Fraunhofer FOKUS

ELAN
Electronic Government
and Applications

ISPRAT

Hertie School
of Governance

Cloud-Computing für die öffentliche Verwaltung

ISPRAT-Studie November 2010

Peter H. Deussen
Linda Strick
Johannes Peters

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage November 2010

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

Telefon: +49-30-3436-7115
Telefax: +49-30-3436-8000
elankontakt@fokus.fraunhofer.de
www.fokus.fraunhofer.de

ISBN 978-3-00-033387-3

Cloud-Computing für die öffentliche Verwaltung

ISPRAT-Studie

November 2010

Dr. Peter H. Deussen
peter.deussen@fokus.fraunhofer.de

Linda Strick
linda.strick@fokus.fraunhofer.de

Fraunhofer-Institut für Offene Kommunikationssysteme
Kaiserin-Augusta-Allee 31
10589 Berlin

Dr. Johannes Peters
johannes.peters@peters-reinberg.de

Hertie School of Governance
Friedrichstraße 180–184
10117 Berlin

Vorwort

Cloud-Computing ist ein aktuelles Schlagwort in der Informationstechnik, das auch an der öffentlichen Verwaltung nicht vorbeigeht. Allerdings sind hier besondere Bedingungen wie die Sensibilität der Verarbeitung personenbezogener Daten, Kontrolle und Sicherheit zu beachten, wie sie für die öffentlichen Aufgaben gegeben sind.

Die vorliegende Studie fasst mit Stand November 2010 perspektivisch kooperatives eGovernments unter dem Blickwinkel der in der Öffentlichkeit viel diskutierten Charakteristiken des Cloud-Computing zusammen. Das Fraunhofer-Institut für Offene Kommunikationssysteme und die Hertie School of Governance haben neben der begrifflichen Eingrenzung des Cloud-Computing durch Fragebögen, Workshops und Recherchen die Rahmenbedingungen festgelegt, Risiken aufgezeigt und Gestaltungsoptionen diskutiert.

Das Fraunhofer-Institut für Offene Kommunikationssysteme und die Hertie School of Governance sowie die Autoren danken dem ISPRAT e. V. für seine Unterstützung. Besonderer Dank gilt darüber hinaus den folgenden Unternehmen, die mit viel Geduld und Zeit durch bilaterale Workshops die Arbeit unterstützt haben: Dataport, IBM Deutschland GmbH, Microsoft Deutschland, Oracle Deutschland B.V. & Co. KG, SAP Deutschland, Siemens AG und Taylor Wessing Deutschland.

Die große technologische und wirtschaftliche Bedeutung des Themas Cloud-Computing spiegelt sich auch in anderen politischen Initiativen wider. So wird in der neuen IT-Strategie der Bundesregierung »Deutschland Digital 2015« eine wichtige Rolle spielen. Zudem hat der IT-Gipfel-Prozess Cloud-Computing als ein zentrales Thema für die nationale Technologie- und Standort-Politik identifiziert. Beim Fünften Nationalen IT-Gipfel am 7. Dezember 2010 in Dresden wird das Thema Gegenstand mehrerer Arbeitsgruppen sein.

Erste Erfahrungen mit dem Cloud-Computing hat das Fraunhofer-Institut in seinem eGovernment-Labor gemacht. Mit Unterstützung unserer Partner werden hier im nächsten Jahr die technischen Voraussetzung

geschaffen sein, auch potentielle Interoperabilitätsszenarien zu demonstrieren.

Zusammenfassung

Der Begriff Cloud-Computing steht für einen der aktuell bedeutendsten Trends in der IT-Branche. Cloud-Computing bezieht sich auf die gemeinsame Nutzung von IT-Ressourcen mit erheblichen Effizienzsteigerungspotenzialen und fördert insoweit den Ansatz zu verstärkter IT-Kooperation. Insoweit erscheint Cloud-Computing auch als eine interessante Option für die unter besonderem Kostendruck stehende öffentliche Verwaltung, und deren Bemühungen um eine Konsolidierung öffentlicher IT-Strukturen. Allerdings stellt sich die Frage, ob — und wie — die mit Cloud-Computing verbundene Virtualisierung von IT über institutionelle Verwaltungsgrenzen hinweg kompatibel ist mit den rechtlichen Anforderungen und Anwendungsgrenzen im öffentlichen Sektor.

Diese Studie hat das Ziel, die Potentiale von Cloud-Computing für den deutschen öffentlichen Sektor aufzuzeigen und Entwicklungsalternativen anhand von ausgewählten Nutzungs- und Anwendungsszenarien zu beschreiben, wobei das Cloud-Computing kritisch aus der Perspektive heutiger Standards, wie sie für Verwaltungen relevant sind, durchleuchtet wird. Sie soll dazu dienen, ein besseres Verständnis für die Bedeutung und Möglichkeiten, aber auch Einschränkungen des Cloud-Computing zu schaffen, und um Wege aufzeigen, um Verwaltungen den Rückgriff auf solche Konzepte zu ermöglichen und zu vereinfachen.

Zunächst ergibt sich aus dem Kontext der rechtlichen und organisatorischen Rahmenbedingungen einer Cloud-basierten IT-Kooperation, dass die wesentliche Fragestellung hier die nach dem Risiko der Nutzung von Cloud-Technologien ist. Im Kern wird gezeigt, dass die auftretenden Risiken dabei durchaus eingrenzbar und beherrschbar erscheinen. Allerdings ergibt sich erheblicher Bedarf, die zu gestaltenden Risikotatbestände nicht in jedem Einzelfall einer Cloud-Migration abzusichern, sondern hier durch Standards für Dienstverträge und -spezifikationen und durch gesetzgeberische Regelungen einen für einzelne Behörden handhabbaren Rahmen bereitzustellen.

Eine anschließende Analyse zeigt, dass privatwirtschaftliche Anbieter sog. »öffentlicher Clouds« als Kooperationspartner für den öffentlichen

Sektor zum jetzigen Zeitpunkt nur bedingt in Frage kommen. Bei Clouds innerhalb des öffentlichen Sektor versprechen Cloud-Technologien aber bereits heute ein hohes Potential zur Konsolidierung von IT-Governance-Prozessen und zur Kooperation von Rechenzentren und behördlichen Dienstleistern. Entsprechende Ausgestaltungsszenarien werden entwickelt und analysiert.

Es zeigt sich, dass ein Zusammenschluss mehrerer Rechenzentren in einer sog. »Community-Cloud« ein aussichtsreiches, wenn auch nicht vollkommen unkritisch zu bewertendes Modell für übergreifende IT-Kooperationen darstellt.

Inhaltsverzeichnis

KAPITEL 1

Einleitung

Cloud-Computing steht ist einer der aktuell bedeutendsten Trends in der IT-Branche. Allerdings ist Cloud-Computing aufgrund seiner teils noch unscharfen Definition und der sich mit hoher Dynamik weiterentwickelnden Konzepte für die meisten Nutzer kaum mehr als ein Schlagwort. Die Basis des Cloud-Computing Konzepts besteht in der Trennung von Nutzung und Betrieb sowohl in Bezug auf Hardware als auch Software. Der Zugriff auf die Ressourcen erfolgt dabei über ein Netzwerk, wobei Ressourcenzuordnungen bedarfsgerecht automatisiert skaliert werden. Wichtigster Vorteil ist die Kosteneffizienz, die durch eine gemeinsame Nutzung wenig oder selten benötigter Ressourcen und Dienste zu erwarten ist. Hinzu kommt die Reduzierung der Personalkapazitäten durch den zu erwartenden geringeren Verwaltungsaufwand von Hard- und Softwarebereitstellung. Cloud-Computing bezieht sich auf die gemeinsame Nutzung von IT-Ressourcen und fördert insoweit den Ansatz zu verstärkter IT-Kooperation. Im Zusammenhang mit zunehmenden öffentlichen IT-Kooperationen kann Cloud-Computing ein Katalysator für die Verwaltungsmodernisierung sein.

Diese Studie hat das Ziel, die Potentiale von Cloud-Computing für den deutschen öffentlichen Sektor aufzuzeigen und Entwicklungsalternativen anhand von ausgewählten Nutzungs- und Anwendungsszenarien zu beschreiben, wobei das Cloud-Computing allerdings kritisch aus der Perspektive heutiger Standards, wie sie für Verwaltungen relevant sind, durchleuchtet wird. Es werden Ausgestaltungsszenarien in Richtung Cloud-Computing unter Berücksichtigung solcher Aspekte entwickelt und analysiert. Die Studie soll dazu dienen, ein besseres Verständnis für die Bedeutung und Möglichkeiten, aber auch Einschränkungen des Cloud-Computings zu schaffen und soll damit Verwaltungen den Rückgriff auf solche Konzepte vereinfachen.

Diese Zielsetzung ist in einem doppelten Sinne ambitioniert. Zum einen gibt es zwar eine Reihe von Initiativen und auch Praxisbeispiele, um die

stark differenzierte IT-Landschaft des deutschen öffentlichen Sektors zu konsolidieren und damit zu eGovernment-Kooperationen zu gelangen. Entsprechende Trends — wie sie insbesondere beim Thema »Shared Services« im Bereich öffentlicher IT zu beobachten sind — befinden sich jedoch noch in einem recht frühen Entwicklungsstadium.[1] Zum anderen befinden sich die (wissenschaftlich präzisierten/fundierten) Erkenntnisse zu Cloud-Computing-Ansätzen noch in einem sehr frühen Stadium.

Auch in der Praxis steckt das Cloud-Computing in Deutschland noch in den Kinderschuhen. Im angloamerikanischen dagegen Raum haben entsprechende Modelle jedoch bereits Fuß gefasst. Beispielsweise lagern eine Reihe US-amerikanischer Behörden Anwendungen in Clouds aus.

Etablierte IT-Dienstanbieter sind bereits für die weitere Nachfrage gerüstet, wie Google, Amazon oder Microsoft, die eine große Anzahl von Rechnern (mehr als 500.000) vorhalten und ihre Angebote für Cloud-Computing intensivieren. Im deutschen Sprachraum ist zu beobachten, dass über die Diskussion in der Fachcommunity und der Fachpresse hinaus — z. B. mit dem 2009 veröffentlichten BITKOM-Leitfaden (BITKOM, 2009) — die Promotion von Cloud-Computing durch IT-Dienstleister in den vergangenen Monaten weiter intensiviert wurde. So platzieren z. B. IBM oder CSC in Fachvorträgen und Workshops Cloud-Ansätze als einen besonders relevanten Entwicklungstrend für die zu erwartenden Strukturveränderungen im deutschen IT-Markt.

1.1 Methodologie

Der Themenbereich »Cloud-Computing für die öffentliche Verwaltung« ist breit angelegt: Aspekte wie rechtliche Vorgaben, organisatorische Strukturen, technologische Potentiale und Einschränkungen, Sicherheitsbedenken, Konsolidierungmöglichkeiten oder Datenschutz sind zu berücksichtigen, um nur einige Stichpunkte zu nennen. Selbstverständlich können in dieser Studie nicht alle Bereiche in der notwendigen Tiefe bearbeitet werden.

Um dennoch eine bzgl. der aktuellen Diskussion relevante Themenauswahl vornehmen zu können, haben wir in einer vorbereitenden Phase der Studie eine Reihe von Workshops mit Anbietern von Cloud-Dienstleistungen und Herstellern entsprechender Technologien, mit etablierten IT-Dienstleistern sowie mit Sicherheits- und Rechtsexperten durchgeführt (vgl. Abb. 1.1). Parallel dazu wurde eine Umfrage erstellt, die sich sowohl an Verwaltungen wie auch an IT-Dienstleister richtete. Da Cloud-Computing in Deutschland in der öffentlichen Verwaltung bisher so gut wie nicht eingesetzt wird, haben wir uns bei dieser Umfrage auf das eng verwandte Gebiet der »Dienstauslagerung« konzentriert: Für eine Behörde, die einen Cloud-Anbieter mit dem Betrieb von Dienstleistungen beauftragt, besteht ja im Ansatz auch eine Outsourcing-Situation.

Diese vorbereitende Phase führte uns zu einer konkreten Auswahl an Themen, die den Kern dieser Studie ausmachen:

[1] Vgl. hierzu (Fiedler u. a., 2010).

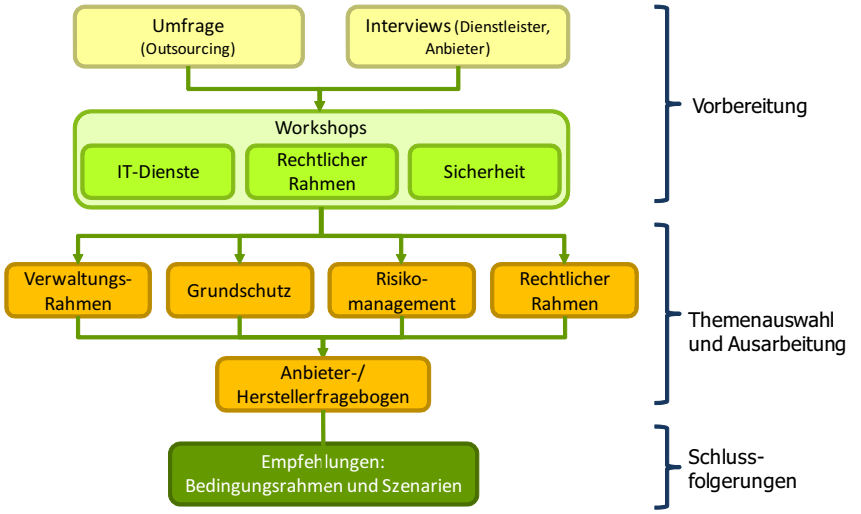


Abbildung 1.1
Vorgehensweise.

- **Verwaltungrahmen**. Welche Governance-Aspekte sind im Zusammenhang mit Cloud-Computing besonders zu beachten?

- **Rechtliche Rahmenbedingungen**. Dieses Thema wird — da er bereits in parallel laufenden Arbeiten in der notwendigen Tiefe behandelt wird — an dieser Stelle nur angeschnitten. Insbesondere im Bereich Datenschutz werden rechtliche Vorgaben im Sinne einer Begriffsbildung behandelt, die für die folgenden Betrachtungen notwendig ist.

Sicherheitsaspekte nehmen notwendigerweise einen breiten Raum in unserer Studie ein, ist doch »Sicherheit in der Cloud« eines der Themen, das die aktuelle Diskussion am meisten bewegen. Wir nähern uns diesem Komplex aus verschiedenen Richtungen:

- **Cloud-Risiken**. Um eine Grundlage zur Strukturierung der aktuellen meist undifferenzierten Diskussion zu schaffen, führen wir zunächst den Begriff der Cloud-spezifischen Gefährdung ein. Es zeigt sich, dass dieser Begriff gut in verschiedene Kategorien aufteilbar ist, die verdeutlichen, welche Gefahren aus der Anwendung bereits bekannter und etablierter Technologien erwachsen und welche tatsächlich mit dem Einsatz von Cloud-Technologien neu hinzukommen.

- **Grundschutz: Outsourcing und Datenschutz**. Wie kann Cloud-Computing aus der heutigen Sicht des öffentlichen Sektors betrachtet werden? Sicher bestehen berechtigte datenschutzrechtliche Bedenken, aber auf welche Aspekte des Cloud-Computing beziehen sich diese genau? Outsourcing in die Cloud wird häufig abgelehnt, aber aufgrund welcher konkreten Bedenken? Welches Raster — außer dem einer generellen Zustimmung (»die Cloud reduziert Verwaltungsaufwände«) oder Ablehnung (»Daten sind in der Cloud nicht sicher«) — ist bei der Bewertung von Cloud-Computing Angeboten anzuwenden?

Als etablierter **Rahmen** zur Bewertung von IT-Systemen gelten die Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese Kataloge stellen eine detaillierte Auflistung konkreter Gefährdungen und entsprechender Maßnahmen dar, die bei einer Zertifizierung (etwa nach (ISO, 2008)) zu beachten bzw. zu implementieren sind. Für Verwaltungen stellen die Kataloge ein Raster dar, mit deren Hilfe z. B. das Angebot eines externen Dienstleisters bewertet werden kann. In dieser Studie verwenden wir die Grundschutzkataloge ebenfalls als »Benchmark«-Test, um Cloud-Computing zu bewerten.

Was aber ist dabei unser **Vergleichsgegenstand**, unsere »*Baseline*«? Outsourcing von IT-Diensten ist eine lang etablierte Praxis. Daten- und Rechenzentren werden von vielen Behörden zur Verwaltung ihrer IT-Systemlandschaften, zum Betrieb von Fachverfahren und für Entwicklungs- und Testaufgaben herangezogen. Wie sich zeigt, weisen viele dieser Dienstleister bereits einzelne Charakteristiken von Cloud-Anbietern auf, ohne allerdings den Schritt zu einem »vollständigen« Cloud-Angebot vollzogen zu haben. Wir definieren als Vergleichsgegenstand deshalb einen »klassischen Dienstleister«, der im Extremfall keine der relevanten Eigenschaften eines Cloud-Anbieters aufweist. Natürlich ist dies als methodologisches Konstrukt zu verstehen und soll weder mit einem konkreten Anbieter noch als Beschreibung des augenblicklichen »*State of the Art*« verwechselt werden.

- **Mindestanforderungen an Cloud-Anbieter**. Vor kurzem wurde durch das BSI ein Eckpunktpapier[2] veröffentlicht, das einen ersten Ansatz zur Bestimmung von Sicherheitsanforderungen an Cloud-Anbieter darstellt und somit den augenblicklichen Stand der Diskussion in diesem Bereich zusammenfasst; dabei werden im wesentlichen nur solche Anforderungen untersucht, die Cloud-Computing von herkömmlichen Technologien unterscheidet; somit repräsentieren die hier angeschnittenen Aspekte das »Delta«, das beim Einsatz von Cloud-Technologien noch zu beachten ist.

- Schließlich wurde ein weiterer **Fragebogen** erstellt, um die Position von Anbietern von Cloud-Dienstleistungen und den Herstellern diesbezüglicher Technologien bzgl. einiger Fragestellungen, die in den vorhergehenden Abschnitten als relevant identifiziert wurden, zu ermitteln — allerdings wurde hier wegen der Komplexität und Breite des Themas nicht versucht, einen umfassenden Ansatz umzusetzen.

Schließlich konnten ausgehend von den oben genannten Themen sowohl Rahmenbedingungen für den Einsatz von Cloud-Technologien wie auch mögliche Ausgestaltungsszenarien identifiziert werden, die als Empfehlungen das Fazit der Studie darstellen.

[2] (BSI, 2010b)

1.2 Zusammenfassung der Ergebnisse

In diesem Abschnitt werden die Ergebnisse der Studie zusammengefasst. Entsprechende Erläuterungen finden sich jeweils am Anfang der jeweiligen Kapitel.

- **Definition**: Diese Studie setzt auf dem Begriff des Cloud-Computing auf, wie er durch das *National Institute of Standards and Technology* (NIST)[3] vertreten wird. Dabei werden eine Reihe von Eigenschaften, die Cloud-Systeme charakterisieren, bestimmt: Automatisierte Diensterbringung auf Anforderung, netzwerkbasierter Realzeitzugang, Ressourcen-Pooling, schnelle Elastizität sowie messbare Dienstqualität. Die Dienstklassen »Software als Dienst«, »Plattform als Dienst« und »Infrastruktur als Dienst« werden unterschieden. Schließlich werden verschiedene Betriebsmodelle klassifiziert: Private, öffentliche, Communty- und hybride Clouds. Aus den Cloud-Eigenschaften lassen sich eine Reihe von Merkmalen herleiten, die einen »klassischen Anbieter« von einem Cloud-Anbieter unterscheiden.

