im Kontext eines Informationsdienstes

AGB: Allgemeine Geschäftsbedingungen

API: Application Programming Interface (Programmierschnittstelle)

Audit: Überprüfung im Kontext der Informationssicherheit

Backup: Sicherheitskopie von Daten

BAO: Bundesabgabenordnung (Österreich)

BSI: Bundesamt für Sicherheit in der Informationstechnik (Deutschland)

Business Continuity: betriebliches Kontinuitätsmanagement

Business Impacts: Beeinträchtigung der üblichen Geschäftsabläufe

CAIQ: Consensus Assessments Initiative Questionnaire

Compliance: Regelkonformität

Confidentiality: Vertraulichkeit im Kontext der Informationssicherheit

CRM: Customer Relationship Management

Cronjobs: wiederkehrende Aufgaben welche automatisiert auf einem IT-System ausgeführt werden

CSA: Cloud Security Alliance (Organisation)

CSP: Cloud Service Provider (-Anbieter)

DDoS/DoS-Attacken: Distributed Denial of Service Attacken

Deployment: Installation und Einrichtung eines Informationssystems

Disaster Recovery: Wiederherstellung der Dienste nach einer schwerwiegenden Unterbrechung

DMS: Dokumentenmanagementsystem

DSG: Datenschutzgesetz (Österreich)

ENISA: European Network and Information Security Agency

Feature: Eigenschaft eines Informationssystems

Firewall: Filtersystem zu Kontrolle des Verkehrs zwischen Computernetzwerken

Front-/Backend: als Frontend werden jene Systemteile bezeichnet welche dem Benutzer näher sind (z.B. User Interface). Als Backend werden die jene Systemteile bezeichnet welche dem eigentlich verarbeitenden System näher sind (z.B. Datenbank).

Governance: Steuerungs- und Regelsystem im Sinne der Aufbau- und Ablauforganisation

Hacker: Person, welche sich unauthorisierten Zutritt zu einem Computersystem verschafft

HIPAA: Health Insurance Portability and Accountability Act (US-Gesetz)

host-based intrusion detection: Erkennung von Angriffsversuchen auf dem Rechner

Hypervisor: Computerprogramm welches eine virtuelle Maschine bereitstellt

IaaS: Infrastructure as a Service

Incident Reporting: strukturierte Berichtslegung von geschäftsbeeinträchtigenden Störfällen

Incident: Vorfall im Zusammenhang mit der Informationssicherheit

IPSec: Internet Protocol Security (verschlüsselter Datenverkehr)

KMU: kleine und mittlere Unternehmen

Load Balancing: Lastverteilung grosser Anfragen oder Berechnungsschritte auf mehrere IT-Systeme

Logfiles: automatisch geführtes Protokoll bestimmter Aktionen von IT-Prozessen

Malware: Schadsoftware

Metadaten: Daten über Daten

OWASP: Open Web Application Security Project

Patch: Update eines Programms zwecks Funktionalitäts- oder Sicherheitsverbesserungen

Penetrationstest: gezielte Sicherheitstests von Rechnern und Netzwerken

Portabilität: Möglichkeit, Daten zwischen verschiedenen Systemen zu transferieren

Public Cloud: Cloud–Angebot, welches einer breiten Masse zur Verfügung steht

Risk Governance Frameworks: Steuerungs- und Regelsystem im Kontext des Risikomanagements

SaaS: Software as a Service

Schlüssel: kryptografischer Schlüssel

Schlüsselmanagement: Verwaltung kryptografischer Schlüssel

SDL: Security Development Lifecycle

Service-Pack: Sammlung von Patches (grösseres Update)

SLA: Service Level Agreement (Vereinbarung bzgl. Dienstqualität)

SPAM: unerwünschte E-Mail-Nachrichten

SSH: Secure Shell (Netzwerkprotokoll und damit verbundene Programme)

SSL: Secure Sockets Layer (Netzwerkprotokoll zur sicheren Datenübertragung)

UGB: Unternehmensgesetzbuch

Vendor Lock-in: Herstellerabhängigkeit

Zwei-Faktor-Authentifizerung: mindestens zwei Faktoren (z.B. Passwort und Biometrie) zur Anmeldung an ein Computersystem erforderlich

TABELLENVERZEICHNIS

ABBILDUNGSVERZEICHNIS

BIBLIOGRAPHIE

1 EINLEITUNG

[1] IDC Cloud Research, abrufbar unter: http://www.idc.com/prodserv/idc_cloud.jsp (letzter Zugriff: 24.03.2014)

[2] How big is Amazon's cloud?, abrufbar unter: http://blog.deepfield.net/2012/04/18/how-big-is-amazons-cloud/ (letzter Zugriff: 24.03.2014

2 DEFINITIONEN UND ABGRENZUNGEN

[3] McCarthy, J., „Centennial Keynote Address", Massachusetts Institute of Technology (MIT), USA, 1961.