  Dieser Teil der Studie versteht sich auch als Zusammenfassung der **Potentiale des Cloud-Computing**. Insbesondere in folgenden Teilen, in denen es um Risiken des Cloud-Computing und ihre Beherrschbarkeit geht, werden wir vielfach auf die Vorteile des Cloud-Computing verweisen.

- **Umfrage**: Als Vorbereitung für die vorliegende Studie wurde ein Fragebogen mit dem Thema »Auslagerung von IT-Dienstleistungen« erstellt, dessen Ergebnisse die Formulierung einer Reihe von vorläufigen Annahmen als Arbeitshypothesen ermöglichen.

  1. Die Auslagerung von Diensten an externe IT-Anbieter ist heute bereits Stand der Technik.
  2. Behörden stehen IT-Kooperationen grundsätzlich positiv gegenüber.
  3. Insbesondere Fachverfahren und Infrastruktur-Dienste sind für eine Auslagerung geeignet. Im Gegensatz dazu werden Plattform-Dienste nur selten ausgelagert. Verfügbarkeit wird als wesentliche Anforderung an Dienstleistungen genannt.
  4. Virtualisierung, eine der Basis-Technologien des Cloud-Computing, wird heute bereits vielfach eingesetzt.

- **Governance-Bezugrahmen**: Zur Identifikation der relevanten Faktoren, die die Nutzung von Cloud-Computing durch die öffentliche Verwaltung bestimmen, setzen wir die Cloud-Eigenschaften Ressourcen-Pooling, virtuelle Bereitstellung und Netzwerkzugang zu vier Bestimmungsfaktor-Gruppen in Beziehung, nämlich »rechtliche Zulässigkeit«, »(wirtschaftliche) Vorteilhaftigkeit«, »Steuerbarkeit« und »Risikobeherrschbarkeit«.

[3] (Mell u. Grance, 2009)

1. Rechtliche Zulässigkeit: Virtualisierung und netzwerkbasierter Zugang verändert die Besitz- und Berechtigungsstrukturen von Leistungserstellungsprozessen sowie von Datenbeständen, woraus verfahrensrechtlich Unsicherheitsräume oder Nichtanwendbarkeitsschwierigkeiten entstehen, die berücksichtigt werden müssen. Besonders zu prüfen ist, ob diese Schwierigkeiten im Rahmen von »*Service Level Agreements*« (SLAs) hinreichend regelbar sind. Rahmenrechtlich ergeben sich neben datenschutzrechtlichen Problemen insbesondere auch vergaberechtliche Fragen, die im Kern wiederum auf den Regelungsbedarf und die Regelungsmöglichkeiten mit dem Instrument SLA hinauslaufen.
2. (Wirtschaftliche) Vorteilhaftigkeit: Während grundsätzliche Effizienzprüfungen für Cloud-Ansätze kaum unterschiedlich zur Bewertung anderer Bündelungsformen stattfinden dürften, ergibt sich aus dem Definitionsmerkmal »virtuell« und dem organisatorischen Merkmal »Kompetenzbündelung« die spezielle Frage, inwieweit die Nutzung von Cloud-Computing-Ansätzen zu grundlegend veränderten behördlichen Zuschnitten und Paradigmen führen.
3. Steuerbarkeit: Das virtuelle und mit »remote«-Zugriff ausgestattete Cloud-Computing wirft grundlegend die Frage auf, ob und wie hier überhaupt noch eine Steuerbarkeit durch die verantwortliche Behörde gewährleistet werden kann.
4. Risikobeherrschbarkeit: Hier ergeben sich insbesondere rechtliche Risikofragestellungen in Bezug auf Nachvollziehbarkeit.

Insgesamt wird deutlich, dass die Fragestellung des Cloud Computing in der öffentlichen Verwaltung im Wesentlichen eine »Risikofragestellung« ist. Wirtschaftlichkeit spielt nur eine untergeordnete Rolle.

- **Rechtliche Rahmenbedingungen**. Im Bereich der öffentlichen Verwaltung gibt es erhebliche Bedenken gegenüber Cloud-Computing. Diese sind einerseits darin begründet, dass besonders öffentliche Verwaltungen prinzipiell eine Schutzpflicht für personenbezogene Daten haben. Aber auch grundsätzliche Betrachtungen lassen Behörden vor der Auslagerung von Prozessen in die Cloud zurückschrecken. Einerseits ist hier die Angst vor dem Verlust von Know-how zu nennen. Weiterhin müssen bestimmte Kernaufgaben in der Verwaltung bleiben.

  Da es sich bei Cloud-Computing um eine Art von »Outsourcing« handelt, können eine Reihe von rechtlichen Fragen in diesem Zusammenhang beantwortet werden. Da es sich beim Cloud-Computing aber auch um Kooperation — innerhalb und zwischen Verwaltungen (und Privatwirtschaft) — handelt, spielen auch hier Fragen der Kooperationsform eine Rolle, die über gesetzliche Einschränkungen hinausgehen und durchaus Anlass für neue Fragestellungen sind.

- **Risiko-Management**: Um den Begriff »Cloud-spezifisches Risiko« besser eingrenzen zu können, verwenden wir die folgende Klassifi-

kation von Schwachstellen in Cloud-Systemen: Solche Schwachstellen sind *Cloud-spezifisch*, wenn

1. sie immanenter Bestandteil oder weit verbreitet in den Cloud-Basis-Technologien sind, oder
2. durch Cloud-Innovationen verursacht werden, die bekannte und erprobte Gegenmaßnahmen unmöglich oder schwierig implementierbar machen, oder
3. ihren Ursprung in einer der Charakteristiken des Cloud-Computings haben.

Unabhängig davon gibt es eine Reihe von Argumenten dafür, dass das Sicherheitsniveau in Cloud-Infrastrukturen deutlich gesteigert werden kann:

- Skalierungseffekte sorgen dafür, dass Systeme weniger angreifbar sind und dass Sicherheitsrichtlinien einfacher durchgesetzt werden können.
- Sicherheit kann zu einem Marktfaktor werden, der zur Entwicklung robusterer Dienste wie auch zur stringenten Implementierung von Sicherheitsmanagementsystemen führen kann.
- Schließlich können einige Sicherheitsfunktionen selbst als Cloud-Dienst angeboten werden.

Im Folgenden betrachten wir im wesentlichen drei Cloud-Betriebsmodelle, nämlich erstens die »private Cloud«, die in etwa dem einer Behörde (oder mehreren Behörden) zugeordneten Daten- oder Rechenzentrum entspricht, das exklusiv für diesen Kundenkreis Dienstleistungen erbringt, zweitens die »Community-Cloud«, die einen Zusammenschluss derartiger Rechenzentren zu einer föderierten, kooperativen Dienstleistungsstruktur darstellt, und drittens die öffentliche Cloud, die neben behördlichen auch private (bzw. privatwirtschaftliche) Kunden akzeptiert und für die Verträge oft kurzfristig und unter Verwendung minimaler Identitätszusicherungen abgeschlossen werden.

- **Outsourcing**: Im Vergleich zu klassischen IT-Dienstleistern ergibt sich für private Clouds ein grundsätzlich positives Gesamtbild bzgl. Sicherheitsfragestellungen, die mit Outsourcing verbunden sind. Das einzige offensichtliche Problem ist das Fehlen von Interoperabilitätsstandards, so dass Insourcing oder ein Wechsel des Dienstleisters zu einem Problem werden kann. Ein ähnliches Bild ergibt sich für Community-Cloud, wobei es hier aufgrund des Umstandes, dass die an der »Community« beteiligten Rechenzentren unterschiedliche Verwaltungsdomänen mit u. U. unterschiedlichen Richtlinien definieren, zu weiteren Schwierigkeiten kommen kann. Insgesamt ist hier ein integriertes, kollaboratives Management von Cloud-Diensten erforderlich, für das zurzeit wenige oder keine Ansätze existieren.

  Hingegen kommen aus der Sicherheitsperspektive Anbieter öffentlicher Clouds als Kooperationspartner für Behörden nur bedingt in

Frage. Ein Hauptproblem ist, dass der Kundenstamm eines Anbieters einer öffentlichen Cloud nicht a-priori bekannt ist: Jeder, insbesondere auch eine Person mit böswilligen Absichten, kann u. U. Zugang zu ggf. kritischen Systemteilen erlangen.

- **Datenschutz**. Ähnlich wie bei der Untersuchung des Outsourcing kommen wir zu dem Schluss, dass private und — wiederum mit Einschränkungen — Community-Clouds valide Modelle für öffentlich-öffentliche Kooperationen sind. Wiederum schneiden öffentliche Clouds im Vergleich zu klassischen Anbietern schlecht ab. Die Gründe hierfür liegen einerseits in dem Aufgabenprofil öffentlicher Clouds, das nicht notwendigerweise auf den Umgang mit personenbezogenen Daten abgestimmt ist, andererseits in mangelnder Transparenz, da für den Auftraggeber umfassende Informationen über die Systeme und Prozesse des Dienstanbieters und ggf. Eingriffe in diese erforderlich sind.

- **Anforderungen an Cloud-Anbieter**. Betrachtet man Mindestsicherheitsanforderungen an Anbieter, die Cloud-Technologien verwenden, ergibt sich für private und Community-Clouds ein deutliches Potential zur Erfüllung dieser Anforderungen, das sich aus den Cloud-Eigenschaften in Verbindung mit dem spezifischen Betriebsmodell ergibt. Für öffentliche Clouds ist dieses Potential in vielen Punkten nicht unmittelbar erkennbar — hier ist eine gesonderte Analyse des jeweiligen konkreten Angebots vorzunehmen.

- **Anbieter- und Herstellerposition.** Einige der in dieser Studie aufgeworfenen Fragen sowie — um den konkreten Stand der Technik zumindest in einigen Bereichen zu ermitteln — allgemeine Fragen zum Cloud-Computing wurden in einem weiteren Fragebogen zusammengefasst und an zwei Cloud-Dienstanbieter sowie einen Hersteller von Cloud-Technologien versandt. Aus den Antworten lässt sich schließen, dass die Idee der Cloud in vielen Aspekten bereits den konkreten Angeboten entspricht. Insbesondere bestehen vielfältige Ansätze für ein integriertes System- und Dienstmanagement. Migration und Portierung von Daten und Anwendungen in bzw. für die Cloud wird durch entsprechende Werkzeuge unterstützt. Datenschutz und Sicherheit wird als Anforderung erkannt. Allerdings wird die geforderte enge Zusammenarbeit zwischen Anbieter und Auftraggeber bei Outsourcing-Projekten zur Erstellung gemeinsamer Sicherheitskonzepte nicht oder nur in Ansätzen reflektiert. Auch sind datenschutzbezogene Fragen bzgl. der Transparenz interner Vorgänge zu klären.

- **Bedingungsrahmen für die Migration in die Cloud**. Es wurden drei wesentliche Bedingungen für die Inanspruchnahme von Cloud-Angeboten erarbeitet, nämlich:

  - Die Verfügbarkeit standardisierter und bereits an anderer Stelle auf Rechtssicherheit geprüfter SLA-Konstrukte für Cloud-Migrationen stellt in erster Linie eine Entlastung der Entscheidungsträger in den einzelnen Behörden dar, die den »Sonderfall« der Cloud-Migration in gängige Praxis verwandeln können.

- Weiterhin wird die Erarbeitung spezieller verfahrensrechtlicher Regelungen und Richtlinien für Cloud-Computing als positive gesetzgeberische Spezifikationen für die IT-technische Auslagerung vorgeschlagen, die als konkrete Handlungsanweisungen für Entscheider vor allem Rechtssicherheit herstellen.
- Externe Anbieterzertifizierung und -aufsicht für Cloud-Anbieter, d. h. ein gesondertes Prüf-, Anerkennungs- und Aufsichtsverfahren, das an dieser Stelle insbesondere für öffentliche Cloud-Anbieter Gültigkeit hätte.

- **Ausgestaltungsszenarien**: Abschließend wird präzisiert, wie Clouds im Einzelnen für Verwaltungen nutzbar gemacht werden können und wo die Probleme bei der Umsetzung derartiger Ausgestaltungsvarianten sind. Wir betrachten zunächst private Clouds, die sich unmittelbar als Umsetzungsszenario anbieten. Community-Clouds sind nicht unmittelbar verwendbar, wobei allerdings zu erwartende Konsolidierungseffekte und Kompetenzbündellungen, die auch die Sicherheit und Beherrschbarkeit solcher Strukturen erhöhen, einen unmittelbaren Anreiz zur Umsetzung solcher Modelle bilden. Wir betrachten hier insbesondere zwei Modellierungsansätze: Einerseits einen übergreifenden Ansatz, der auf der gemeinschaftlichen Erbringung von Dienstleistungen durch die beteiligten Rechenzentren beruht, und andererseits einen Kompetenz-basierten Ansatz, in dem Community-Clouds als Zusammenschluss von Kompetenzzentren aufgefasst werden.

  Schließlich betrachten wir auch die Einbeziehung von öffentlichen Cloud-Anbietern bzw. hybride Ausgestaltungsmodelle mit öffentlichem Cloud-Anteil. Wenn datenschutzrechtliche Fragestellungen unberührt bleiben, stellen solche Modelle u. U. einen gangbaren Weg zur Umsetzung öffentlich-privater Partnerschaften dar.

1.3 Dokumentengliederung

Diese Studie gliedert sich in vier Teile:

- Teil I befasst sich mit dem augenblicklichen Stand der Diskussion. In Kapitel I.1 wird zunächst der Begriff des Cloud-Computing definiert. Weiterhin werden Charakteristiken von Cloud-Anbietern abgeleitet. Kapitel I.2 fasst die Ergebnisse einer Umfrage zum Thema Outsourcing zusammen.
- Teil II befasst sich mit Rahmenbedingungen. In Kapitel II.1 wird ein Governance-Bezugsrahmen erarbeitet. Kapitel II.2 befasst sich mit spezifischen rechtlichen Rahmenbedingungen insbesondere zum Datenschutz und zur Datensicherheit.
- In Teil III schließlich wird eine Risikoanalyse des Cloud-Computing vorgenommen. Nachdem der Risikobegriff in Kapitel III.1 für das Cloud-Computing präzisiert wurde, werden in den Kapiteln III.2

und III.3 Sicherheitsaspekte betrachtet, die sich auf das Outsourcing von Diensten und Funktionen in die Cloud sowie auf datenschutzrechtliche Anforderungen beziehen. Allgemeine Sicherheitsanforderungen an Cloud-Anbieter werden in Kapitel III.4 diskutiert. Schließlich werden in Kapitel III.5 die Ergebnisse der Anbieter- bzw. Herstellerumfrage thematisiert.

- Der abschließende Teil IV befasst sich zunächst in Kapitel IV.1 mit den Rahmenbedingungen für eine Umsetzung von Cloud-Computing als Dienstleistungsmodell für die Verwaltungen. Kapitel IV.2 schließlich diskutiert konkrete Umsetzungsszenarien. Kapitel IV.3 gibt neben einer kurzen Zusammenfassung einen Ausblick auf Themen, die Ausgangspunkte für weitere Arbeiten darstellen.

Weiterhin ist umfangreiches Hintergrundmaterial in verschiedenen Anhängen verfügbar:

- Anhang A enhält ein Kompendium an Meinungen und Ansichten zum Begriff Cloud-Computing, die aus verschiedenen Quellen zusammengestellt sind und die die Notwendigkeit unterstreichen, eine einheitliche Definition dieses Begriffs zu finden.
- Anhang B enthält die vollständige Auswertung der Umfrage.
- Anhang C gibt die Antworten der an die Anbieter und Hersteller gerichteten Fragen anonymisiert wider.
- Anhang D diskutiert Begriffe wie »Risiko« und »Schwachstelle« und erläutert exemplarisch einen Risikomanagementprozess.
- Anhang E erläutert den Aufbau der BSI-Grundschutzkataloge.

Teil I

Stand der Diskussion

KAPITEL I.1

Bestandsaufnahme — Was ist Cloud-Computing?

Zusammenfassung

Diese Studie setzt auf dem Begriff des Cloud-Computing auf, wie er durch das NIST vertreten wird. Dieser Begriff wird mittlerweile auch von anderen Autoren als »die« relevante Definition anerkannt. Dabei werden eine Reihe von Eigenschaften, die Cloud-Systeme charakterisieren, bestimmt: Automatisierte Diensterbringung auf Anforderung, netzwerkbasierter Realzeitzugang, Ressourcen-Pooling, schnelle Elastizität sowie messbare Dienstqualität. Die Dienstklassen »Software als Dienst«, »Plattform als Dienst« und »Infrastruktur als Dienst« werden unterschieden. Schließlich werden verschiedene Betriebsmodelle bestimmt: Private, öffentliche, Community- und hybride Clouds.

Aus den Cloud-Eigenschaften lassen sich eine Reihe von Merkmalen herleiten, die einen »klassischen Anbieter« (im Sinne eines abstrakten, methodologischen Konstrukts) von einem Cloud-Anbieter (der nicht weniger abstrakt als Anbieter definiert ist, der alle Cloud-Merkmale vollständig implementiert) unterscheiden. Diese Trennung wird in den Kapiteln III.2 und III.3 verwendet, um Cloud-Computing bzgl. heute gültiger Standards zu bewerten.

I.1.1 Orientierung

Was ist Cloud-Computing? Andy Isherwood, Hewlett-Packard's Vizepresident für »European Software Sales«, äußert in einem Interview die Ansicht:

> *A lot of people are jumping on the [cloud] bandwagon, but I have not heard two people say the same thing about it. There are multiple definitions out there of «the cloud».*[1]

Cisco CEO Larry Elison wählt deutlichere Worte:

> *The interesting thing about Cloud Computing is that we've redefined Cloud Computing to include everything that we already do . . . I don't understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads.*[2]

Experten sind sich uneinig, wie der Begriff »Cloud-Computing« zu definieren ist.

Tatsächlich finden sich in den einschlägigen Online-Zeitschriften, Blogs und verschiedenen Artikeln eine ganze Reihe von Ansichten zum Begriff »Cloud-Computing«. So veröffentlichte das »Cloud Computing Journal« Anfang 2009 einen Artikel[3] mit 21 Expertenmeinungen zu diesem Thema. Ein anderer Blog[4] bringt es auf weitere 18 Ansichten.[5]

So zeigen sich industrielle Entscheidungsträger, Wissenschaftler und Verwaltungsexperten gleichermaßen verwirrt darüber, was mit Cloud-Computing eigentlich gemeint ist. Eine genaue Analyse der vorhandenen Definitionsversuche ergibt jedoch ein kohärentes Bild, da verschiedene Eigenschaften und Anforderungen wiederholt genannt werden. Fest steht, dass Cloud-Computing nicht als neue Technologie oder Funktionsangebot verstanden werden kann, sondern heute bereits verfügbare Technologien in konsolidierter Form wie Virtualisierung, Grid- und Utility-Computing und WEB 2.0, nutzbar macht und damit die Erstellung und Angebot einer breiten Funktionspalette erlaubt.

Zusammenfassung der hier verwendeten Definition des »Cloud-Computings«.

Für diese Studie verwenden wir die in den folgenden Abschnitten I.1.2–I.1.5 detailliert Definition[6], die sich wie folgt zusammenfassen lässt:

> *Clouds bestehen aus institutionsübergreifenden Pools von Ressourcen wie etwa Hardware, Entwicklungsplattformen und elektronischen Diensten. Diese Ressourcen werden virtualisiert zur Verfügung gestellt und können dynamisch konfiguriert und damit elastisch an aktuelle Anforderungen (anfallende Lastbedingungen oder Dienstkombinationen) angepasst bzw. skaliert werden, wodurch eine optimierte Ressourcennutzung ermöglicht wird. Der Zugang zu diesen Ressourcen erfolgt »remote« etwa über das Internet. Dabei können Ressourcenanbieter und -nutzer organisatorisch getrennt sein.*
>
> *Zusammenfassend ist Cloud Computing ein Modell, das »on-demand« und Online den Zugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen wie Netzwerke, Server, Speichersysteme, Anwendungen und Dienste ermöglicht. Diese kön-*

[1] Andy Isherwood, zitiert nach ZDnet News, 11.12.2008

[2] Larry Ellison, zitiert nach Wall Street Journal, September 26, 2008

[3] http://cloudcomputing.sys-con.com/node/612375

[4] http://jameskaskade.com/?p=594

[5] Eine Zusammenstellung verschiedener Meinungen darüber, was Cloud-Computing eigentlich ist, findet sich in Anhang A.

[6] Diese Definition ist (Vaquero u. a., 2009) entnommen und leicht abgewandelt worden, um die organisatorische Trennung von Ressourcennutzung und -verwaltung stärker zu betonen.

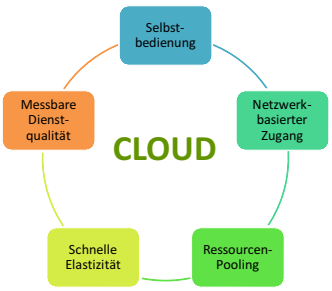


Abbildung I.1.1
Cloud-Eigenschaften nach (Mell u. Grance, 2009).

nen passgenau, schnell, kostengünstig und mit minimalem Verwaltungsaufwand bereitgestellt und abgerufen werden.

Organisationen, die Cloud-Ressourcen nutzen, sind selbst also nicht oder nur zum Teil mit der Verwaltung der Ressourcen beschäftigt; diese Aktivitäten finden beim Ressourcenanbieter statt. Für die Nutzerorganisation entfällt dadurch die Notwendigkeit, eigene Infrastruktur, Dienstplattformen und Dienste anzuschaffen und zu unterhalten. Es werden Geschäftsmodelle möglich, die Ressourcen auf Nutzungsbasis anbieten und abrechnen bzw. ihren Wert einschätzen.

Definition des NIST.

In den USA hat das *Nationale Institut für Standards und Technologie* (NIST) eine allgemeine Definition des Cloud-Computings erstellt, die häufig zitiert wird und eine geeignete Basis für eine präzisere Begriffsbestimmung bietet.

I.1.2 Eigenschaften

Das NIST bestimmt zunächst eine Reihe von Eigenschaften, die das Konzept »Cloud-Computing« begrifflich umreißen, die hier leicht gekürzt und den Anforderungen dieser Studie entsprechend wiedergegeben werden:

I.1.2.1 Automatische Diensterbringung auf Anforderung

Selbstbedienung in der Cloud.

Nutzer sind in der Lage, selbstständig Dienste und Ressourcen anzufordern, ohne dass eine Interaktion mit menschlichen Operatoren auf Seiten des Anbieters notwendig wird.

I.1.2.2 Netzwerkbasierter Real-Zeit-Zugang

Cloud-Dienste werden über ein Neztwerk bezogen.

Auf Ressourcen und Dienste kann in Echtzeit netzwerkbasiert unter Verwendung von Standardtechnologien (Internet, dedizierte Netzwerke, »*Virtual Private Networks*«, etc.) zugegriffen werden.[7] Auf der Seite des

[7] In der Literatur wird häufig angegeben, dass der Zugang zur Cloud über das (öffentlichen) Internet erfolgt. Um in dieser Studie auch den Einsatz von Cloud-Technologien in Rechenzentren untersuchen zu können, die über dedizierte (vom Internet isolierte) Netzwerke verfügen, verwenden wir hier eine umfassendere Definition.

Klienten können Geräte wie PCs, Laptops, Mobiltelefone oder PDAs eingesetzt werden.

I.1.2.3 Ressourcen-Pooling

Ressourcen-Pools abstrahieren von konkreten Servern, Netzwerken, uws.

Die Ressourcen des Anbieters sind in Pools konsolidiert, die eine parallele Diensterbringung für multiple Nutzer erlaubt. Die Zuordnung von Ressourcen an Kunden geschieht dynamisch und in einer dem aktuellen Bedarf des Kunden angepassten Weise.

I.1.2.4 Schnelle Elastizität

Elastizität vermittelt die Illusion unbegrenzter Ressourcen.

Ressourcen und Dienste werden »elastisch« zur Verfügung gestellt, d. h. entsprechend seines augenblicklichen Bedarfs erhält der Benutzer innerhalb eines gering bemessenen Zeitrahmens Ressourcen in adäquaten Quantitäten. Für den Nutzer entsteht dadurch die Illusion, dass Ressourcen in unbeschränkten Quantitäten zur Verfügung stünden.

I.1.2.5 Messbare Dienstequalität

Messbarkeit ist ein integrales von Cloud-Diensten.

Cloud-Systeme verfügen über eingebaute Monitoring- und Messfunktionen, die sowohl eine optimierte Ressourcen-Nutzung wie auch eine Validation der erreichten Dienstqualität seitens des Nutzers erlaubt.

I.1.3 Dienstklassen

Prominente Anbieter wie Amazon, Google, SUN, Microsoft, IBM, Oracle, Salesforce.com etc. erweitern ständig ihre Cloud-Computing Dienstleistungen und bieten kategorisierte Dienstleistungen für Infrastruktur, Datenbank, Geschäftsprozessmanagement, Handelsplattformen, Abrechnung, Buchhaltung, Email, Datenaustausch, Datenverarbeitung und Web Services an. Dabei wird zwischen verschiedenen Klassen von Dienstleistungen unterschieden, die sich nach dem Grad ihrer Spezialisierung anordnen lassen: Software als Dienst (software-as-a-service, SaaS), Plattform als Dienst (platform-as-a-service, PaaS) und Infrastruktur als Dienst (infrastucture-as-a-service, IaaS). Tab. I.1.1 gibt einen Überblick über die folgende Diskussion der verschiedenen Klassen von Cloud-Diensten.

I.1.3.1 SaaS: Software als Dienst

SaaS: Anwendungen über das Internet.

Das Angebot des Anbieters besteht in Anwendungen, d. h. der Nutzer kann »remote« auf Software zugreifen, die auf den Servern des Anbieters läuft. Die Nutzung der Anwendungen durch den Kunden wird vertraglich geregelt und beinhaltet die benötigten Hard- und Software Lizenzen sowie Vereinbarungen über die Wartung und den Betrieb der angebotenen Software. Die Administration der Software und der darunterliegenden Cloud-Infrastruktur, des Netzwerks, der Server, der Betriebssysteme

Klasse	Beschreibung	Beispiele
SaaS	Zugang zu Anwendungen	Google Apps, Microsoft CRM online Salesforce.com, WebEx
PaaS	Entwicklungs- und Laufzeitumgebungen zur Bereitstellung und Ausführung eigener Anwendungen	Force.com, Google-App Engine, Microsoft Azure
IaaS	Virtualisierte Rechnerressourcen, Speicher, Netzwerk, etc.	Amazon EC2+ S3, AppNexus, HP Cloud Enabling Computing, Oracle, IBM, Sun Microsystems, Hadoop

Tabelle I.1.1
Klassen von Cloud-Diensten.

und des Speichers obliegt dem Cloud-Anbieter. Der Kunde muss hierfür keine Ressourcen aufwenden. Auch Upgrades und Updates werden durch den Anbieter vorgenommen. Allerdings muss sich der Kunde in der Regel mit einer Standardlösung zufrieden geben, individuelle Anpassungen an Kundenbedürfnisse sind bei den zurzeit angebotenen Lösungen ohne weiteres nicht möglich. Die bekanntesten Beispiele in dieser Dienstklasse sind:

Beispiele für SaaS-Anbieter.

- Goggle bietet mit Google Apps Office-Anwendungen wie Textverarbeitung, Tabellenkalkulation, Email oder Kalenderanwendungen an, die über einen Webbrowser bezogen werden können.
- SAP, das seine Geschäftslösung Business ByDesign über das Internet gegen eine monatliche Gebühr pro Benutzer anbietet

I.1.3.2 PaaS: Plattform als Dienst

PaaS: Laufzeit- und Entwicklungsumgebungen.

PaaS bietet dem Cloud-Kunden die Möglichkeit, eigene Anwendungen innerhalb einer Entwicklungsumgebung zu erstellen und in den durch den Cloud-Anbieter zur Verfügung gestellten Laufzeitumgebungen auszuführen. Auch hier werden alle Administrationsaufgaben durch den Anbieter wahrgenommen. Anders als bei SaaS hat der Kunde hier allerdings die Kontrolle über die Anwendung, da er sie selbst entwickelt und konfiguriert hat.

Zwei wesentliche Dienstleistungen werden als PaaS angeboten: Entwicklungsplattformen und betriebliche Plattformen. Die Entwicklungsplattformen bieten Entwicklern die Möglichkeit, Anwendungen zu entwickeln und ihren Code in der Cloud ausführen zu lassen. Entsprechende Werkzeuge und Entwicklungsframeworks werden vom Anbieter bereitgestellt. Beispiel für eine Anwendungsplattform in der Cloud sind:

Beispiele für PaaS-Anbieter.

- Die Google App Engine.
- Salesforce.com bietet eine betriebliche Plattform für die Entwicklung, Verwaltung und den Einsatz von maßgeschneiderten Geschäftsanwendungen an.

I.1.3.3 IaaS: Infrastruktur als Dienst

IaaS: Rechenleistung, Speicherplatz, Netzwerk.

In dieser Variante stellt der Anbieter Speicher, Netzwerkzugang und sowie Rechenleistungen zur Verfügung, so dass der Kunde die Möglichkeit hat, eigene Software auf nativen Plattformen (die jedoch vom Anbieter virtualisiert werden) auszuführen. Der Kunde kann auch ein bevorzugtes Betriebssystem in die Cloud einbringen. Für den Kunden entsteht dadurch die Illusion, über einen Pool oder ein Netzwerk von physikalischen Maschinen zu verfügen. Wie bei den zuvor beschriebenen Cloud-Diensten muss der Kunde die virtualisierte Infrastruktur nicht verwalten. Allerdings hat er hier die Kontrolle über das Betriebssystem, den Speicher, und die eigene Anwendungen und kann zusätzliche Netzkomponenten wie Firewalls und Lastverteiler einbringen.

IaaS ist vor allen Dingen für hochskalierte Anwendungen von Vorteil, die massive Rechenleistung in Form großer »Serverfarmen« benötigen. Eine weitere Anwendung ist die Durchführung von Skalierbarkeits- und Performanztests großer IT-Systeme. Die Ressourcen für solche Tests können kostengünstig und flexibel aus der Cloud bezogen werden und müssen nicht in Form spezifischer Hardware vorhanden sein oder langfristig aufrecht erhalten werden.

Zurzeit werden Infrastrukturdienste in zwei Formen angeboten, einerseits als Bereitstellung von Speichermöglichkeit und andererseits als Rechenleistung auf Basis virtueller Infrastrukturen.

Beispiel für einen IaaS-Anbieter.

- Amazon bietet zum Beispiel die Elastic Computing Cloud (EC2) als Dienst für Rechenleistung an und den Simple Storage Service (S3) als Speicherdienst.

I.1.4 Dienstverträge

Die Art und Weise, in der Cloud-Dienste genutzt werden können, wird in Dienstleistungsverträgen, den sogenannten »Service Level Agreements« (SLAs) festgelegt und ist abhängig von der Beziehung zwischen Kunden und Cloud-Dienstanbieter. Beispiele für Themenbereiche, die in Dienstverträgen behandelt werden können, sind:

I.1.4.1 Datenschutz

Datenschutz ist ein wesentliches Element in Dienstverträgen, wenn personenbezogene Daten erhoben, gespeichert, verarbeitet oder übermittelt werden.

Datenschutz umfasst eine Definition des Personenkreises, der auf spezifische Daten zugreifen darf sowie die Art und Weise, in der die Einhaltung einer Zugriffsberechtigung sichergestellt wird. Fragen in diesem Zusammenhang sind:

- Wie werden Daten verschlüsselt?
- Welche Abstufungen von Zugangsberechtigungen gibt es?
- Dürfen Daten ausgelagert und durch Dritte bearbeitet werden?
- Wo werden Sicherheitskopien schutzwürdiger Daten gespeichert?

- In welcher Weise sind beteiligte Datenzentren gegen Angriffe abgesichert?
- Was geschieht, wenn Verträge neu vergeben werden?
- Wie sind die Prozesse definiert, mit denen Kundennachfragen oder -beschwerden zur Datensicherheit behandelt werden?
- Wie oft werden Audits durchgeführt und welche Werkzeuge kommen dabei zum Einsatz?
- Wie wird die Löschung von Daten behandelt?

I.1.4.2 Verfügbarkeit

adressiert die Erreichbarkeit von Dienstleistungen beziehungsweise Maßnahmen im Falle eines Ausfalls. In diesem Zusammenhang sind die folgenden Fragen von Bedeutung:

Was geschieht, wenn ein Dienst ausfällt?

- Wie genau ist der Ausfall von Diensten definiert? Sieht der Anbieter die vorübergehende Abschaltung von Diensten zu Wartungszwecken vor?
- Gibt es im Falle der vorübergehenden oder permanenten Nichterreichbarkeit einen alternativen Anbieter, der die entstehende Arbeitslast übernimmt?
- Wie kann die Schwere eines Dienstausfalls bemessen werden? Stehen hierfür Werkzeuge oder Prozeduren zur Verfügung?
- Wie wird der Kunde für Einbußen, die durch einen Dienstausfall entstehen, kompensiert?
- Wird der Grad der Redundanz geregelt, die der Anbieter aufbringt, um Ausfallzeiten zu vermeiden?

I.1.4.3 Kosten

Wichtig ist u. a.:

Welches Tarifmodell wird verwendet?

- Welches Abrechnungsmodell wird verwendet (basierend auf Nutzung, Verkehr, Speicher usw.)?
- Wie werden Steuern und externe Kosten wie etwa Lizenzgebühren verrechnet?
- Gibt es versteckte Kosten oder zusätzliche Kosten für Schulung, Wartung, usw.?

I.1.5 Betriebsmodelle

Cloud-Dienste werden über das Internet bzw. ein IP-basiertes Netzwerk bezogen. Betriebs-, Eigentums- und Organisationsaspekte können dazu führen, dass die Nutzung der Dienste nur einer beschränkten Anzahl von

Nutzern gewährt werden kann. Abhängig von der Benutzergruppe ergeben sich damit verschiedene Arten von Clouds, die sich zunächst grob in *öffentliche* und *private* Clouds unterteilen lassen. Daneben betrachten wir noch den Fall der *Community-Cloud* als kooperatives Modell, bei dem Cloud-Dienste durch verschiedene Anbieter kollaborativ angeboten werden. Grundsätzlich können Community-Clouds abhängig von der Benutzergruppe sowohl als öffentliche wie auch als private Clouds strukturiert werden. In dieser Studie wollen wir jedoch lediglich solche Community-Clouds betrachten, die über einen definierten Kundenkreis und einen dedizierten Netzzugang verfügen. Um dennoch Kooperationen etwa zwischen öffentlich-rechtlichen (die private oder Community-Clouds betreiben) und privatwirtschaftlichen Anbietern diskutieren zu können, betrachten wir weiterhin die *hybride Cloud*.

Worin unterscheiden sich die verschiedenen Cloud-Betriebsmodelle?

Grundsätzlich können Cloud-Betriebsmodelle wie folgt charakterisiert werden:

- Ist der Kundenkreis des Cloud-Anbieters a-priori bekannt oder können sich neue Benutzer jederzeit registrieren? Diese Frage hat u. a. Bezüge zu der Art des Vertrags zwischen Kunden und Anbieter: Je offener eine Cloud bzgl. ihres Kundenstamms ist, desto weniger ist die Ausarbeitung spezifischer vertraglicher Regelungen möglich — an die Stelle der SLAs treten AGBen.
- Befindet sich die Cloud-Infrastruktur auf dem Firmen- bzw. organisationseigenen Gelände (»on-premise«) oder an einem anderen Standort oder gar verschiedenen Standorten (»off-premise«)? Im zweiten Fall treten zusätzliche Fragestellungen bzgl. der Absicherung des Zugangs zur Cloud auf. Weiterhin sind Aspekte der Auftragsdatenverarbeitung zu berücksichtigen (Datenschutz und Datensicherheit).
- Befindet sich die Cloud-Infrastruktur auf dem organisationseigenen Gelände des Kunden (»on-premise«) kann weiterhin die Frage gestellt werden, ob die Cloud-Infrastruktur durch die entsprechende Organisation selbst verwaltet wird oder ob ein externer Anbieter mit dieser Aufgabe vertraut ist, was wiederum Auswirkungen datenschutzrechtlicher Natur haben kann.

I.1.5.1 Private Cloud

Private Clouds: Firmen- oder behördeneigene Rechenzentren bzw. externe Dienstleister mit eindeutigen Kundenbezug.

Bei einer privaten Cloud (*private clouds*, vgl. Abb. I.1.3 (a)) befinden sich sowohl Anbieter als auch Nutzer innerhalb derselben Organisation (Firma, Verwaltung). Dadurch werden eine Reihe von Fragestellungen (beispielsweise dem Bereich Datensicherheit) mehr oder minder hinfällig. Man unterscheidet die folgenden Evolutionsstufen:

- *Exploratory Cloud*: Hier steht das Ausprobieren von Cloud-Funktionalität innerhalb eines Unternehmens im Vordergrund. Dabei geht es insbesondere darum, Potentiale und Nachteile für konkrete Anwendungen herauszufinden und Erfahrungen im Umgang mit Clouds zu gewinnen.

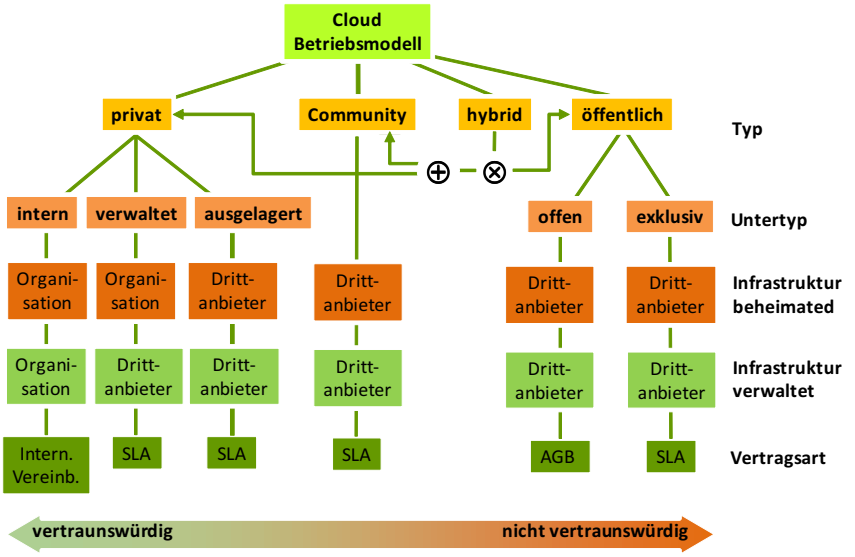


Abbildung I.1.2
Taxonomie der Cloud-Betriebsmodelle.