[4] Cloud Computing Grundlagen, abrufbar unter: https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html (letzter Zugriff: 24.03.2014)

[5] Mell, P., Grance, T., "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, 2011.

[6] Ein-Personen-Unternehmen in Österreich, abrufbar unter: http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=357341&DstID=17 (letzter Zugriff: 24.03.2014)

[7] Klein- und Mittelbetriebe in Österreich: https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/KMU_Definition.html (letzter Zugriff: 24.03.2014)

3 VERWANDTE ARBEITEN

[8] ASIT - Österreichisches Informationssicherheitshandbuch – Cloud Strategie; https://www.sicherheitshandbuch.gv.at/

[9] EuroCloud Austria. Leitfaden Cloud-Computing. Recht, Datenschutz & Compliance (2011); http://www.eurocloud.at/projekte/publikationen/leitfaeden.html

[10] Eurocloud.Austria – Cloud-Verträge – Was Anbieter und Kunden besprechen sollten; http://www.eurocloud.at/projekte/publikationen/leitfaeden.html

[11] Wirtschaftskammer Österreich – IT Sicherheitshandbuch; http://www.bmi.gv.at/cms/BK/praevention_neu/info_material/files/IT_Sicherheitshandbuch.pdf

[12] Bundeskanzleramt Österreich – Cloud-Computing-Positionspapier; http://www.bka.gv.at/site/4291/default.aspx

[13] EGIZ – E-Government und Cloud-Computing; http://www.egiz.gv.at/de/research/5-Cloud-Computing-im-E-Government-in-Europa

[14] Wirtschaftsagentur Wien – Software as a Service – Verträge richtig abschließen; http://www.clusterwien.at/files/uploads/2013/02/SAAS_SoftwarebroschuereDruck.pdf

[15] BSI Sicherheitsempfehlungen für Cloud Computing Anbieter; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile

[16] Bitkom Cloud Computing – Was Entscheider wissen müssen; http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf

[17] Datenschutzrechtliche Anforderungen an Cloud-Computing, abrufbar unter: https://www.european-privacy-seal.eu/results/fact-sheets/Cloud%20Computing%20FS-201207-DE.pdf (letzter Zugriff: 24.03.2014)

[18] ENISA Cloud-Computing – Benefits, Risks, and Recommendations for Information Security; http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[19] ENISA Survey – An SME perspective on Cloud-Computing; http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey

[20] ENISA – Critical Cloud Computing – A CIIP perspective on cloud computing services; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

[21] RAND Europe – The Cloud – Understanding the Security, Privacy and Trust Challenges; http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-

security-privacy-trust-challenges-2010_en.pdf

[22] http://de.wikipedia.org/wiki/Hypervisor

[23] NIST, Special Publication 800-144 – Guidelines on Security and Privacy in Public Cloud Computing (2011); http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[24] Larry Ponemon, Security of Cloud Computing Users, Ponemon Institute, May 12, 2010, <URL: http://www.ca.com/files/IndustryResearch/security-cloud-computing-users_235659.pdf>

[25] NIST, Special Publication 800-146, Cloud Computing Synopsis and Recommendations; http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

[26] Cloud Computing Security Considerations; http://www.asd.gov.au/infosec/cloudsecurity.htm

[27] CSA Security Guidance for Critical Areas of Focus in Cloud Computing; https://cloudsecurityalliance.org/research/security-guidance/

[28] Gartner – Assessing the Security Risks of Cloud Computing; https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing

[29] CSA – The Notorious Nine: Cloud Computing Top Threats in 2013; https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[30] Zeus bot found using Amazon's EC2 as C&C server, abrufbar unter: http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/ (letzter Zugriff: 24.03.2014)

[31] GRC Stack, abrufbar unter: https://cloudsecurityalliance.org/research/grc-stack/ (letzter Zugriff: 24.03.2014)

[32] The FedRAMP Security Controls Baseline

4 TECHNISCHE UND RECHTLICHE GRUNDLAGEN

[33] Sosinsky, Barrie: Cloud Computing Bible (2011)

[34] Datenschutzrechtliche Anforderungen an Cloud-Computing, abrufbar unter: https://www.european-privacy-seal.eu/results/fact-

sheets/Cloud%20Computing%20FS-201207-DE.pdf (letzter Zugriff: 24.03.2014)

[35] Göllner, DI Johannes, MSc: Unterlagen zu Vorlesung „Einführung in Risikomanagement“