- Abteilungs-Cloud: Hierbei handelt es sich um eine Cloud, die lediglich innerhalb einer Abteilung genutzt wird. Dies bedeutet insbesondere, dass Anbieter und Nutzer innerhalb der gleichen Abteilung zu finden (bzw. personell identisch) sind und sich somit eine vereinfachte Nutzer/Anbieter-Beziehung ergibt.
- Unternehmens-Cloud: Im Gegensatz zur Abteilungs-Cloud sind Anbieter und Nutzer in unterschiedlichen Unternehmensabteilungen beheimatet.
- Schließlich sollen auch solche Clouds als »privat« bezeichnet werden, in denen die IT-Dienstleistung zwar von einem externen Anbieter erbracht wird, jedoch ein eindeutiger Kundenbezug besteht (d. h. der Dienstleister arbeitet im Auftrag eines einzigen oder einer kleinen Gruppe von Kunden). Diese Festlegung erlaubt es uns auch kleinere, an eine bestimmte Behörde angegliederte Rechenzentren, die Cloud-Technologien als technologisches »Upgrade« etablieren, in unsere Überlegungen mit einzubeziehen.

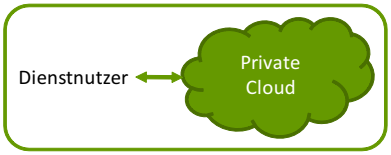
Private Modelle somit können entweder als interne, verwaltete oder externe Clouds aufgesetzt werden, je nachdem inwieweit externe Anbieter mit der Wartung und dem »hosting« der Cloud-Infrastruktur beauftragt sind. Für interne private Clouds, die »on-premise« beheimatet sind und durch die nutzende Organisation selbst verwaltet werden, werden Nutzungsbedingungen durch interne Vereinbarungen festgelegt. Für verwaltete oder externe Clouds werden SLAs zur Vertragsgestaltung verwendet.

I.1.5.2 Community-Cloud

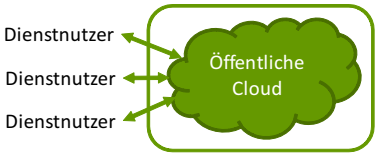
Community-Cloud: Zusammenschluß mehrerer Anbieter privater Clouds.

In diesem Model schließen sich mehrere (hier private) Cloud-Anbieter zusammen, um für einen definierten Kundenkreis gemeinsam Cloud-Dienstleistungen zu erbringen. Dieses Modell ist besonders geeignet, um

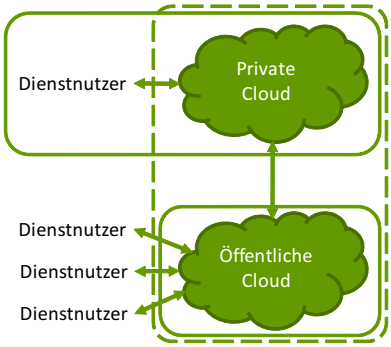
Abbildung I.1.3
Cloud-Betriebsmodelle.



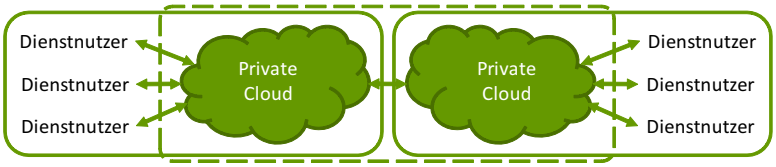
I.1.3 (a): Private Cloud



I.1.3 (b): Öffentliche Cloud



I.1.3 (c): Hybride Cloud



I.1.3 (d): Community-Cloud

den Zusammenschluss verschiedener — etwa kommunaler — Rechenzentren zu einem Verbund zu untersuchen. Ein Beispiel für einen derartigen Zusammenschluss ist das Projekt »Zielarchitektur Basisinfrastruktur« (ZaBI) des Dienstleisters Dataport (Isberner, 2010).[8]

Aus der Sicherheitsperspektive unterscheiden sich Community- von privaten Clouds insbesondere durch den Umstand, dass Daten und Prozesse verschiedene administrative Bereiche durchlaufen können, in denen unterschiedliche Sicherheits- und Verwaltungsrichtlinien gelten können. Auch aus der Verbindung der Cloud-Rechenzentren untereinander ergibt sich ein erhöhtes Risikopotential.

Die Infrastruktur in diesem Fall ist grundsätzlich ausgelagert; ihre Verwaltung wird durch einen externen (oder mehrere externe) Anbieter übernommen. Verträge sind als SLAs gestaltet.

I.1.5.3 Öffentliche Cloud

Öffentliche Clouds: Dienste für Jedermann.

Öffentliche Clouds (*public clouds*, vgl. Abb. I.1.3 (b)) können von beliebigen Personen und Unternehmen genutzt werden und sind nicht mehr auf die interne Anwendungen in einer einzelnen Institution oder einem Unternehmen beschränkt. Datensicherheit wird in öffentlichen Clouds zu einem Problem; Akteure müssen über Konzepte und Modelle zur Auslagerung sensibler Daten verfügen. Zwei Unterformen der öffentlichen Cloud sind zu unterscheiden:

[8] Vgl. auch http://www.rechenzentrum2010.de/de/

- Exklusive Clouds setzen voraus, dass sich sowohl Anbieter als auch Nutzer kennen. Sie handeln feste Konditionen aus und schließen einen SLA-basierten Vertrag ab. Es gibt keine Unbekannten.
- Bei offenen Clouds kennen sich Anbieter und Nutzer nicht notwendigerweise. Dies hat zur Folge, dass der Anbieter sein Angebot ohne direkten Input vom Kunden entwickeln und in Form von generischen Dienstverträgen festschreiben muss. Auf Grund der Vielzahl an potentiellen Nutzern müssen auch Geschäftsabschlüsse sowie die Nutzung von Diensten anbieterseitig vollautomatisch ablaufen. Nutzungsvereinbarungen werden generisch durch AGBen festgelegt.

I.1.5.4 Hybride Cloud

Hybride Clouds: Kombinationen zwischen privaten bzw. Community-Clouds und öffentlichen Clouds.

Hybride Clouds (*hybrid clouds*, vgl. Abb. I.1.3 (c)) werden aus privaten bzw. Community-Clouds und öffentlichen Clouds aggregiert, die zwar an sich unabhängige organisatorische Einheiten bilden, aber über standardisierte oder proprietäre Technologie miteinander verbunden sind, so dass Daten- und Anwendungsinteroperabilität unterstützt wird. Ein Beispiel ist eine private Cloud eines Unternehmens, die durch eine öffentliche Cloud zum Abfangen von Lastspitzen und Ausfallzeiten unterstützt wird.

Hybride Modelle sind sowohl im Bezug auf Vertragsgestaltungen wie auch datenschutzrechtlich besonders problematisch, da das Beziehungsgeflecht zwischen Auftraggebern und Anbietern sehr komplex werden kann.

Festlegung. Da das Begriffspaar öffentlich/privat sowohl auf die Art der in Rede stehenden Cloud als auch den Status ihres Betreibers angewendet werden kann, ist eine Begriffsfestlegung notwendig: Wir beziehen die Attribute »öffentlich« bzw. »privat« hier jeweils auf die Art der Cloud, d. h.

- ein **privater Cloud-Betreiber** (bzw. -Anbieter) ist ein öffentlich-rechtlicher oder privatwirtschaftlicher Betreiber (oder Anbieter) einer privaten Cloud, während
- ein **öffentlicher Cloud-Betreiber** (-Anbieter) ein öffentlich-rechtlicher oder (und dies ist der zu erwartende Regelfall) ein privatwirtschaftlicher Betreiber (Anbieter) einer öffentlichen Cloud ist.

I.1.6 Abgrenzung zu klassischen IT-Dienstleistungsangeboten

Informationstechnologie ist längst zum primären Hilfsmittel der behördlichen Aufgabenerfüllung geworden. Dienstauslagerung an Anbieter der

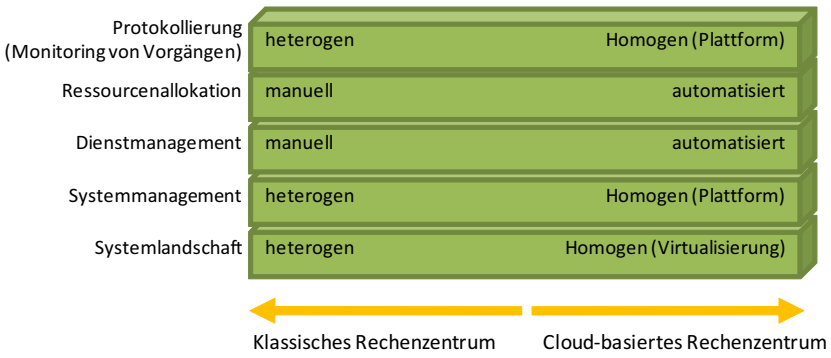


Abbildung I.1.4
Klassisches Rechenzentrum im Vergleich zu einem Cloud-basierten Rechenzentrum.

öffentlichen Hand und zunehmend auch an private Anbieter zur Kostenoptimierung und Kompetenzbündelung ist gängige Praxis. Wie können wir einen klassischen Dienstanbieter von einem unterscheiden, dessen Angebot auf Cloud-Technologien beruht?

Methodologische Diskriminierung: Wie können Cloud-Anbieter von klassischen Dienstleistern unterschieden werden?

Eine direkte Anwendung der in Abschnitt I.1.2 diskutierten Eigenschaften hilft uns unmittelbar nicht weiter, da eben auch klassische Dienstleister aktuelle Technologien einsetzen und deren Angebot zumindest in Teilen eben diese Eigenschaften aufweist. Externe Anbieter stellen einen netzwerkbasierten Zugang zu Diensten mit Hilfe von Web-basierten Technologien zur Verfügung. Verschlüsselung bei der Datenübertragung ist eine Mindestanforderung für Dienste, die nicht über dedizierte und besonders gesicherte Netze angeboten werden. Der Einsatz von Virtualisierungstechnologien sorgt dafür, dass Ressourcen-Pools gebildet und dynamisch skalierbar angeboten werden können.

In der vorliegenden Studie (insbesondere in den Kapiteln III.2 und III.3) benötigen wir aus methodologischen Gründen jedoch eine Vergleichsbasis, um Cloud-Innovationen bzgl. verschiedener Kriterien beurteilen zu können. Diese Basis wollen wir im folgenden einen »klassischen Dienstleister« nennen. Damit meinen wir jedoch weder einen spezifischen Anbieter von IT-Dienstleistungen, noch wollen wir damit den augenblicklichen Stand der Technik charakterisieren.

Für unsere weitere Diskussion verwenden wir deshalb die in Abb. I.1.4 dargestellten Diskriminierungsmerkmale:

Virtualisierung kann zu einer homogenisierten Infrastruktur führen.

- **Systemlandschaft** (heterogen/homogen). Ein ISPRAT-Whitepaper[9], das die Probleme und Potentiale von IT-Kooperationen untersucht, verweist darauf, dass heutige IT-Landschaften organisch gewachsen sind und ihre Betriebsstabilität, Sicherheit und Kontinuitätsmanagement oftmals verbesserungswürdig sind. Finanzmittel reichen nur für die Aufrechterhaltung des Betriebs sowie für Neubeschaffungen von Systemen am Ende ihrer Lebensdauer aus. Der Einsatz von homogenisierte Lösungen ist deshalb nur schwer zu erreichen. Im Unterschied dazu erlauben Cloud-spezifische Lösungen wie etwa Virtualisierung, dass eine

[9] (Graudenz u. Schramm, S. 10f).

homogene Abstraktion der unterliegenden Hardware-, Speicher- und Netzwerkressourcen möglich wird.

- **Systemmanagement** (heterogen/homogen). Aufbauend auf dem vorhergenden Argument muss auch für die Mechanismen und Prozesse, die das Management dieser Systemlandschaften betreffen, für klassische Anbieter eine Tendenz zu heterogenen Insellösungen angenommen werden. Erfahrung und »best practice« von Systemadministratoren ersetzt häufig dokumentierte und automatisierte Prozesse. Es kommen selbstentwickelte »Mikrowerkzeuge« (*shell scripts* bzw. *batch files*) zum Einsatz, die sich für spezifische Anwendungen bewährt haben. Im Unterschied dazu erfordert eine Cloud-Infrastruktur die Verfügbarkeit eines homogenisierten Ansatzes zur Systemadministration, der durch vielfältige plattformintegrierte Mechanismen unterstützt wird (z. B. die automatisierte Verwaltungen von *VM-Images*, Monitoringmechanismen, usw.).

Vereinheitlichte bzw. automatisierte Prozesse zum Systemmanagement.

- **Dienstmanagement** (manuell/automatisiert). Auch im Bereich Dienstmanagement kann für klassische Dienstleister eine Tendenz zu manuell (d. h. durch die Erstellung von dienstspezifischen Konfiguration durch Systemadministratoren) durchgeführtem Managementprozessen angenommen werden. Ressourcenpooling, Elastizität, messbare Dienstqualität und Selbstbedienung erfordern hingegen einen hohen Automatisierungsgrad für die Verwaltung von Diensten.

Cloud-Dienste erfordern ein weitgehend automatisiertes Management.

Die beiden folgenden Aspekte sind für die weitere Diskussion von besonderer Bedeutung:

- **Ressourcenallokation** (manuell/automatisiert). Mechanismen, die eine bedarfsabhängige Skalierung von Ressourcen unterstützen, die einem Dienst zugeordnet sind, sind integraler Bestandteil einer Cloud-basierten Infrastruktur. Klassische Anbieter (insbesondere solche, die auf den Einsatz von Virtualisierungslösungen verzichten) sind tendenziell auf eine manuelle Zuordnung von Ressourcen zurückgeworfen.

Automatisierte Ressourcenallokation kann helfen, DDoS-Angriffen zu begegnen.

- **Protokollierungsmechanismen** (heterogen/homogen). Das Monitoring von Systemereignissen ist ein integraler Bestandteil des System- und Dienstmanagements eines Rechenzentrums. Letztlich dienen solche Messungen auch zur Bestimmung der Dienstqualität, die dem Dienstnutzer angeboten wird. In klassischen Infrastrukturen existiert häufig eine große Anzahl von aufgabenspezifischen Monitoring-Lösungen, da auf unterschiedlichen Systemschichten ganz verschiedenartige Messansätze verwendet werden müssen. In Cloud-Architekturen müssen Messverfahren, die ja teilweise auch an den Kunden weitergegeben und durch diesen konfigurierbar sind, zumindest einen höheren Grad an Homogenität und Generizität aufweisen.

Die Verfügbarkeit weitreichender Protokollierungsmöglichkeiten ist datenschutzrechtlich relevant.

KAPITEL I.2

Umfrage: Dienst-Auslagerung im öffentlichen Sektor

Zusammenfassung

Als Vorbereitung für die vorliegende Studie wurde ein Fragebogen zum Thema Auslagerung von IT-Dienstleistungen erstellt. Aus den vorliegenden Antworten kann eine Reihe von vorläufigen Annahmen als Arbeitshypothesen hergeleitet werden.

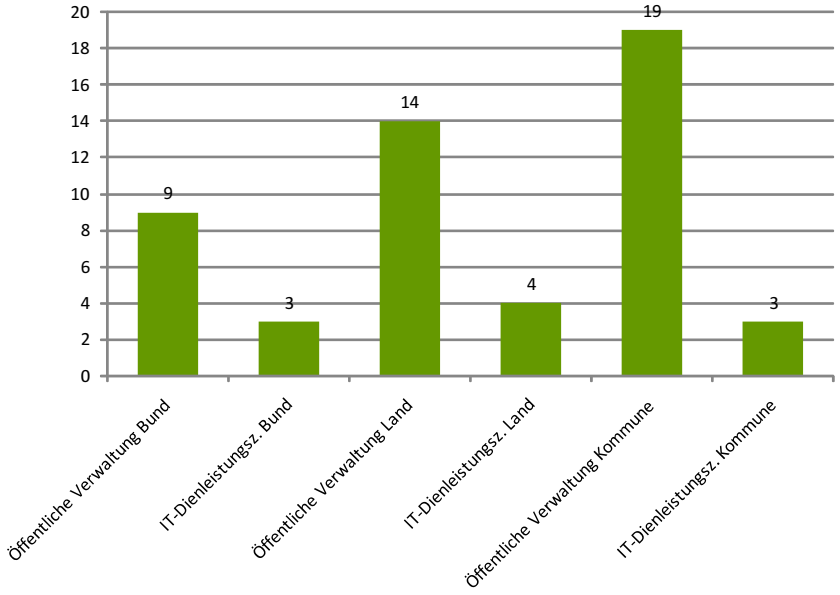
1. *Die Auslagerung von Diensten an externe IT-Anbieter ist heute bereits Stand der Technik.*
2. *Behörden stehen IT-Kooperationen grundsätzlich positiv gegenüber.*
3. *Insbesondere Fachverfahren und Infrastruktur-Dienste sind für eine Auslagerung geeignet. Im Gegensatz dazu werden Plattform-Dienste nur selten ausgelagert. Verfügbarkeit wird als wesentliche Anforderung an Dienstleistungen genannt.*
4. *Virtualisierung, eine der Basis-Technologien des Cloud-Computing, wird heute bereits vielfach eingesetzt.*

Als Vorbereitung für die vorliegende Studie wurde ein Fragebogen zum Thema Auslagerung von IT-Dienstleistungen erstellt und an 512 Einrichtungen der öffentlichen Hand versandt. Der geringe Rücklauf von 52 Antworten erlaubt zwar keine strenge, quantitative Auswertungen, dennoch können aus den vorliegenden Antworten eine Reihe von vorläufigen Annahmen als Arbeitshypothesen hergeleitet werden.

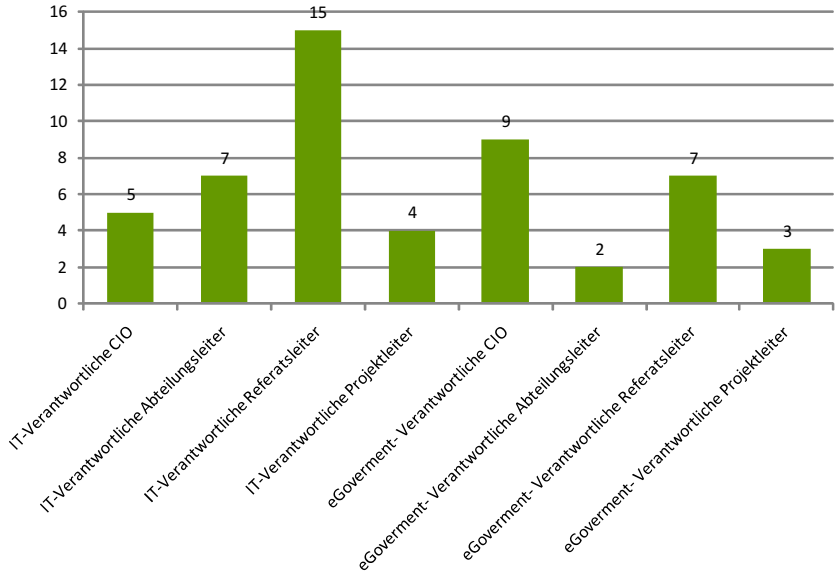
Der Rücklauf unserer Umfrage beträgt mit 52 Antworten etwa 10 % der ausgesendeten Anfragen.