[36] Commission decisions on the adequacy of the protection of personal data in third countries, abrufbar unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (letzter Zugriff: 24.03.2014)

[37] EuroCloud.Austria: 6. Cloud Services – Vertragsbruch in der Cloud – Was tun?, anzufordern unter: http://www.eurocloud.at/projekte/publikationen/leitfaeden.html (letzter Zugriff: 25.03.2014)

[38] Schwellenwerte-Verordnung 2014, abrufbar unter: http://portal.wko.at/wk/format_detail.wk?angid=1&stid=628847&dstid=335 (letzter Zugriff: 24.03.2014)

[39] Vgl. Reichstädter, P., Cloud Computing Positionspapier 2011, Bundeskanzleramt Österreich, 2011.

[40] Teletrust Pressemitteilung vom 22.05.2013: „Achtung, Grauzone: Journalistischer Quellenschutz bei staatlichem Zugriff auf Cloud-Speicher“, , abrufbar unter: https://www.teletrust.de/de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=564&cHash=26a2c6b48933604968775edc5aa790c1 (letzter Zugriff: 25.03.2014)

[41] Weichert, Thilo / Clementi, Lillian [Translator]. Cloud Computing & Data Privacy. Verfügbar unter https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf (2011)

[42] Borges, Georg / Brennscheidt, Kirstin. Rechtsfragen des Cloud Computing – ein Zwischenbericht. In: Borges, Georg / Brennscheidt, Kirstin. Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. (2012)

[43] Eckhardt, Jens. Datenschutz im „Cloud Computing“ aus Anbietersicht. In: Borges, Georg / Brennscheidt, Kirstin. Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. S.104. (2012)

[44] Giannakaki, Maria. The EU Data Protection Directive revised: New challenges and perspectives. Verfügbar unter http://www.kalaw.gr/wmt/userfiles/papers_184-giannakaki-full_text-en-v001(2).pdf

[45] Schelleckens, B.J.A. The European Data Protection Reform in the Light of Cloud Computing

[46] European Commission. Commission decisions on the adequacy of the protection of personal data in third countries. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/ (2013)

[47] Wybitul, Tim / Patzak, Andrea. Safe Harbor: More Stringent Requirements for the Transfer of Data to the USA. Available at http://www.mayerbrown.com/files/Publication/613f8a8c-4731-47d6-8509-f08934d61f84/Presentation/PublicationAttachment/352ad8f2-8e3f-44be-aae4-f9cbcb9b9157/Legal_Update_SafeHarbor_14_6.pdf

[48] Marchini, Renzo. Cloud Computing Under The European Commission's Proposed Regulation To Revise The EU Data Protection Framework. In World Data Protection Report Volume 12, Number 2 (2012).

[49] U.S.-EU Safe Harbor List, abrufbar unter: https://safeharbor.export.gov/list.aspx (letzter Zugriff: 24.03.2014)

[50] U.S.-EU Safe Harbor Overview, abrufbar unter: http://export.gov/safeharbor/eu/eg_main_018476.asp (letzter Zugriff: 24.03.2014)

[51] Beschluss des Düsseldorfer Kreises am 28./29. April 2010. Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html (letzter Zugriff: 24.03.2014)

[52] Microsoft admits Patriot Act can access EU-based cloud data,, abrufbar unter: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225 (letzter Zugriff: 24.03.2014)

[53] Inanspruchnahme des Patriot Acts und anderer US-rechtlicher Regelungen zur Beschaffung von personenbezogenen Daten aus dem Raum der Europäischen Union durch US-Behörden abrufbar unter: https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html (letzter Zugriff: 24.03.2014)

[54] 50C36, abrufbar unter: http://uscode.house.gov/download/pls/50C36.txt (letzter Zugriff: 24.03.2014)

[55] Dutch government to ban U.S. providers over Patriot Act concerns, abrufbar unter: http://www.zdnet.com/blog/btl/dutch-government-to-ban-u-s-providers-over-patriot-act-concerns/58342 (letzter Zugriff: 24.03.2014)

[56] Hogan Lovells' Revealing Study About Governmental Access to Data in the Cloud Detailed in White Paper Released at Brussels Program, abrufbar unter: http://www.hoganlovells.com/hogan-lovells-revealing-study-about-governmental-

access-to-data-in-the-cloud-detailed-in-white-paper-released-at-brussels-program-05-23-2012/ (letzter Zugriff: 24.03.2014)

[57] Staten, James. Is Cloud Computing Ready For The Enterprise? Forrester Research, Inc, 2008.

[58] Aljabre, Abdulaziz. Cloud Computing for Increased Business Value. International Journal of Business and Social Science Vol. 3 No. 1; January 2012.