Anmerkung. Um sprachlich komplexe Sätze zu vermeiden, erlauben wir uns im Folgenden eine leichte Ungenauigkeit: Wir schreiben häufig,

Abbildung I.2.1
Beteiligung an einer Umfrage zum Thema »Auslagerung von IT-Dienstleistungen«.



I.2.1 (a): Insitutionen ($N = 52$).



I.2.1 (b): Personen ($N = 52$).

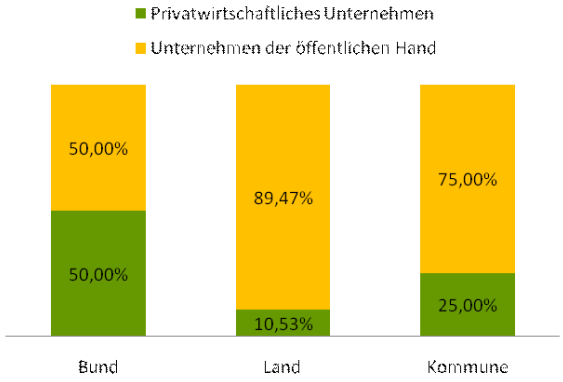


Abbildung I.2.2
Anteil ausgelagerter Dienstleistungen an private bzw. Anbieter der öffentlichen Hand ($N = 49$).

dass k % der befragten Institutionen in dieser oder jener Weise verfahren — gemeint ist natürlich, dass k % der eingegangenen Antworten auf die entsprechende Frage in der genannten Weise gelautet haben. Wir geben jeweils die Anzahl N der tatsächlich eingegangenen Antworten auf eine Frage an. Die vollständige Auswertung der Umfrage findet sich aufgeschlüsselt nach den gestellten Fragen in Anhang B.

I.2.1 Beteiligung

Abb. I.2.1 schlüsselt die erhaltenen Antworten nach der Art der Institutionen und deren Mitarbeiter auf, die sich an der Umfrage beteiligt haben. Öffentliche Verwaltungen auf kommunaler, Länder- und Bundesebene haben sich am stärksten beteiligt. Zu einem geringen Anteil sind auch Antworten von IT-Dienstleistungszentren eingegangen (Abb. I.2.1 (a)).

Die Positionen der Teilnehmer an der Umfrage wird in Abb. I.2.1 (b) genauer aufgeschlüsselt. Den überwiegende Anteil der Antworten steuerten IT-verantwortlichen Referatsleitern bzw. Abteilungsleitern bei.

I.2.2 Dienstauslagerung

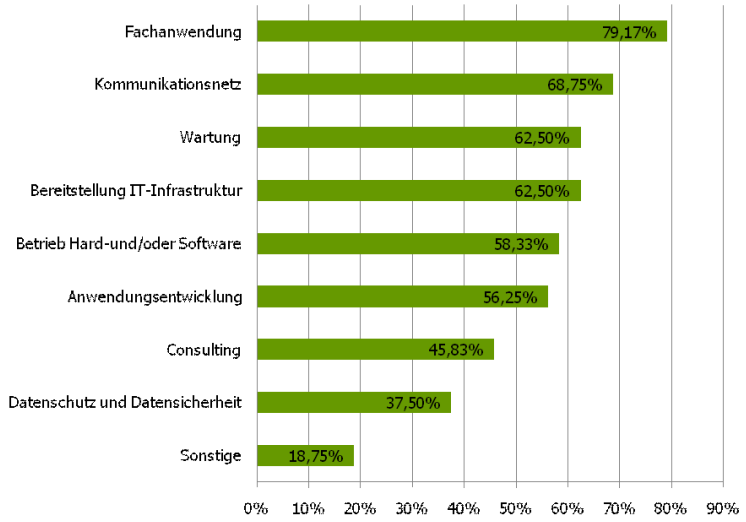
75 % der befragten Institutionen haben Dienstleistungen an externe Anbieter ausgelagert.

Die Auslagerung von Diensten an externe IT-Anbieter ist heute bereits eine etablierte Verfahrensweise. Etwa 75 % der Institutionen, die sich an der Umfrage beteiligt haben, haben IT-Dienstleistungen an externe Dienstleister ausgelagert. Auf Bundesebene ist eine relativ hohe Anzahl von privatwirtschaftlichen Unternehmen mit der Übernahme von Diensten für Verwaltungen betraut. Auf kommunaler und Länderebene überwiegen deutlich Dienstleister der öffentlichen Hand (Abb. I.2.2).

Insbesondere Fachverfahren und Infrastruktur-Dienste sind für eine Auslagerung geeignet. Im Gegensatz dazu werden Plattform-Dienste nur selten ausgelagert (Abb. I.2.3).

Bevorzugt (bei 79 % der befragten Institutionen) werden dabei Fachanwendungen in Anspruch genommen (Abb. I.2.3); in diesem Zusammen-

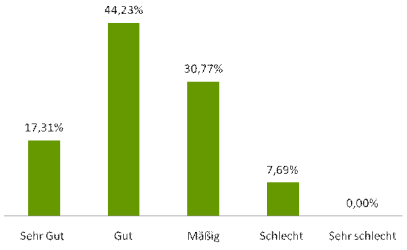
Abbildung I.2.3
Art der ausgelagerten Dienstleistungen ($N = 48$).



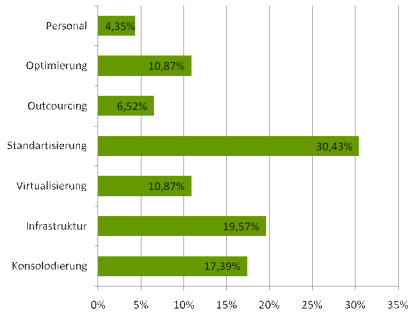
hang ist auch der relativ hohe Anteil an angepassten Softwarelösungen für Fachverfahren und bereichsübergreifende Prozesse zu sehen, der in Abb. I.2.8 dokumentiert ist). Auch Kommunikations- und Recheninfrastruktur sowie Wartungsaufgaben werden häufig ausgelagert. Dagegen verbleiben Consulting-Aufgaben und auch Aufgaben, die Datensicherheit und Datenschutz betreffen, häufig innerhalb der Behörde.

Die eigene IT-Landschaft wird als »gut« bis »mäßig« charakterisiert (Abb. I.2.4 (a)). Neben einer Stärkung der IT-Infrastruktur werden Standardisierung und Konsolidierung als Verbesserungsmöglichkeiten favorisiert (Abb. I.2.4 (b)). Interessant ist das mangelnde Interesse an der Auslagerung weiterer Dienstleistungen und der Optimierung von Verwaltungsprozessen. Der relativ geringe Wunsch nach Virtualisierung erklärt sich dadurch, dass die meisten der befragten Institutionen, nämlich 87 %, bereits über Virtualisierungslösungen verfügen.

Abbildung I.2.4
Bewertung der eigenen IT-Landschaft.



I.2.4 (a): Zufriedenheit ($N = 52$.)



I.2.4 (b): Änderungswürnsche ($N = 46$).

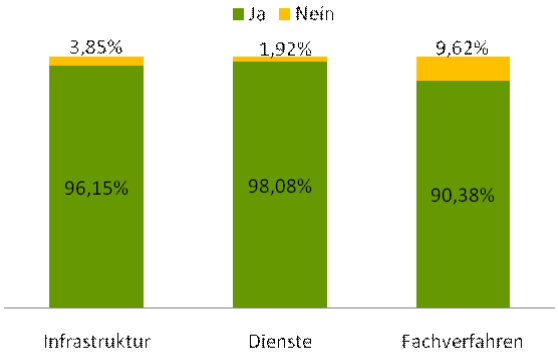


Abbildung I.2.5
Bereitschaft zur ressortübergreifenden Kooperation ($N = 52$).

Immerhin 18 % der befragten Institutionen haben schon einmal bereits ausgelagerte Dienstleistungen in das eigene Rechenzentrum zurückgeholt bzw. neu an andere externe Anbieter vergeben. Dabei wurden die folgenden Gründe genannt:

18 % der Befragten haben bereits ausgelagerte Dienstleistungen zurückgeholt.

- Hoher Aufwand für Abstimmung mit dem Anbieter und Nachbearbeitung der Ergebnisse
- Unzureichender Service, mangelndes Fachwissen und Flexibilität
- Zu großer Zeitaufwand für Software-Updates, Patches etc.
- Mangelnde Dienstqualität bzgl. Sicherheit und Verfügbarkeit
- Zur Bildung einer kritischen Masse von Anbietern für eine Neuausschreibung

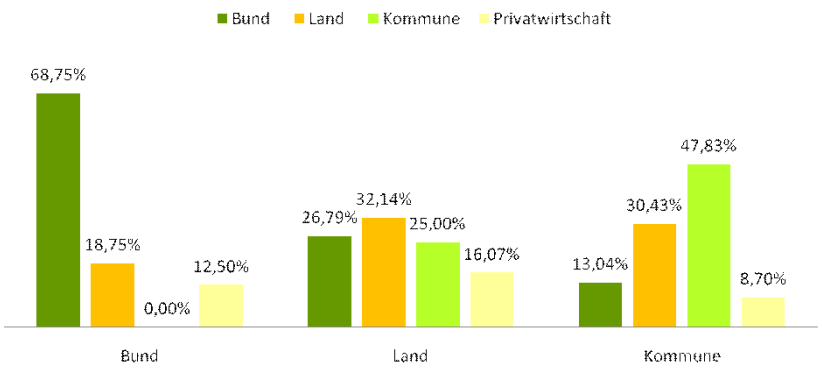


Abbildung I.2.6
Bereitschaft zur ebenenübergreifenden Kooperation ($N = 46$).

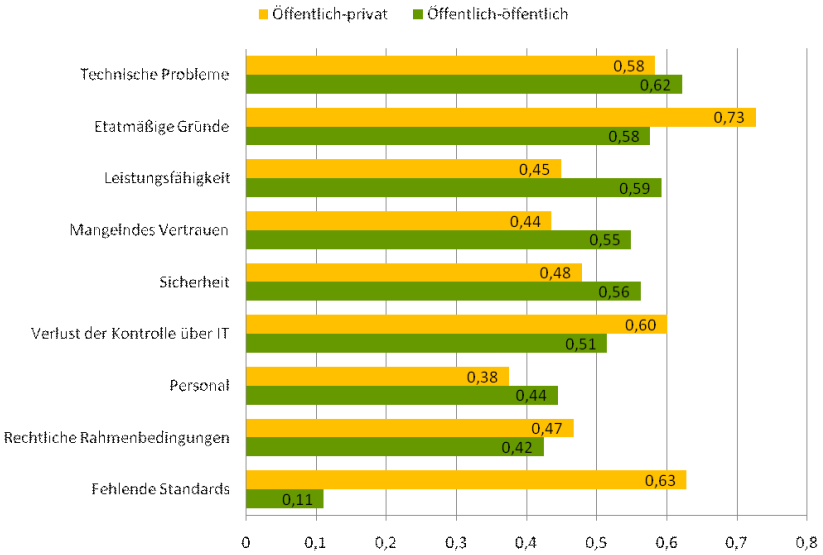


Abbildung I.2.7
Hemmnisse für eine IT-Kooperation ($N = 49$).

I.2.3 Zusammenarbeit

Behörden stehen der Auslagerung von Diensten an externe Anbieter grundsätzlich positiv gegenüber. Eine hohe Kooperationsbereitschaft (auch ressort- und ebenenübergreifend) impliziert ein gutes Potential für die Konsolidierung von Dienstleistungen.

78% aller Behörden sind bereit, Überkapazitäten zu teilen. Auch ressortübergreifende Kooperationen sind für die meisten Behörden denkbar.

Generell ist eine hohe Bereitschaft zur Zusammenarbeit festzustellen. So haben 78 % der befragten Institutionen geäußert, dass sie bereit seien, Überkapazitäten im IT-Bereich mit anderen Behörden zu teilen. Die verbleibenden 24% der Befragten, die sich hier negativ geäußert haben, haben u. a. die folgenden Gründe dafür angegeben:

- Es gibt zu wenig standardisierte Anwendungen
- Externe Dienstverträge können nicht garantiert werden
- Sicherheit und Verfügbarkeit sind nicht sichergestellt
- Die verwendeten Fachverfahren sind zu komplex, um von Externen effizient bearbeitet zu werden
- Datenschutzrechtliche Bedenken

Ressortübergreifende Kooperationen sind für die meisten Behörden sowohl für Fachverfahren, sonstige Dienste und Infrastruktur denkbar (Abb. I.2.5). Ebenenübergreifende bzw. privatwirtschaftliche Kooperationen werden auf Bundes- bzw. kommunaler Ebene weniger positiv betrachtet, während die Bereitschaft der Länder für eine ebenenübergreifende Kooperation relativ ausgewogen ist.

Als Hemmnisse für eine IT-Kooperation werden insbesondere technische Probleme, Leistungsfähigkeit, etatmäßige Gründe, Furcht vor Kontrollverlust sowie fehlende Standards angegeben (vgl. Abb. I.2.7), wobei die-

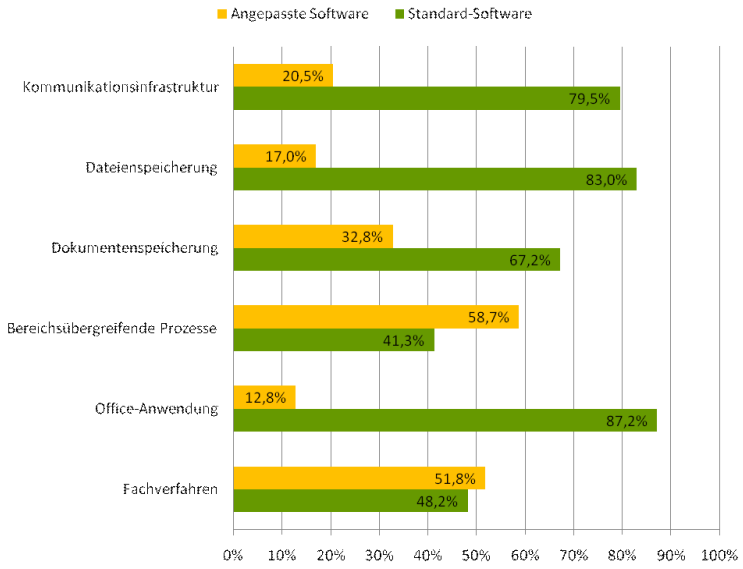


Abbildung I.2.8
Verhältnis von verwendeter angepasster zu Standardsoftware (zum Rücklauf vgl. S. 160).

se Aussagen aufgrund des geringen Rücklaufs der Umfrage kritisch zu bewerten sind. Auffällig sind jedoch die folgenden Verhältnisse:

- Etatmäßige Gründe werden bevorzugt als Hindernis für eine öffentlich-private Kooperation angegeben.
- Die Leistungsfähigkeit privater Anbieter wird im Vergleich zu der öffentlicher Anbieter als geringer eingestuft.
- Fehlende Standards werden als wesentliche Hemmnis für die Kooperation mit privatwirtschaftlichen Anbietern gesehen.

Mangelndes Vertrauen in die Leistungsfähigkeit und fehlende Standards werden als Gründe gegen eine öffentlich-private Kooperation genannt.

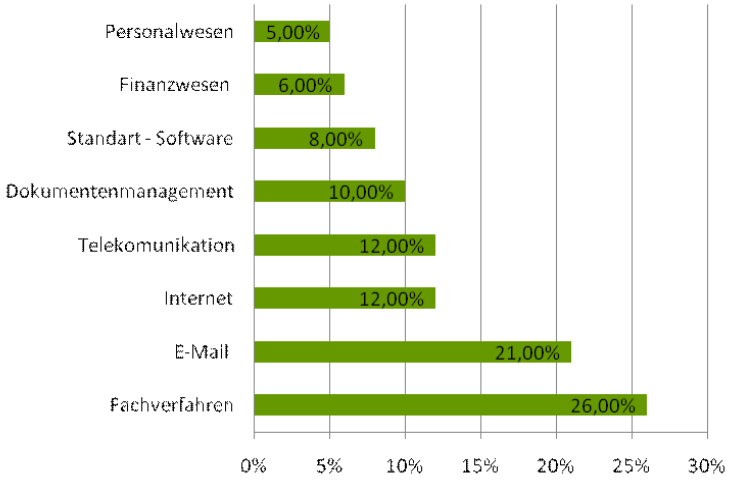


Abbildung I.2.9
Priorisierung von IT-Anwendungen bzgl. Verfügbarkeit und Zuverlässigkeit ($N = 52$).

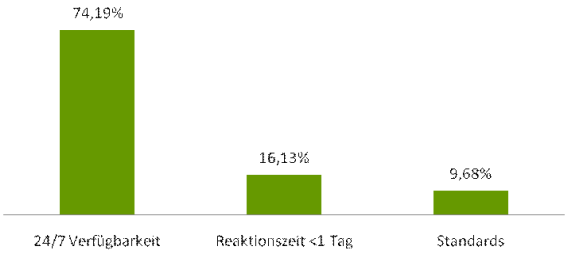


Abbildung I.2.10 *Priorisierung von Anforderungen ($N = 31$).*

I.2.4 Anforderungen an Anwendungen

Vergleicht man das Verhältnis von Standard- zu angewandter Software (Abb. I.2.8), so ergibt sich (wenig überraschend), dass generische Aufgaben wie die Bereitstellung einer Kommunikationsinfrastruktur, Daten- und Dokumentenspeicherung sowie Office-Aufgaben in der überwiegenden Anzahl der Fälle durch Standardlösungen unterstützt werden. Andererseits fällt der relativ hohe Anteil (48 %) von Standardsoftware für die Unterstützung von Fachverfahren auf.

Die Verfügbarkeit von Fachverfahren wird als wichtig eingestuft.

Die Verfügbarkeit und Zuverlässigkeit von Anwendungen zur Unterstützung von Fachverfahren wird von 26 % der Befragten als sehr wichtig eingeschätzt (Abb. I.2.9). Funktionierende Email-Systeme sind für 21 % der Befragten besonders wichtig. Andere Anwendungen (Telekommunikation, Internet, usw.) werden als weniger wichtig eingeschätzt.

Allerdings wurde hohe Verfügbarkeit (24/7) von der überwiegenden Anzahl der Befragten (74 %, Abb. I.2.9) als wichtigste Anforderung an die Bereitstellung von Software genannt. Schnelle Reaktionszeiten und Standardisierung waren nur 16% bzw. 9% der Befragten wichtig.

I.2.5 Einsatz von Virtualisierungslösungen

Ein weiterer Fragenkomplex adressiert die Verwendung von Virtualisierung in den verwaltungseigenen Rechenzentren bzw. bei IT-Dienstleistern. Virtualisierungslösungen als Basis-Technologie des

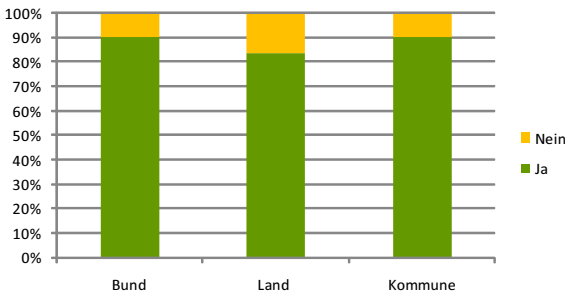


Abbildung I.2.11 *Verwendung von Virtualisierungslösungen ($N = 48$).*

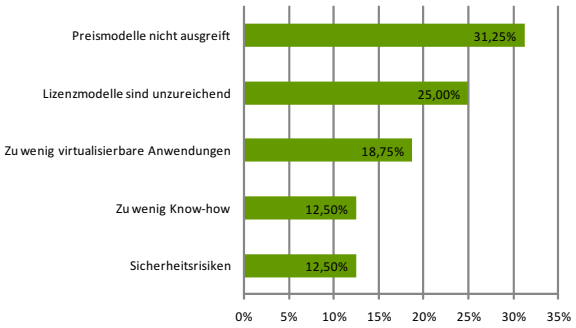


Abbildung I.2.12
Hindernisse beim Einsatz von Virtualisierungslösungen ($N = 16$).