[59] Chorafas N. Dimitris. Cloud Computing Strategies. CRC Press, 2011.

[60] Metzger, Christian; Reitz, Thorsten; Villar Juan. *Cloud Computing Chancen und Risiken aus technischer und unternehmerischer Sicht.* München: Carl Hanser Verlag München, 2011.

[61] Anwendungspotenziale von Cloud Computing im Handel, abrufbar unter: http://winfwiki.wifom.de/index.php/Anwendungspotenziale_von_Cloud_Computing_im_Handel (letzter Zugriff: 24.03.2014)

[62] Gonzalez, Reyes; Gasco, Jose; Llopis, Juan. Information systems outsourcing reasons and risks: a new assessment. In: Industrial Management & Data Systems.

[63] Antonopoulos, Nick; Gillam. Lee. Cloud Computing Principles, Systems and Applications. Springer-Verlag, London. 2010.

[64] Fenz et. al, KIRAS – Monitoring zur Datensicherheit in Österreich (DaMon Studie), 2012.

[65] Buyya, Rajikumar; Broberg, James; Goscinski, Andrzej. CLOUD COMPUTING Principles and Paradigms. Hoboken, NJ 07030, USA: John Wiley & Sons, Inc., 2011.

[66] Cloud Computing und Vertragsgestaltung, abrufbar unter: http://www.business-cloud.de/cloud-computing-und-vertragsgestaltung/ (letzter Zugriff: 24.03.2014)

[67] Höllwarth, Tobias, Cloud Migration. German edition, Heidelberg, München, Landsberg, Frechen, Hamburg, Huethig Jehle Rehm GmbH, 2012.

[68] Meir-Huber, Mario. Cloud Computing, Praxisratgeber und Einstiegsstrategien. Frankfurt am Main, Software & Support Media GmbH, 2011.

5 RECHTLICHE UND TECHNISCHE EVALUIERUNG

[69] Referenzen zu Kapitel 5.5.2

Amazon. (8. 8 2013). *Amazon Agreement*. Von http://aws.amazon.com/agreement/ abgerufen

Amazon. (8. 8 2013). *Amazon S3*. Von Functionality: http://aws.amazon.com/s3/ abgerufen

Amazon. (8. 8 2013). *Amazon SLA*. Von http://aws.amazon.com/s3-sla/ abgerufen

Amazon. (8. 8 2013). *Amazon Web Services: Overview of Security Processes*. Von http://aws.amazon.com/articles/1697?_encoding=UTF8&jiveRedirect=1 abgerufen

Amazon. (9. 8 2013). *AWS privacy note.* Von http://aws.amazon.com/privacy/ abgerufen

Amazon Overview of Security Processes- WhitePaper. (9. 8 2013). *Amazon Web Services: Overview of Security Processes- WhitePaper.* Von http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf abgerufen

Data Liberation Front. (16. 8 2013). Von http://www.dataliberation.org/ abgerufen

Dropbox. (9. 8 2013). *Allgemeine Geschäftsbedingungen*. Von https://www.dropbox.com/privacy#terms abgerufen

Dropbox. (24. 9 2013). *Buy Dropbox for Business*. Von https://www.dropbox.com/business/buy abgerufen

Dropbox. (20. 8 2013). *Datenschutzrichtlinien.* Von https://www.dropbox.com/privacy abgerufen

Dropbox. (9. 8 2013). *Dropbox Developer.* Von https://www.dropbox.com/developers abgerufen

Dropbox. (8. 8 2013). *Dropbox Security Guide.* Von https://www.dropbox.com/static/business/resources/Guide_Security.pdf abgerufen

Dropbox. (8. 8 2013). *Dropbox Sicherheit*. Von https://www.dropbox.com/business/security abgerufen

Dropbox. (20. 8 2013). *Dropbox-Versionshinweise.* Von https://www.dropbox.com/release_notes abgerufen

Dropbox. (8. 8 2013). *Is Dropbox HIPAA, FERPA, SAS 70, Safe Harbor, ISO 9001, ISO 27001,or PCI compliant?* Von https://www.dropbox.com/help/238/en abgerufen

Dropbox. (8. 8 2013). *Official Blog of Dropbox for Business*. Von Introducing a new admin console and sharing controls for Teams: https://www.dropboxatwork.com/2013/02/introducing-a-new-admin-console-and-sharing-controls-for-teams/ abgerufen

Dropbox. (9. 8 2013). *Vereinbarung für „Dropbox für Unternehmen“*. Von https://www.dropbox.com/privacy#business_agreement abgerufen

Dropbox. (19. 8 2013). *Wie sicher ist Dropbox?* Von https://www.dropbox.com/help/27/de abgerufen

Dropbox-Datenschutzrichtlinien. (9. 8 2013). *Datenschutzrichtlinien*. Von https://www.dropbox.com/privacy#privacy abgerufen

Fabasoft. (12. 8 2013). *AGB.* Von http://www.fabasoft.com/de/contract.html abgerufen

Fabasoft. (16. 8 2013). *API.* Von http://developer.foliocloud.com/en/api.html abgerufen

Fabasoft. (16. 8 2013). *Audit Log Configuration in the Object Class.* Von http://help.fabasoftfolio.com/index.php?topic=doc/Configuration-of-Audit-Logs/audit-log-configuration-in-the-object-class.htm abgerufen

Fabasoft. (24. 8 2013). *Business Shop*. Von http://www.foliocloud.com/business-shop_en.html abgerufen

Fabasoft. (12. 8 2013). *Cloud Assurance.* Von http://trust.fabasoft.com/de/cloud-assurance.html abgerufen

Fabasoft. (16. 8 2013). *Fabasoft Zertifikate.* Von https://www.fabasoft.com/de/zertifizierungen-pruefungen.html abgerufen

Fabasoft. (12. 8 2013). *Performance Characteristics of Data Center Operation.* Von http://www.fabasoft.com/FscHttpServlet?fscurl=https%3A%2F%2Fsaas.fabasoft.com%2Ffabasoftp%2Fdownload%2FCOO.2222.2001.1.4720157 abgerufen

Fabasoft. (12. 8 2013). *Performance Characteristics of Data Security.* Von http://www.fabasoft.com/FscHttpServlet?fscurl=https%3A%2F%2Fsaas.fabasoft.com%2Ffabasoftp%2Fdownload%2FCOO.2222.2000.9.105525 abgerufen

Fabasoft. (20. 8 2013). *Sicher und Zuverlässig.* Von http://www.foliocloud.com/sicher-und-zuverlaessig.html abgerufen

Fabasoft. (12. 8 2013). *Sicherheit und Datenschutz* . Von http://trust.fabasoft.com/de/sicherheit-datenschutz.html abgerufen

Fabasoft. (16. 8 2013). *Zwei-Faktor-Authentifizierung.* Von http://help.foliocloud.com/index.php?topic=doc/SPI-Fabasoft-Folio-Cloud-medio-ger/zwei-faktor-authentifizierung.htm abgerufen

Google. (12. 8 2013). *Certification & data privacy.* Von http://www.google.com/apps/intl/en-GB/trust/data_protection.html abgerufen

Google. (16. 8 2013). *Code of Conduct.* Von http://investor.google.com/corporate/code-of-conduct.html abgerufen

Google. (12. 8 2013). *Data center security video.* Von http://www.youtube.com/watch?v=1SCZzgfdTBo abgerufen

Google. (12. 8 2013). *Datenschutzerklärung und Nutzungsbestimmung*. Von http://www.google.com/policies/privacy/ abgerufen

Google. (2013, 9 23). *Google Apps for Business (Online) Agreement*. Retrieved from http://www.google.com/apps/intl/en/terms/premier_terms_ie.html

Google. (16. 8 2013). *Google Apps Platform.* Von https://developers.google.com/google-apps/ abgerufen

Google. (12. 8 2013). *Google Apps Service Level Agreement.* Von http://www.google.com/apps/intl/en/terms/sla.html abgerufen

Google. (12. 8 2013). *Google Apps Trust- Sicherheit.* Von http://www.google.com/apps/intl/de/trust/security.html abgerufen

Google. (16. 8 2013). *IT Security White Paper.* Von http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf abgerufen

Google. (12. 8 2013). *Online Agreement*. Von http://www.google.com/apps/intl/de/terms/premier_terms.html abgerufen

Google. (12. 8 2013). *Rechenzentren- Daten und Sicherheit.* Von http://www.google.com/about/datacenters/inside/data-security/index.html abgerufen

Google. (12. 8 2013). *Standorte Rechenzentren.* Von http://www.google.com/about/datacenters/inside/locations/index.html abgerufen

Google. (12. 8 2013). *Vereinbarung.* Von http://www.google.com/apps/intl/de/terms/premier_terms.html abgerufen

Microsoft. (9. 8 2013). *Security Audit.* Von http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm abgerufen

Microsoft. (2013). *Administrative Access*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/online/legal/v2/?docid=24

Microsoft. (9. 8 2013). *Configure audit settings.* Von http://office.microsoft.com/en-us/sharepoint-server-help/configure-audit-settings-for-a-site-collection-HA102031737.aspx abgerufen