Cloud-Computing impliziert bereits eine Reihe von Vorbehalten (vgl. Kapitel III.4), so dass eine genauere Analyse des augenblicklichen Einsatzes solcher Technologien Hinweise darauf geben kann, inwieweit mit solchen Vorbehalten tatsächlich umgegangen wird. Tatsächlich setzten immerhin zwischen 80 % und 90 % der Befragen (abhängig davon, ob die entsprechenden Organisationen auf Bundes-, Länder- oder Kommunalebene agieren) Virtualisierung ein (Abb. I.2.11).

Virtualisierung ist Stand der Technik.

Als Hindernisse, die gegen die Einführung von Virtualisierungslösungen sprechen, wird insbesondere das Fehlen von ausgereiften Preis- bzw. Lizenzmodellen genannt (31 % bzw. 25 %, vgl. Abb. I.2.12). Weiterhin wird das Fehlen virtualisierbarer Anwendungen mit immerhin annähernd 19 % als Grund gegen den Einsatz von Virtualisierung genannt. Auffällig ist aber, dass Sicherheitsprobleme mit nur 12,5 % als weniger relevant eingeschätzt werden. Demgegenüber stehen allerdings besondere Sicherheitsbedenken, die im Zusammenhang mit dem Einsatz von Virtualisierung im Cloud-Umfeld genannt werden: Insbesondere ist hier der unsachgemäße Umgang mit VM-Images zu nennen, wie auch potentielle Schwachstellen von Hypervisoren bzw. virtuellen Maschinen, die in der Übernahme solcher System bzw. dem Ausbrechen aus deren Sicherheitskontexten durch einen Angreifer bestehen (vgl. Kapitel III.1 bzw. III.4).

Teil II

Rahmenbedingungen

KAPITEL II.1

Governance-Bezugsrahmen

Zusammenfassung

Zur Identifikation der relevanten Faktoren, die die Nutzung von Cloud-Computing durch die öffentliche Verwaltung bestimmen, setzen wir die Cloud-Eigenschaften Ressourcen-Pooling, virtuelle Bereitstellung und Netzwerkzugang zu vier Bestimmungsfaktor-Gruppen, nämlich »rechtliche Zulässigkeit«, »(wirtschaftliche) Vorteilhaftigkeit«, »Steuerbarkeit« und »Risikobeherrschbarkeit« in Beziehung:

1. *Rechtliche Zulässigkeit/Verwaltungsrecht: Virtualisierung und der netzwerkbasierter Zugangs verändert die Besitz- und Berechtigungsstrukturen von Leistungserstellungsprozessen sowie von Datenbeständen, woraus verfahrensrechtlich Unsicherheitsräume oder Nichtanwendbarkeitsschwierigkeiten enstehen, die entsprechend berücksichtigt werden müssen. Besonders zu prüfen ist, ob diese Schwierigkeiten im Rahmen von SLAs hinreichend regelbar sind.*

2. *Rechtliche Zulässigkeit/Rahmenrecht: Hier ergeben sich neben datenschutzrechtlichen Problemen insbesondere auch vergaberechtlicher Fragen, die im Kern wiederum auf den Regelungsbedarf und die Regelungsmöglichkeiten mit dem Instrument SLA hinauslaufen.*

3. *(Wirtschaftliche) Vorteilhaftigkeit/kamerale Effizienz: Während grundsätzliche Effizienzprüfungen für Cloud-Ansätze kaum unterschiedlich zur Bewertung anderer Bündelungsformen stattfinden dürften, ergibt sich aus dem Definitionsmerkmal »virtuell« und dem organisatorischen Merkmal »Kompetenzbündelung« die spezielle Frage, inwieweit die Nutzung*

von Cloud-Computing-Ansätzen zu grundlegend veränderten behördlichen Zuschnitten und Paradigmen führen.

4. *Steuerbarkeit/Durchführungssteuerung: Die virtuelle und mit »remote«-Zugriff versehene Cloud-Computing-Ausgestaltung wirft grundlegend (und massiv) die Frage auf, ob und wie hier überhaupt noch eine Steuerbarkeit durch die verantwortliche Behörde gewährleistet werden kann.*
5. *Risikobeherrschbarkeit/Rechtsrisiko: Hier ergeben sich insbesondere Rechtsrisikofragestellungen in Bezug auf Nachvollziehbarkeit.*

Insgesamt wird deutlich, dass die Fragestellung des Cloud-Computing in der öffentlichen Verwaltung im Wesentlichen eine »Risikofragestellung« ist.

Für den Untersuchungsfokus dieser Studie wollen wir nachfolgend eingrenzen, welche Faktoren (in welchem Umfang) relevant für die Einführung bzw. Umsetzung von entsprechenden Cloud-Computing-Konzepten sind. Hierfür beschränken wir uns an dieser Stelle auf Cloud-Konzepte für Verwaltungen im deutschen Bedingungskontext (also auf föderal-differenzierte Strukturen und streng subsidiäre Aufgabenverteilungen).

Relevante Perspektiven.

Greifen wir die vorstehenden begrifflichen und konzeptionellen Abgrenzungen von Cloud-Computing auf (vgl. Abschnitt I.1.2), sind vor allem zwei Perspektiven zu unterscheiden, die für die Entwicklung eines Governance-Bezugsrahmens von besonderer Bedeutung sind:

Funktionalperspektive: Aufgabenbündellung beim Cloud-Anbieter.

- Einerseits eine **funktions- bzw. aufgabenbezogene Sichtweise**, in der durch Cloud-Ansätze eine Bündelung der Aufgabenwahrnehmung — und zwar speziell der gesamten oder teilweisen Aufgabendurchführung[1] — beim Cloud-Anbieter stattfindet, in dem verschiedene Nutzer/Kunden gleichartige Dienste oder Verrichtungen in einer Cloud bearbeiten lassen. Diese funktionsorientierte Sichtweise findet sich (in praktisch gleicher Form) auch bei anderen Bündelungsmodellen öffentlicher Dienstleistungen über verschiedene Behörden (und auch Ebenen) wieder, z. B. bei der Konsolidierung von IT-Funktionen in gemeinsam getragenen »Shared Service-Centern«.

Institutionenperspektive: Rollenverteilung Anbieter/Besteller.

- Andererseits eine **institutionenorientierte Sichtweise**, bei der eine klare Rollenverteilung vorliegt, nämlich bei der »Cloud-Institution«

[1] Verwaltungswissenschaftlich eingeführt ist das Konstrukt von Aufgabengewährleistungsverantwortung und Aufgabendurchführungsverantwortung. Dabei ist davon auszugehen, dass die einer Behörde (z. B. gesetzlich) zugewiesene Aufgabe (bzw. Pflicht zur Aufgabenwahrnehmung) grundsätzlich nicht delegierbar ist, also die Verantwortung für die vorgeschriebene (Art der) Aufgabenerfüllung stets bei der Behörde verbleibt oder durch weitere (rechtliche) Regelung an Dritte/andere Behörden übertragen wird. Dies schließt natürlich nicht aus, dass unter Gewährleistungsverantwortung der zuständigen Behörde Dritte in die operative Aufgabendurchführung eingebunden werden. Dabei wird allerdings vorausgesetzt, dass die zuständige Behörde die Ordnungsmäßigkeit der Aufgabenwahrnehmung über alle (auch von Dritten durchgeführte Teile) sicherstellt.

die Rolle eines Dienstanbieters, dem eine öffentliche Verwaltungsinstitution bzw. Behörde in der Rolle eines Nachfragers oder »Bestellers« gegenübersteht.

Nachfolgend sammeln und diskutieren wir über beide Sichtweisen hinweg Bestimmungsfaktoren, die im Zusammenhang mit Cloud-Modellen besonders relevant erscheinen.

II.1.1 Funktionalperspektive (Prozessperspektive)

Gegenstand einer funktionalen Governance-Perspektive für Cloud Ansätze sind öffentliche (Verwaltungs-) Aufgaben (oder — m. a. W. — die Durchführung öffentlicher Verwaltungs- bzw. Leistungsprozesse), bei der die Wahrnehmung der Aufgabe insgesamt oder in (Prozess-) Bestandteilen bei einem oder mehreren Dritten realisiert wird. Dabei liegt die originäre Aufgabenverantwortung (z. B. auf Grundlage gesetzlicher Bestimmungen) bei einer (oder verschiedenen) Behörde(n). Bekanntlich ist dabei die Verantwortung der aufgabenwahrnehmenden Behörde nicht nur auf die Gewährleistung der Aufgabe beschränkt, sondern umfasst auch die Durchführung des Leistungserstellungsprozesses selbst. Dies gilt z. B. für die Einhaltung von Verfahrensregeln, die ggf. auch Rechte von Kunden (Bürgern, Wirtschaftsunternehmungen oder andere Behörden und Institutionen) berühren.

Verantwortlichkeit für behördliche Aufgabengewährleistung ist nicht delegier- oder teilbar.

Aus grundsätzlichen rechtlichen Gründen ist die Aufgaben(gewährleistungs)verantwortung von Behörden nicht delegier- oder teilbar. Darüber hinaus gibt es eine Reihe von Restriktionen, inwieweit gerade bei hoheitlichen Akten oder beispielsweise beim Umgang mit bürger- oder kundenbezogenen Daten die Verwaltungsprozesse (ganz oder teilweise) sogar zwingend durch bestimmte Organe oder Behörden gehandhabt werden müssen (z. B. bei Fachprozessen in der Steuerverwaltung zur Wahrung des Steuergeheimnisses). Ansonsten sind jedoch Behörden bei der Ausgestaltung ihrer Leistungserstellungsprozesse (also der Aufgabendurchführung) im Rahmen gegebener Verfahrensregeln weitgehend frei. In diesem Sinne ist auch die (Teil-) Erstellung durch Dritte im Sinne einer Auslagerung der Leistungserstellung (Fremdbezug oder Einkauf in von Dritten betriebene Institutionen bzw. kooperative Leistungserstellung mit solchen Institutionen) prinzipiell zulässig.

Gebot der wirtschaftlichen Aufgabenerfüllung.

Innerhalb des von eventuellen Aufgabendurchführungsanforderungen gesetzten Rahmens besteht für deutsche Behörden die Anforderung, die zu verantwortenden Aufgaben nach einem strengen Gebot der wirtschaftlichen Aufgabenerfüllung wahrzunehmen. Dieses impliziert, dass bei alternativ zur Verfügung stehenden Varianten der Leistungserstellung stets die Variante zu wählen ist, die bei gegebener Leistungsqualität die niedrigsten Kosten verursacht.

Wie an anderer Stelle[2] grundlegend untersucht, gelten spätestens seit den 90er Jahren — durch technologische Innovationen im IT-Bereich — gänzlich andere Potenziale zur Bündelung von Dienstleistungsprozes-

[2] Vgl. (Fiedler u. a., 2010).

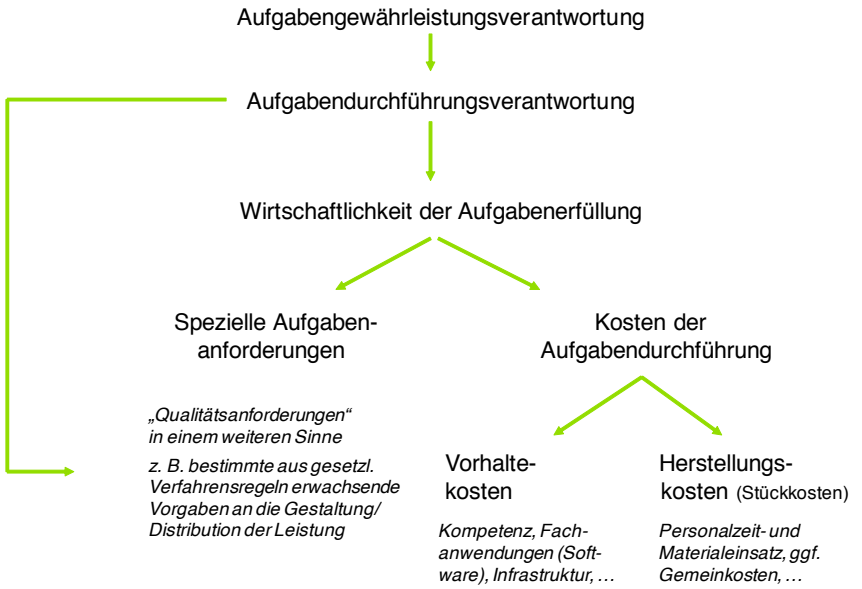


Abbildung II.1.1
Parameter behördlicher Aufgabenorganisation (eigene Darstellung).

sen. Insbesondere die Möglichkeiten räumlich entörtlichter Leistungserstellungsprozesse, die durch vernetzte IT-Anwendungen ermöglicht werden, haben Effizienzkalküle grundlegend verschoben, und zwar für den öffentlichen Sektor dahingehend, dass einzelne Behörden die Wirtschaftlichkeitspotenziale von Fall-/Vorgangszahlenakkumulationen nicht mehr ausschöpfen können, sondern entsprechende wirtschaftliche Fall-/Vorgangszahlen nur über eine Vielzahl von Institutionen gebündelt realisiert werden können.

Motive für Bündelungen der behördlichen Leistungserstellung.

Die Motive bzw. Zielsetzungen für weitergehende Bündelungen entsprechen den allgemeinen Gründen für höhere Betriebsgrößen und zielen im Kern auf drei Ansatzpunkte ab:

Senkung von Transaktionskosten, Kompetenzbündelung, Komplexitätsreduktion und Integration.

- Transaktionskosten-Senkungspotentiale durch größere Einheiten
- Leistungssteigerungspotentiale insbesondere durch Bündelung von Kompetenz in größeren Betriebsgrößen
- Strategische Kostensenkungspotentiale vor Allem durch die mit der Bildung größerer und bzw. einer verringerten Anzahl von Einheiten einhergehender Komplexitätsreduzierungen. Dieses bezieht sich unter anderem auf eine Reduzierung der Vielfalt unterschiedlicher Standards, Systeme und (Fach-)Applikationen im öffentlichen Sektor. Ferner werden in diesem Zusammenhang auch bessere Möglichkeiten behörden(ebenen)übergreifender Integration angeführt.

Demongraphischer Wandel.

Weiterhin wird — aus einer strategischen Sicht — reklamiert, dass es in Anbetracht eines absehbaren demographischen Fachkräftemangels, im umkämpften IT-Fachkräfte-Arbeitsmarkts und sich abzeichnender weiterer Spezialisierungserfordernisse auch wichtige Wettbewerbsargumente für größerteilig aufgestellte öffentliche IT-Dienstleister zu beachten sind. Es wird befürchtet, dass bei (zu) kleinteiliger Aufstellung das Leis-

tungspotenzial öffentlicher Marktteilnehmer gegenüber privatwirtschaftlichern Wettbewerbern mittelfristig nicht mithalten kann.

Diese Motive bzw. Zielsetzungen, die die Vorteile von Bündelungen betonenden, lassen jedoch keinen klaren Schluss darauf zu, welche wie konsolidierte (größerteilige) Strukturen unter heutigen Rahmenbedingungen zukünftig realisiert werden können. (Alternative) Gestaltungsmodelle könnten z. B. stärker konsolidierte staatliche Strukturen, vermischte Strukturen wie z. B. in »Shared Service«-Institutionen oder auch marktorientierte Bündelungsstrukturen sein. In der Diskussion entsprechender Modelle bzw. Strukturveränderungen finden sich jedoch (noch) Vorbehalte gegenüber eventuell zu starken (und damit nachteiligen) Konsolidierungen bzw. Konzentrationen im öffentlichen IT-Sektor:

- Entsprechende Barriereargumente resultieren vor Allem aus der außerordentlichen Kleinteiligkeit deutscher föderaler Verwaltungsstrukturen in Verbindung mit der verwaltungsspezifischen Aufgabenorientierung. Da strukturelle Bündelungsprozesse im öffentlichen Sektor üblicherweise durch komplette Aufgabenverlagerungen stattfinden (Verbandsbildungen) oder aber durch komplexe Governance-Anforderungen belastet sind (Aufgabengewährleistungsverantwortung bei Fachthemenverwaltung in Verbindung mit der Aufsicht gegenüber dritten aufgabendurchführenden Institutionen), werden speziell Steuerungs- und Verantwortlichkeitsprobleme für kleinere Behörden befürchtet. Gleichzeitig — bei »Shared Service«-Konstruktionen — implizieren großzahlige Basisverwaltungsstrukturen bei wenigen (großen) IT-Institutionen eventuelle Balanceprobleme.[3]

  Föderale Strukturen: Steuerungs- und Verantwortlichkeitsprobleme für kleinere Behörden.

- Weitere Unsicherheiten bei der Bestimmung angemessener Konsolidierungsgrößen ergeben sich auch aus der fachlichen Vielfalt im öffentlichen Sektor. Über alle Infrastruktur-IT-Aufgaben hinaus stellen die IT-Anwendungen der Fachverwaltungen den Kern öffentlicher IT dar. In der historischen Entwicklung ist die heutige Vielfalt und auch das Angebot der zurzeit anerkannten Standards bei IT-Fachapplikationen in einem Entwicklungswettbewerb dezentraler Strukturen entstanden, wobei ggf. unterschiedlichen Kontexte und auch (z. B. landes-) gesetzliche Vorgaben zu einer oftmals positiv wahrgenommenen Entwicklungsbreite beigetragen haben. In diesem Zusammenhang wird durchaus kritisch hinterfragt, inwieweit gebündelte (Groß-) Strukturen die Innovations- und Dezentralitätsvorteile heutiger Strukturen beeinträchtigen und damit auch nachteilige Effekte haben.

  Entwicklungsbreite bzw. Innovations- und Dezentralitätsvorteile heutiger Strukturen.

Die Überlagerung funktional-prozessualer Fragen durch entsprechende institutionenorientierte Problemdiskussionen macht es schwierig, zu

[3] Die heute ausgeprägten nach Verwaltungsebenen und ferner regional differenzierten IT-Fachverwaltungsstrukturen können in diesem Zusammenhang auch als kontextbezogen differenzierte Bündelungsstrukturen verstanden werden. Während Bund und Landesverwaltungen mit vergleichsweise wenigen Behörden hier geringere Abstimmungs-, Koordinations- und Balanceprobleme haben, ist die für Kommunen vorgehaltene IT-Fachverwaltungslandschaft deutlich breiter aufgestellt, um hier der größeren Anzahl von Schnittstellen und auch den Belangen kleiner und kleinster Behörden besser entsprechen zu können.

konkreten Lösungsmodellen und -empfehlungen zu kommen. Die Erfahrung mit bisherigen Veränderungstrends bei der Reorganisation von Aufgabenteilungen bei öffentlichen Aufgaben zeigt, dass entsprechende Strukturdiskussionen nur eingeschränkt ergiebig sind.

Insoweit wollen wir an dieser Stelle nachfolgend die Perspektive verändern und nunmehr die Überlegungen institutionen- bzw. rollenorientiert fortführen.