Microsoft. (2013). *Die zehn wichtigsten Fragen zur Vertrauenswürdigkeit* . Abgerufen am 7. 8 2013 von http://office.microsoft.com/de-at/business/office-365-trust-center-die-zehn-wichtigsten-fragen-zur-vertrauenswurdigkeit-sicherheit-und-datenschutz-in-der-cloud-FX104029824.aspx

Microsoft. (7. 8 2013). *Dienstkontinuität*. Abgerufen am 7. 8 2013 von http://office.microsoft.com/de-at/business/office-365-verfugbarkeit-der-onlinedienste-FX104028266.aspx

Microsoft. (9. 8 2013). *Es sind ihre Daten.* Von http://office.microsoft.com/de-de/business/office-365-portabilitat-von-onlinedaten-FX103045783.aspx abgerufen

Microsoft. (2013). *Konformitätsbenachrichtigungen*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/online/legal/v2/?docid=32&langid=de-DE

Microsoft. (7. 8 2013). *Managing Access to the Exchange Online Service*. Von Ask Perry: http://blogs.technet.com/b/perryclarke/archive/2012/05/16/managing-access-to-the-exchange-online-service.aspx abgerufen

Microsoft. (2013). *Microsoft Datenschutzrichtlinien*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/privacystatement/de-at/core/default.aspx?CTT=114

Microsoft. (9. 8 2013). *Microsoft Dynamics CRM Online Security and Service Continuity.* Von http://www.microsoft.com/en-us/download/confirmation.aspx?id=30187 abgerufen

Microsoft. (2013). *Office 365 – Datenschutzbestimmungen*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/online/legal/v2/?docid=43&langid=de-de

Microsoft. (9. 8 2013). *Office for developers.* Von http://msdn.microsoft.com/en-US/office abgerufen

Microsoft. (7. 8 2013). *Privacy in the Public Cloud: The Office 365 Approach.* Von http://www.microsoft.com/en-us/download/confirmation.aspx?id=28540 abgerufen

Microsoft. (9. 8 2013). *Security Development Lifecycle.* Von http://www.microsoft.com/security/sdl/default.aspx abgerufen

Microsoft. (7. 8 2013). *Security in Office 365 White Paper.* Von http://www.microsoft.com/en-us/download/confirmation.aspx?id=26552 abgerufen

Microsoft. (2013. 8 2013). *Security, Audits and Certification.* Von http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm abgerufen

Microsoft. (7. 8 2013). *The Microsoft Online Services Diagnostics and Logging (MOSDAL) Support Toolkit*. Von http://support.microsoft.com/kb/960625 abgerufen

Microsoft. (2013). *Third Parties*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/online/legal/v2/?docid=26

Microsoft. (2013). *Unabhängig geprüft*. Abgerufen am 7. 8 2013 von http://office.microsoft.com/de-at/business/von-einem-drittanbieter-verifiziert-die-sicherheit-und-der-datenschutz-von-office-365-FX103089231.aspx

Microsoft. (7. 8 2013). *Unablässige Sicherheit*. Von http://office.microsoft.com/de-at/business/microsoft-losungen-fur-unternehmenssicherheit-FX103045813.aspx abgerufen

Microsoft. (9. 8 2013). *Vertrag über Microsoft Dienste.* Von http://windows.microsoft.com/de-de/windows-live/microsoft-services-agreement abgerufen

Microsoft. (2013). *Vorreiter in Sachen Transparenz*. Abgerufen am 7. 8 2013 von http://office.microsoft.com/de-at/business/office-365-transparenz-fur-unternehmen-FX103046257.aspx

Microsoft. (2013). *Where is my Data*. Abgerufen am 7. 8 2013 von http://www.microsoft.com/online/legal/v2/?docid=25

Salesforce. (14. 8 2013). *Administrative Reports.* Von https://help.salesforce.com/help/doc/en/reports_administrative.htm abgerufen

Salesforce. (14. 8 2013). *Data Export.* Von http://help.salesforce.com/apex/HTViewSolution?id=000005243&language=en_US abgerufen

Salesforce. (14. 8 2013). *Developer Site.* Von http://developer.force.com/de abgerufen

Salesforce. (13. 8 2013). *Internationale Datenschutzgesetze.* Von https://trust.salesforce.com/trust/de/laws/ abgerufen

Salesforce. (19. 8 2013). *Is all traffic to and from Salesforce.com APIs are encrypted ?* Von http://help.salesforce.com/apex/HTViewSolution?id=000171016&language=en_US abgerufen

Salesforce. (14. 8 2013). *Master Subscription Agreement.* Von http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf abgerufen

Salesforce. (19. 8 2013). *Monitoring Set-up Changes.* Von http://login.salesforce.com/help/doc/en/admin_monitorSet-up.htm abgerufen