II.1.2 Institutionenperspektive (Rollenorientierung)

Unabhängig von einer funktional-prozessorientierten Betrachtung kann man für die Beschreibung von Cloud-Computing-Ansätzen eine stärker rollenorientierte Unterscheidung vornehmen:

Rolle der Behörde: Besteller, Rolle des Cloud-Anbieters: Lieferanten.

1. Dabei ist die Behörde bzw. die jeweilige Verwaltungsinstitution die beziehende oder bestellende Stelle im arbeitsteiligen Leistungsprozess (Besteller) und
2. der Cloud-Computing-Dienstanbieter die in einem Fremdbezugsverhältnis liefernde Stelle (Lieferant).

Insgesamt wird die Cloud Konstruktion also als ein Kontraktverhältnis für den (Fremd-)Bezug von Diensten eingeordnet. Dabei ist bei einer solchen institutionen- bzw. rollenorientierten Sicht ganz unerheblich, in welchem strukturellen Verhältnis Besteller und Lieferant zueinander stehen. Dies schließt auch eventuelle. »Shared Service«-Strukturen mit einem Engagement des Bestellers als (Mit-)Träger der Lieferanteninstitution ein.

SLAs zur ergebnisorientierten Steuerung widersprechen bestehenden hierarchischen Steuerungsformen bzw. Governance-Mechanismen.

Im Verhältnis zwischen Besteller und Lieferant sind entsprechende Steuerungsmechanismen erforderlich. Das kann nur über hinreichend spezifizierte Leistungsvereinbarungen realisiert werden.[4] Dabei regeln Dienstverträge oder SLAs[5] das Verhältnis zwischen Besteller und Lieferant. Auf der Basis der SLAs erfolgt eine ergebnisorientierte Steuerung, indem detailliert Qualität, Mengen, Preise etc. vertraglich vereinbart sind.[6] Für die öffentliche Verwaltung in Deutschland sind vertraglich gestaltete Steuerungsmechanismen für die Arbeitsteilung von Leistungserstellungsprozessen trotz der Erfahrungen des Neuen Steuerungsmodell (NSM) weitestgehend neu. Sie können unabhängig von ihrer konkreten Ausprägung als ein Paradigmenwechsel für institutionelle Gestaltungsformen betrachtet werden, da bestehende hierarchische Steuerungsformen bzw. Governance-Mechanismen in Frage gestellt werden. Denn nach der Legitimationsvorstellung der traditionellen Staatsorganisation werden durch die Herauslösung von (Teil-) Prozessen vertikal-hierarchische Legitimationsketten durchbrochen,[7] da unmittelbare Einflussmöglichkeiten auf die Handlungsausführung durch die Ergebnissteuerung reduziert werden.

[4] Vgl. (Fischer u. Sterzenbach, 2006).

[5] Vgl. Abschnitt I.1.4.

[6] Vgl. (Colman, 2006; Walther, 2006).

[7] Vgl. (Schuppan, 2006, 2007).

Allerdings sind in der allgemeinen Public-Management-Diskussion eher umfassendere Produkte als Steuerungsobjekt vorgesehen und nicht einzelne Services (oder Prozessteile davon), wie sie in Cloud Computing-Ansätzen umgesetzt werden. Auch ist es prinzipiell unstrittig, dass Behörden im Wege der Beschaffung arbeitsteilig mit externen Dritten zusammenarbeiten können. Insoweit ist es eher eine graduelle und gegebenenfalls auch eine aus dem speziellen Aufgaben- bzw. Rechtsverständnis zu beantwortende Frage, in wie weit bestimmte Arbeitsteilungen mit externen Dritten zu Problemen der Steuerbarkeit führen.

II.1.3 Entwurf eines Cloud-Computing-Bezugsrahmens

Um zu verstehen, welche Faktoren in welcher Art und Weise die Nutzung von Cloud-Computing durch die öffentliche Verwaltung bestimmen, greifen wir die eingangs diskutierten in diesem Kapitel bedeutsamen Definitionsmerkmale

Konstituive Cloud-Eigenschaften, die in diesem Kapitel relevant sind.

- institutionenübergreifendes Pooling von IT-Ressourcen (Hardware, Entwicklungsplattformen und elektronische Dienste),
- virtuelle Bereitstellung/Nutzung und
- Netzbasierte Nutzung (»remote«, etwa über das Internet oder ein dediziertes Netzwerk)

auf[8] und stellen jeweils einen Bezug her

1. zu den vorstehend unterschiedene Perspektiven »Prozess« (Funktionen) und »Rolle« (Institutionen) und
2. zu in vier Gruppen zusammengestellten Bestimmungsfaktoren, die sich aus der Funktionen- und Institutionen-Perspektive ableiten lassen.

Bestimmungsfaktoren für Gestaltungs- und Handlungsoptionen in öffentlichen Institutionen.

Die dabei hier verwendeten vier Bestimmungsfaktoren-Gruppen

- rechtliche Zulässigkeit,
- (wirtschaftliche) Vorteilhaftigkeit,
- Steuerbarkeit und
- Risikobeherrschbarkeit

spiegeln dabei Gestaltungs- bzw. Handlungsebenen wider, die für Entscheidungen öffentlicher Institutionen über die Nutzung vonCloud-Computing relevant sind.

II.1.3.1 Bestimmungsfaktorengruppe »rechtliche Zulässigkeit«

Die rechtliche Zulässigkeit ist eine selbstverständliche und strenge Bedingung für eine entsprechende Nutzung von Cloud-Computing. Für die öf-

[8] Vgl. Abschnitt I.1.2.

fentliche Aufgabenwahrnehmung sind neben der generellen rechtlichen Zulässigkeit vor allem drei rechtliche Bereiche[9] als Bestimmungsfaktoren wichtig:

Fachspezifisches Recht: Steuerrecht, Verfassungsrecht, usw.

- In sog. fachspezifischem Recht — z. B. dem Steuerrecht — sind behördliche Zuständigkeiten sowie die jeweilige Aufgabenwahrnehmung bindend geregelt. In regulatorischer Hinsicht sind hier u. a. auch Vorgaben des Verfassungsrechts zu beachten, insbesondere zum Umgang mit Vorgängen, die für die nationale Sicherheit von Bedeutung sind, sowie allgemein zur Durchführung staatlicher Aufgaben durch Dritte.

Verwaltungsverfahrensrecht: Regelungen zur Aufgabendurchführung.

- Im Verwaltungsverfahrensrecht sind bindende Regelungen für die Aufgabendurchführung enthalten, und zwar bis gegebenenfalls hin zur detaillierten Ausgestaltung von Prozessen. Dabei gibt es allgemeine Verwaltungsverfahrensregelungen und in einer Vielzahl von Fällen auch gesetzliche und Rechtssprechungs-Anforderungen zu Fachgebieten.

Rahmenrecht: Insbesondere Datenschutz- und Vergaberecht.

- Als sog. Rahmenrecht sind allgemeine Rechtsvorschriften — und im Zusammenhang mit eGovernment ist vor allem das Datenschutzrecht hervorzuheben — zu beachten. Daneben stellen sich bei der Beauftragung Dritter (Fremdbezug von IT-Leistungen) regelmäßig vergaberechtliche Fragen.

Die genannten rechtlichen Bestimmungsfaktoren leiten sich in der Funktionalperspektive aus der behördlichen Aufgabenverantwortung und in der Institutionenperspektive aus Steuerungsanforderungen ab.

II.1.3.2 Bestimmungsfaktorengruppe »(wirtschaftliche) Vorteilhaftigkeit«

Die wirtschaftlichen Verbesserungspotenziale werden in der Literatur als Hauptargument für die Umsetzung von Cloud-Computing-Ansätzen hervorgehoben. In öffentlichen Institutionen spielen ökonomische Zieldimensionen dabei eine deutlich weniger große Bedeutung als in Unternehmen. In keinem Falle lassen sich existentielle Institutionsrisiken ableiten. Insoweit ist auch das substantielle Hauptargument für privatwirtschaftliche Unternehmen, an Bündelungs- bzw. Industrialisierungstrends teilzunehmen, für den öffentlichen Sektor nur eingeschränkt relevant.

Ökonomische Vorteile sind kein zwingender Grund für Strukturveränderungen.

Ungeachtet dessen, dass Kostensenkungs- und Wirtschaftlichkeitssteigerungsbemühungen vermutlich durchgängig zu den Oberzielen in deutschen Verwaltungsinstitutionen gehören, ist das Vorliegen entsprechender Potentiale noch lange kein zwingender Grund für Strukturänderungsentscheidungen, wie sie mit der Nutzung von Cloud-Computing einhergehen (Bündelung/Verlagerung). Denn strukturelle Änderungen — insbesondere solche, die mit Übertragungen von Aufgabenbestandteilen und gegebenenfalls der Begründung neuer Verwaltungsinstitutionen verbunden sind — bedürfen eines legislativen Verfahrens und greifen zudem tief in die aus politischer Willensbildung erwachsene gegebene

[9] Aus nationaler und europäischer Gesetzgebung sowie Rechtsprechung.

Gesamtstruktur von Verwaltungen ein. Der damit verbundene Aufwand und auch die Unsicherheiten, ob nicht andere politisch relevante Zieldimensionen gegen entsprechende Strukturanpassungen sprechen, stellen grundsätzliche Barrieren für solche Entscheidungen dar. Zudem sind Strukturentscheidungen im öffentlichen Sektor in der Regel langfristig wirksamer als entsprechende institutionelle Transformationen im Privatsektor.

Trotzdem: Wenn Verwaltungen IT-Infrastrukturen und IT-Dienstangebote über eine Cloud nutzen, dann brauchen sie sich u. a. nicht um die Beschaffung von Ressourcen, die Wartung, Lizenzen und Versionen zu kümmern. Sie können sich stattdessen stärker auf das Kerngeschäft und die Fachprozesse konzentrieren. In einer engeren ökonomischen Betrachtung ist dabei zu prüfen, welche operativen und strategischen Nutzenpotenziale dadurch erschließbar sind. In diesem Zusammenhang ist auch zu beleuchten, wie durch Veränderung der Geschäftsmodelle hinzuwachsende Kosten/Aufgaben (z. B. Kontrahierung, Qualitätssicherung usw.) sowie Risiken zu bewerten sind (z. B. Betreiber-/Ausfallrisiken, Kompetenzrisiken usw.).

Bestimmungsfaktoren der Gruppe »wirtschaftliche Vorteilhaftigkeit«.

Als einzelne Bestimmungsfaktoren in der Gruppe »(wirtschaftliche) Vorteilhaftigkeit« unterscheiden wir hier wiederum drei:

Leistungsadäquanz: Ist das Aufgabenergebnis und die Aufgabendurchführung grundsätzlich gewährleistet?

- Unter Leistungsadäquanz verstehen wir das Kriterium, ob bestimmte Gestaltungsformen der Aufgabenwahrnehmung (z. B. mit Nutzung von Cloud-Computing) es ermöglichen, die qualitativen Anforderungen an Aufgabenergebnis und Aufgabendurchführung zu gewährleisten. Die Hervorhebung dieses Kriteriums für die öffentliche Aufgabenwahrnehmung rechtfertigt sich, weil die qualitative Aufgabenwahrnehmung rechtlich vorgegeben ist, also nicht wie in wirtschaftlichen Kontexten zur Umsetzung eines bestimmten Effizienzniveaus variierbar ist.

Kosteneffizienz im öffentlichen Bereich bedeutet Kostenminimierung.

- Das Kriterium der Kosteneffizienz erwächst aus dem Wirtschaftlichkeitsgebot für Verwaltungshandeln. Es ist im öffentlichen Bereich grundsätzlich als Kostenminimierungskriterium auszulegen,[10] d. h. bei gegebenem Aufgaben- und Leistungsumfang sind Gestaltungsformen mit minimalen Kosten zu wählen.

Kamerale Effizienz bezieht sich auf den Haushalt einer Institution.

- Über die reine Kosteneffizienz hinaus ist als dritter Faktor dieser Gruppe auch die sog. kamerale Effizienz zu berücksichtigen. Kamerale Effizienz ist ein Konstrukt der Einnahmen-Ausgabenebene. In ihr wird zusätzlich berücksichtigt, inwieweit durch Gestaltungsdispositionen erhöhte punktuelle Haushaltsbelastungen (z. B. durch Investitionen) entstehen oder vorhandene Ausgabenbindungen (z. B. im Personalbereich) haushaltswirksam reduziert werden können. In einem weiten Verständnis sind beim Faktor kamerale Effizienz auch die mittel- und langfristigen Finanzwirkungen bei der Wahl von Cloud-Computing-Lösungen zuzuordnen (z. B. Vorhaltekosten, Risiken).

[10] Im Gegensatz zum Unternehmenskontext, wo daneben auch Optimierung nach Leistungsmaximierungskriterien (bei gegebenen Kosten) gebräuchlich sind.

Die Faktoren der Gruppe (wirtschaftliche) Vorteilhaftigkeit leiten sich primär aus der Funktionalperspektive und hier speziell den Bündelungsmotiven ab.

II.1.3.3 Bestimmungsfaktorengruppe »Steuerbarkeit«

Aus der speziellen Aufgabenverantwortungsausprägung im öffentlichen Bereich ergibt sich die hohe Bedeutung der Bestimmungsfaktorengruppe »Steuerbarkeit«. Wir unterscheiden hier drei einzelne Faktoren:

Ergebnissteuerung: Steuerung der Qualität der Aufgabenerfüllung.

- Die Ergebnissteuerung bildet die Pflicht der jeweiligen Behörde ab, in qualitativer Hinsicht eine den gesetzlichen Vorgaben entsprechende und damit rechtssichere Verwaltungsleistung nachzuhalten. M. a. W. sind öffentliche Institutionen also nicht nur verantwortlich für die letztliche »Qualität« ihrer Verwaltungsdienstleistungen, sondern müssen bei der Gestaltung der Aufgabenwahrnehmung auch absichern, dass sie diese »Qualität« auch selbst steuernd beeinflussen können. Aus diesem Grund stellen die Leistungsspezifikationen und gegebenenfalls Qualitätskontrollen regelmäßig einen gewichtigen Gegenstand der SLA's dar.

Durchführungssteuerung: Einhaltung spezifischer Vorgaben während der Aufgabendurchführung.

- In direktem Bezug dazu steht die Durchführungssteuerung, weil entsprechend gesetzlicher Vorgaben Behörden ebenso sicherstellen müssen, dass spezifische Vorgaben im Leistungserstellungsprozess streng eingehalten werden.

Übergreifende Steuerung: Aufgabenunabhängige Steuerung (z. B. Sicherstellung vergaberechtlicher Regelungen).

- Der weitere Faktor »Übergreifende Steuerung« bezieht sich auf die jenseits einzelner Aufgaben bzw. Verwaltungsprodukte durch Behörde wahrzunehmenden Steuerungspflichten. Dazu gehört u. a. die Einhaltung vergabe- und wettbewerbsrechtlicher Regelungen bei der Auswahl und Beauftragung von Cloud-Anbietern. In einem strategischen Kontext ist die thematische Verantwortung einer Behörde zu nennen, z. B. bei der Ausgestaltung von Vorhaltekompetenzen entsprechend ihrer Zuständigkeit.

Die Kriterien der Gruppe Steuerbarkeit leiten sich in der Funktionalperspektive vor allem aus Bündelungsbarrieren ab sowie in der Institutionenperspektive aus dem (für Cloud-Computing-Ansätze zu unterstellende) Steuerungsbedarf bei Fremdbezug. Grundsätzlich sind Steuerungskriterien bei Cloud-Ansätzen besonders relevant, weil sie immanent einhergehen mit Aufgabenbündelungen und Arbeitsteilungen mit Dritten. Dabei erhalten die Steuerungsprobleme unterschiedliche Relevanz in Abhängigkeit von der Partnerwahl (im öffentlichen Bereich oder aber bei Einbeziehung privatwirtschaftlicher Partner bzw. Anbieter).

Standardisierte Verträge und effektives Controlling sind eine Voraussetzung für die Steuerbarkeit von Gestaltungsformen, die auf Cloud-Computing zurückgreifen.

Bei der Steuerung ist zu berücksichtigen, dass bei Cloud-Ansätzen gegenüber bisherigen Formen der Leistungserstellung mit höheren Aufwänden zu rechnen ist. Insbesondere entstehen Transaktionskosten durch die Anbahnung, Abwicklung, Kontrolle und Anpassung von Verträgen.[11] Bei Kostenvergleichen sind deshalb nicht nur Produktions-, sondern auch Transaktionskosten zu berücksichtigen. Erst wenn diese in der Summe

[11] Vgl. (Picot, 2003, S. 270).

geringer sind und der Nutzen höher ist als bei anderen zur Verfügung stehenden Arrangements, kommen sie als Organisationsform in Betracht. Dabei spielt die Standardisierung von Verträgen sowie die Möglichkeiten des IT-Einsatzes eine wichtige Rolle. Denn sowohl die Standardisierung von Verträgen als auch IT-Controllingsysteme können wesentlich dazu beitragen, Anbahnungs- und Kontrollkosten zu reduzieren.

II.1.3.4 Bestimmungsfaktorengruppe »Risikobeherrschbarkeit«

In engem Zusammenhang mit den Faktorengruppen »rechtliche Zulässigkeit« und »(wirtschaftliche) Vorteilhaftigkeit« steht die Bestimmungsfaktorengruppe »Risikobeherrschbarkeit«. Wir unterscheiden hier wieder drei Faktoren:

- Unter Rechtsrisiko verstehen wir die Gefahr, dass es in Bezug auf eine gewählte Gestaltung der Aufgabenwahrnehmung unter Verwendung des Cloud-Computings entweder insgesamt oder aber in Bezug auf einzelne Verwaltungsakte zu nicht rechtssicheren Leistungsergebnissen kommt. Dies schließt Verfahrensfehler ein.

  Rechtsrisiko: rechtsunsichere Ergebnisse, z. B. Verfahrensfehler.

- Das Effizienzrisiko hinsichtlich des Cloud-Computings besteht im Wesentlichen darin, dass die angestrebten wirtschaftlichen Verbesserungseffekte in toto nicht realisiert werden können. Dabei sind in diesem Faktor auch die Folgekosten von Verfahrensumstellungen — z. B. hinsichtlich ganzer Behördenstrukturen — zu berücksichtigen.

  Effizienzrisiko: Wirtschaftliche Verbesserungseffekte kommen nicht zum Tragen.

- Ein eigenständiges Risiko aufgrund der Einbeziehung Dritter in die Aufgabenwahrnehmung ist das Abhängigkeitsrisiko. Damit ist gemeint, dass bei Auslagerungen von (Teil-) Prozessen spezielle Risiken entstehen, wie z. B. Kompetenzverluste, Leistungs-/Kostenrisiken bei Partnerwechsel oder Missbrauchsrisiken.

  Abhängigkeitsrisiko: Kompetenzverluste, Probleme beim Partnerwechsel, Mißbrauch.

Über den engen Zusammenhang von Aufgabenverantwortung/rechtliche Zulässigkeit und Risiko besteht eine Interdependenz zur Bestimmungsfaktorengruppe Steuerbarkeit, weil die Begrenzung von Risiken i. d. R. durch das Vorhalten leistungsfähiger Steuerungssysteme zu erfolgen hat.

II.1.3.5 Relevanz der Bestimmungsfaktorengruppen

In Abb. II.1.2 haben wir grafisch die Ableitung der Bestimmungsfaktoren aus Funktionalperspektive und Institutionenperspektive dargestellt.