Salesforce. (14. 8 2013). *Push Patch Updates.* Von http://wiki.developerforce.com/page/Push_Patch_Updates abgerufen

Salesforce. (16. 8 2013). *Salesforce Privacy Policy.* Von http://www.salesforce.com/company/privacy/ abgerufen

Salesforce. (14. 8 2013). *Salesforce System Status.* Von http://trust.salesforce.com/trust/status/ abgerufen

Salesforce. (25. 9 2013). *Salesforce.com-Tools zur Unterstützung der Datenschutzeinhaltung*. Von https://trust.salesforce.com/trust/de/tools/ abgerufen

Salesforce. (16. 8 2013). *Secure, private, and trustworthy: enterprise Cloud-Computing with Force.com.* Von http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf abgerufen

Salesforce. (25. 9 2013). *Secure, private, and trustworthy: enterprise Cloud-Computing with Force.com*. Von http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf abgerufen

Salesforce. (14. 8 2013). *Security White Paper.* Von http://wiki.developerforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper abgerufen

Salesforce. (13. 8 2013). *Sicherheitsüberblick.* Von https://trust.salesforce.com/trust/de/security/ abgerufen

Salesforce. (16. 8 2013). *System status.* Von https://trust.salesforce.com/trust/status/ abgerufen

Salesforce. (13. 8 2013). *Unterstützung der Datenschutzeinhaltung.* Von https://trust.salesforce.com/trust/de/tools/ abgerufen

SAP. (19. 8 2013). *AGB.* Von http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CEoQFjAA&url=http%3A%2F%2Fdownload.sap.com%2Fcorporate-en%2Fdownload.epd%3Fcontext%3DCB23E5D8F1D9E1C1C2992D25874D1E5C435A0CF80DC45A3FA9586BC7689ECC99B89CC9F18C7889DF34BBBD51DC10D5355A9B317 abgerufen

SAP. (19. 8 2013). *Allgemeine Geschäftsbedingungen für SAP Cloud-Services der SAP Österreich GmbH.* Von download.sap.com/corporate-en/download.epd?context=408546370FC301158EC1C0E2D5E0131988C2E0FDCB2B40A791EE1C0C07DE68BA29C416003F0B2D91D8DD2B28CF01B06F08DA3516D08A6A33 abgerufen

SAP. (19. 8 2013). *Application Lify cycle management.* Von http://scn.sap.com/docs/DOC-27063 abgerufen

SAP. (18. 8 2013). *Business Application Programming Interfaces.* Von http://help.sap.com/saphelp_46c/helpdata/de/61/f3f0371bc15d73e10000009b38f8cf/frameset.htm abgerufen

SAP. (19. 8 2013). *How SAP Protects Your Web Applications from Security Vulnerabilities.* Von http://sapinsider.wispubs.com/Article/How-SAP-Protects-Your-Web-Applications-from-Security-Vulnerabilities/4100 abgerufen

SAP. (19. 8 2013). *Multi-factor authentication, why not?* Von http://scn.sap.com/community/netweaver-portal/blog/2013/03/03/multi-factor-authentication-why-not abgerufen

SAP. (19. 8 2013). *NAVIGATOR (SAP- Partner) -Uncovering the Unknown: SAP Cloud Data Security & Compliance Update.* Von http://sapinfo.nbs-us.com/blog/bid/273835/Uncovering-the-Unknown-SAP-Cloud-Data-Security-Compliance-Update abgerufen

SAP. (19. 8 2013). *Privacy.* Von http://www.sap.com/austria/about/company/legal/privacy.epx#retention abgerufen

SAP. (20. 8 2013). *Protecting your data – and your business securely with SAP.* Von https://www54.sap.com/pc/tech/application-foundation-security/software/security-at-sap/index.html abgerufen

SAP. (19. 8 2013). *SAP Store Quick Guide.* Von https://wbhelp.sap.com/saphelp_sapstore/30/EN/ktp/Products/01200314690800001975/SAPStore/QG_SAPStore.html abgerufen

SAP. (19. 8 2013). *Security Patch Process FAQ.* Von http://scn.sap.com/community/security/blog/2012/03/27/security-patch-process-faq abgerufen

SAP. (20. 8 2013). *Set-up von Serviceverbindungen für den Remote Support durch SAP.* Von http://help.sap.com/saphelp_nw70ehp1/helpdata/de/96/ea39e6feb4457793cb00d1fee4e8fd/content.htm abgerufen

US Department of Commerce. (9. 8 2013). *U.S.-EU Safe Harbor Overview*. Von http://export.gov/safeharbor/eu/eg_main_018476.asp abgerufen

6 RISIKOANALYSE CLOUD-NUTZUNG

[70] Lighting in Dublin knocks Amazon and Microsoft data centers offline, abrufbar unter: http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/ (letzter Zugriff: 24.03.2014)

[71] Windows Azure Service disruption Update, abrufbar unter: https://blogs.msdn.com/b/windowsazure/archive/2012/03/01/windows-azure-service-disruption-update.aspx (letzter Zugriff: 24.03.2014)

[72] Online backup company Carbonite loses customers data and sues suppliers, abrufbar unter: http://techcrunch.com/2009/03/23/online-backup-company-carbonite-loses-customers-data-blames-and-sues-suppliers/ (letzter Zugriff: 24.03.2014)

[73] T-Mobile Sidekick disaster, abrufbar unter: http://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/ (letzter Zugriff: 24.03.2014)

[74] Evernote's July 1st server problem, abrufbar unter: http://blog.evernote.com/2010/08/09/july1/ (letzter Zugriff: 24.03.2014)

[75] Google Gmail Outage, abrufbar unter: http://www.huffingtonpost.com/2011/03/03/google-gmail-outage_n_830229.html (letzter Zugriff: 24.03.2014)

[76] CSA – The Notorious Nine: Cloud Computing Top Threats in 2013

[77] Amazon website treat, abrufbar unter: http://www.theregister.co.uk/2010/04/20/amazon_website_treat/ (letzter Zugriff: 24.03.2014)

[78] Amazon EC2 bot control channel, abrufbar unter: http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/ (letzter Zugriff: 24.03.2014)

[79] Insider threats to cloud computing, abrufbar unter: http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/ (letzter Zugriff: 24.03.2014)

[80] Zimmermann, 1980

[81] First an outage, abrufbar unter: http://betanews.com/2011/10/27/first-an-outage-now-a-lawsuit-us-canadian-blackberry-users-want-compensation/ (letzter Zugriff: 24.03.2014)

[82] Class action lawsuit targets Microsoft, abrufbar unter: http://arstechnica.com/gaming/2008/01/class-action-lawsuit-targets-microsoft-for-xbox-live-outages/ (letzter Zugriff: 24.03.2014)

[83] Blackberry services return, abrufbar unter: http://betanews.com/2011/10/13/blackberry-services-return-after-historical-global-outage/ (letzter Zugriff: 24.03.2014)

[84] Urteil 16.000 Euro Schadenersatz, abrufbar unter: http://www.zdnet.de/41558761/urteil-16-000-euro-schadenersatz-fuer-datenverlust-durch-stromausfall/ (letzter Zugriff: 24.03.2014)

[85] Grundwerte Informationssicherheit, abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhal

t/Glossar/glossar_node.html (letzter Zugriff: 24.03.2014)

[86] LA Bonn Urteil, abrufbar unter: http://openjur.de/u/454361.html (letzter Zugriff: 24.03.2014)

[87] F35 JSF aircraft program, abrufbar unter: http://spectrum.ieee.org/riskfactor/computing/it/f_35_jsf_aircraft_program_pene (letzter Zugriff: 24.03.2014)

[88] Dropbox authentication, abrufbar unter: http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/ (letzter Zugriff: 24.03.2014)

[89] Cloud site Dropbox drops the ball, abrufbar unter: http://www.consumeraffairs.com/news04/2011/06/cloud-site-dropbox-drops-the-ball.html (letzter Zugriff: 24.03.2014)

[90] Dropbox facing class action lawsuit, abrufbar unter: http://www.geek.com/news/dropbox-facing-class-action-lawsuit-over-any-password-worked-glitch-1396291/ (letzter Zugriff: 24.03.2014)

[91] Cloud storage Dropbox lawsuit, abrufbar unter: http://www.tomsguide.com/us/Cloud-storage-dropbox-lawsuit-Arash-Ferdowski-Cristina-Wong,news-11673.html (letzter Zugriff: 24.03.2014)

[92] Chameleon click fraud, abrufbar unter: http://www.infosecurity-magazine.com/view/31389/chameleon-click-fraud-botnet-costs-advertisers-6m-per-month/ (letzter Zugriff: 24.03.2014)

[93] TrueCrypt, abrufbar unter: www.truecrypt.org/ (letzter Zugriff: 24.03.2014)

[94] TAVUU, abrufbar unter: www.tavuu.com/ (letzter Zugriff: 24.03.2014)

7 LEITFÄDEN FÜR BEHÖRDEN UND KMUS

[95] Königs H.P., 2013, (Königs Hans Peter, 2013, IT-Risikomanagement mit System Praxisorientiertes Management von Informationssicherheits- und IT-Risiken, 4. Auflage, Springer Vieweg, Springer Fachmedien Wiesbaden)