Dabei zeigt sich bereits — aus der Häufung von Pfeilverbindungen nachvollzogen — die besondere Relevanz von rechtlicher Zulässigkeit sowie von Steuerbarkeitsfragen. Wenn man nun — wie gezeigt — die drei an dieser Stelle relevanten konstituiven Definitionsmerkmale des Cloud-Computings in einen Bezug zu den Ableitungen setzt, wird deutlich, dass die überwiegende Anzahl von Bezügen sich auf der Definitionsebene »Pooling« ergibt. Wenn man diese Häufung interpretiert, kommen wir zu

dem Befund, dass hier die grundsätzlichen Probleme einer (institutionenübergreifenden) Bündelung und Verlagerung öffentlicher Aufgaben abgebildet werden. M. a. W. handelt es sich hier nicht um speziell mit Cloud-Computing verknüpften Bestimmungsfaktoren-Prüfungen, vielmehr treten die gleichen Bezüge auch bei jeder anderen Gestaltung von Aufgabenwahrnehmungen mit Dritten (z. B. bei »Shared Service«-Modellen) auf.

Hingegen weisen die Bezüge der beiden anderen Definitionsebenen

- »virtuell« (virtuelle Bereitstellung) und
- »remote« (netzwerkbasierter Zugang, z. B. über das Internet)

auf spezifisch für Cloud Computing-Ansätze geladene Bestimmungsfaktoren hin.

Welche Bestimmungsfaktoren sind relevant?

Diesen Abschnitt abschließend kann an dieser Stelle thesenartig herausgearbeitet werden, wo besonders relevante Bestimmungsfaktoren speziell für Gestaltungsmodelle mit Cloud-Computing liegen. Entsprechend der Kennzeichnung in Abb. II.1.2 liegen diese Bezüge vor Allem bei nachfolgenden Bestimmungsfaktoren:

Cloud-Computing widerspricht dem heutigen Verwaltunsverfahrensrecht zugrundeliegenden Paradigmen. Kann dieser Widerspruch durch SLAs aufgelöst werden?

1. Rechtliche Zulässigkeit/**Verwaltungsverfahrensrecht**: Gleichermaßen aufgrund von Virtualisierung und des netzwerkbasierten Zugangs verändert die Umsetzung von Cloud-Ansätzen die Besitz- und Berechtigungsstrukturen wesentlicher Bestandteile des Leistungserstellungsprozesses sowie von Datenbeständen. Es ist davon auszugehen, dass verfahrensrechtliche Vorgaben und Restriktionen heute noch von ganz anderen Paradigmen und Prozessmodellen für Verwaltungsverfahren ausgehen. Deshalb ist anzunehmen, dass verfahrensrechtlich Unsicherheitsräume oder Nichtanwendbarkeitsschwierigkeiten bei der Umsetzung von Cloud-Ansätzen entstehen und hinsichtlich einer stärkeren Nutzung von Cloud-Computing bearbeitet werden müssen. Besonders zu prüfen ist, ob entsprechende Unsicherheiten/Nichtanwendbarkeiten im Rahmen von SLAs hinreichend regelbar sind, oder ob es hier rechtlichen Handlungsbedarf gibt.

Datenschutz und Vergaberecht.

2. Rechtliche Zulässigkeit/**Rahmenrecht**: rahmenrechtlich erscheint besonders die Datenschutzproblematik bei der Auslagerung von Daten in die Clouds diskussionswürdig. Darüber hinaus ergibt sich eine hohe Relevanz vergaberechtlicher Fragen, die im Kern wiederum auf den Regelungsbedarf und die Regelungsmöglichkeiten mit dem Instrument SLA hinauslaufen.

Führt Cloud-Computing zu grundlegend veränderten behördlichen Zuschnitten und Paradigmen?

3. (Wirtschaftliche) Vorteilhaftigkeit/**kamerale Effizienz**: während grundsätzliche Effizienzprüfungen für Cloud-Ansätze kaum unterschiedlich zur Bewertung anderer Bündelungsformen stattfinden dürften, ergibt sich aus dem Definitionsmerkmal »virtuell« und aus der Funktionalperspektive »Kompetenzbündelung« die spezielle Frage, inwieweit die Nutzung von Cloud-Computing-Ansätzen zu grundlegend veränderten behördlichen Zuschnitten und Paradigmen führen (und im Zusammenhang damit die Frage, ob dies strategisch erwünscht ist).

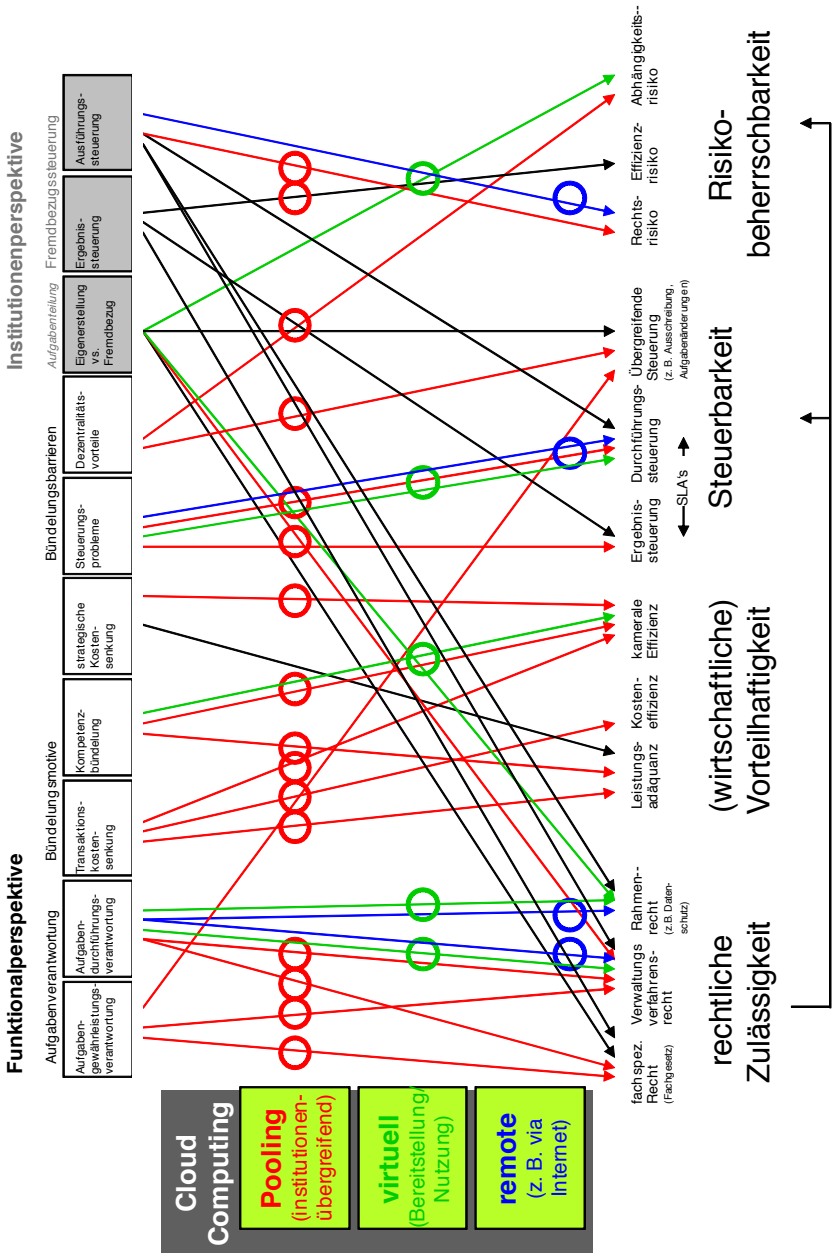


Abbildung II.1.2
Entwurf eines Bezugsrahmens (eigene Darstellung).

Verhindern Virtualisierung und Neztwerkzugriff eine effektive Durchführungssteuerung?

4. Steuerbarkeit/**Durchführungssteuerung**: Die virtuelle und mit Netzwerkzugang ausgestaltete Cloud-Computing-Ausgestaltung wirft grundlegend (und massiv) die Frage auf, ob und wie hier überhaupt noch eine Steuerbarkeit durch die verantwortliche Behörde gewährleistet werden kann.

Sind Verfahrensfehler kontrollierbar bzw. nachvollziehbar?

5. Risikobeherrschbarkeit/**Rechtsrisiko**: hinsichtlich der Risikobeherrschbarkeit ergeben sich insbesondere Rechtsrisikofragestellungen, und zwar primär mit Fokus auf die Nachvollziehbarkeit und durch Systeme beherrschbare Verfahrensfehler.

Diese fünf grobe Theseneinordnungen erscheinen dabei ggf. weiter differenzierbar nach Dienstklassen und Betriebsmodellen.

Cloud-Computing wirft im wesentlichen Fragen nach den Risiken auf; wirtschaftliche Erwägungen spielen eine untergeordnete Rolle.

Bereits an dieser Stelle wird sehr deutlich, dass insgesamt die Fragestellung des Cloud-Computing in der öffentlichen Verwaltung eine »Risikofragestellung« ist. Denn — bei gegebenem bzw. auch zukünftig anpassbarem Rechtsrahmen — ergeben sich praktisch keine spezifischen Fragestellungen hinsichtlich grundsätzlicher wirtschaftlicher Vorteilhaftigkeit. Im Gegenteil: Sowohl bisherige Literatur- und Praxisberichte als auch die in dieser Studie ebenfalls im Kapitel I.2 dokumentierten Erwartungen der Nutzer hinsichtlich Dienst-Auslagerungen lassen kaum Zweifel zu, dass das Outsourcing und die Bündelung selbst durchgängig mit hohen Vorteilserwartungen verknüpft ist. Weil Cloud-Computing-Ansätze ja aufgrund der deutlich besseren (multilateralen) Kapazitätsnutzungskosten von Infrastruktur und Diensten grundsätzlich höhere Effizienzniveaus (im Vergleich zu »klassischen« Bündelungen z. B. als bilateraler »Shared Service«) unterstützen, ist ceteris paribus davon auszugehen, dass bei geeigneten Geschäftsmodellen eine hohe Attraktivität für die öffentliche Verwaltung besteht, Cloud-Ansätze intensiv zu nutzen.

Insoweit konzentriert sich die nachfolgende Untersuchungsarbeit dieser Studie folgerichtig auf die Möglichkeiten der Verwaltung, eine solche (intensive) Nutzung auch umzusetzen. Unmittelbar folgend sei deshalb zuerst ein Blick auf die heutigen rechtlichen Rahmenbedingungen geworfen, also insbesondere auf explizite rechtliche Regelungen, die Cloud-Computing-Nutzungen betreffen (Kapitel II.2). Diesen Rahmen (zunächst) voraussetzend, richtet sich die Perspektive dann im Teil III auf die Risiken des Cloud-Computing aus einer anwendungstechnisch-konstruktiven Sicht.

KAPITEL II.2

Rechtliche Rahmenbedingungen

Zusammenfassung

Im Bereich der öffentlichen Verwaltung gibt es erhebliche Bedenken gegenüber Cloud-Computing, die zum einen darin begründet sind, dass besonders öffentliche Verwaltungen prinzipiell eine Schutzpflicht personenbezogener Daten haben, in ihrer Verantwortung gegenüber den Bürgern, die ihnen diese Daten anvertrauen. Aber auch aus einer grundsätzlichen Betrachtung heraus lassen die Potentiale der Auslagerung von Prozessen Behörden zurückschrecken, einerseits aus Angst vor Verlust von Know-how, andererseits müssen bestimmte Kernaufgaben in der Verwaltung bleiben. Da es sich bei Cloud-Computing um eine Art von »Outsourcing« handelt, können eine Reihe von rechtlichen Fragen in diesem Zusammenhang beantwortet werden. Da es sich beim Cloud Computing aber auch um Kooperationen — innerhalb und zwischen Verwaltungen (und Privatwirtschaft) — handelt, spielen auch hier Fragen der Kooperationsformen eine Rolle, die über gesetzliche Einschränkungen hinausgehen und durchaus Anlass für neue Fragestellungen geben. Im Vorkapitel II.1 sind die rechtliche Bedingungsfaktoren bereits schematisch eingeordnet worden. Dieses Kapitel gibt nun einen speziellen Überblick zu den rechtlichen Rahmenbedingungen ohne den Anspruch auf Vollständigkeit.

II.2.1 Generelle Rechtsfragen bei IT-Kooperationen

In Anlehnung an (Kammer u. Schulz, 2010) sind als rechtliche Kernfragen über die insbesondere beim Cloud-Computing inhärenten Datenschutzprobleme[1] hinaus vor allem

- organisationsrechtliche,
- vergaberechtliche und
- spezialrechtliche

Regelungen zu diskutieren.

Organisationsrecht. Organisationsrechtlich bestehen insbesondere Fragen zum Verwaltungskooperationsrechts (z. B. um einen Verwaltungsverband) oder nach Flexibilisierungen vorhandener Organisations- und Gesellschaftsformen. Dazu gehören auch Fragen der Beteiligung Privater an öffentlich-rechtlichen Rechtsformen, und auch der Nutzbarmachung von Rechtsformen des Privatrechts für die öffentliche Hand. Ferner werden bei Kooperationen immer wieder die Verbote unzulässiger Mischverwaltung problematisiert. Dazu gehört das Problem, ob und inwieweit IT (oder ihre Verlagerung auf einen Dritten bzw. die gemeinschaftliche Erbringung) sich auf die Verwaltungsentscheidung auswirkt und daher demokratisch-rechtsstaatlich bedenklich erscheint.

In diesem Zusammenhang ist die Diskussion um eventuelle Neubewertungen im Kontext des Art. 91c GG noch im Anfangsstadium, über den ja ebenfalls die Zulässigkeit von Kooperationen (speziell im IT-Bereich) konstruierbar ist. Dabei sind allerdings der Anwendungsbereich (Bund/Land, Land/Land-Zusammenarbeit, Rolle der Kommunen und sonstiger Selbstverwaltungsträger) und die Gegenstände der Zusammenarbeit (»informationstechnische Systeme«) noch weitgehend unspezifiziert.

Aufgabenwahrnehmung. Die hier insgesamt zu berücksichtigende Kernproblematik der verfassungsrechtlich problematischen Preisgabe von Entscheidungskompetenzen beginnt dort, wo den beteiligten Verwaltungsträgern eine Änderung des Verwaltungsverfahrens oder der Verwaltungsorganisation und damit die eigenverantwortliche Aufgabenwahrnehmung unmöglich gemacht wird. Eigenverantwortliche Aufgabenwahrnehmung setzt nach dem Bundesverfassungsgericht voraus, *»dass der jeweils zuständige Verwaltungsträger auf den Aufgabenvollzug hinreichend nach seinen eigenen Vorstellungen einwirken kann«*. Daran fehle es in der Regel, *»wenn Entscheidungen über Organisation, Personal und Aufgabenerfüllung nur in Abstimmung mit einem anderen Träger getroffen werden können«*. Allerdings kann man davon ausgehen, dass sich diese strenge Anforderung nur auf den Gesetzesvollzug im engeren Sinne richtet, also nicht auf die in Behörden auch sonstig zu erfüllenden Funktionen, wie etwa die erste Beratung und Betreuung im Front-Office, die Datenerhebung, -verarbeitung und -speicherung sowie zahlreiche Servicefunktionen. Schulz's Meinung nach gilt dieses im Grundsatz auch für das Cloud-Computing, welches sich letztendlich

[1] Vgl. hierzu nachfolgend Abschnitt II.2.2

als eine konsequente Fortschreibung oder Neuorganisation des kooperativen eGovernments darstellt. Im Zusammenhang mit der fortschreitenden Elektronisierung der Verwaltungsverfahren und der Verlagerung von (Teil-) Prozessen in gemeinsam genutzte Clouds ist jedoch zu beachten, dass die Vorgabe von Standards infrastruktureller Art, aber vor allem konkreter Softwareanwendungen, das zulässige Maß an Selbstbindung überschreiten kann.[2]

Vergaberecht.

Die allgemeinen vergaberechtlichen Probleme bei IT-Kooperationen, speziell auch bei Cloud-Computing-Migrationen, thematisieren insbesondere, ob eine vergaberechtsfreie Beauftragung möglich und damit eine hinreichend effektive und partnerschaftlich orientierte Zusammenarbeit realisierbar ist. An dieser Stelle soll auf diese spezielle Problematik nicht näher eingegangen werden, sondern auf vertiefte rechtliche Betrachtungen hierzu verwiesen werden (Schulz, 2010). Im Kern laufen die Überlegungen gegenwärtig darauf hinaus, dass bei Verbleib in staatlichen Organisationssphären (aller Partner) nicht von formalen, vergaberechtlichen Beschaffungsprozessen auszugehen ist. Andererseits muss auch hier die Rolle des Art. 91c GG bewertet werden. Bisher ungeklärt ist, ob er tatsächlich (wie im Rahmen des Gesetzgebungsprozess andiskutiert) vergaberechtliche Auswirkungen hat, in dem er die Zusammenarbeit im Bereich der IT als innerstaatlichen Organisationsakt vom Vergaberecht ausnimmt. Dabei stellt sich wiederum die Frage nach der konkreten Reichweite der Vorschrift. Schließlich ist auch noch zu klären, ob eine Anpassung der gesetzlichen Vorgaben — z. B. des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) — in der Lage wäre, die Zusammenarbeit der öffentlichen Hand vergaberechtlich zu privilegieren.

Spezialgesetzliche Regelungen.

Von nicht zu vernachlässigender Bedeutung — jedoch bisher kaum behandelt — sind Rechtsfragen, die daraus resultieren, dass IT-Kooperationen oder Cloud-Computing-Migrationen in spezialgesetzlich erfassten Bereichen realisiert werden. Während sich die organisations-, gesellschafts- und vergaberechtlichen Fragestellungen dort in der Regel in der gleichen Weise stellen, wie im Bereich der »allgemeinen Verwaltung«, existieren in spezialgesetzlich erfassten Bereichen vor allem spezifische datenschutzrechtliche Fragestellungen. So gibt es z. B. für die Leistungsträger nach dem Sozialgesetzbuch (SGB) eine spezielle Vorschrift zur Auftragsdatenverarbeitung, die die Einbindung privater (im Vergleich zu anderen öffentlichen) Stellen zusätzlich erschwert. In einigen Verwaltungsbereichen (Justiz, Polizei) wird zudem zu klären sein, ob eine Kooperation mit »anderen« Verwaltungsbereichen überhaupt zulässig ist; z. B. wird derzeit diskutiert, ob Standardisierungsbeschlüsse des IT-Planungsrates auch für die Justizverwaltung Geltung beanspruchen oder der Unabhängigkeit der Justiz entgegenstehen. Als entsprechend problematische Rechtsbereiche gelten heute mindestens das Sozialrecht, das Abgaben- und Steuerrecht, das Melderecht und der rechtliche Rahmen der Justiz- und Polizeiverwaltung.

Weiterhin stellt sich die Frage, ob eine organisatorische Zusammenfassung über »fachlichen Grenzen« hinweg in Betracht kommt, ob also die Begründung von IT-Kooperationen nicht nur im Bereich der allgemeinen

[2] Vgl. dazu (Schulz, 2010).

Verwaltung, sondern z. B. auch unter Einbeziehung von Sozialversicherungsträgern (und damit Sozialdaten) denkbar ist.

II.2.2 Datenschutz

Zielsetzung.

Die Zielsetzung des Datenschutzes ist in §1 des Bundesdatenschutzgesetz (BDSG) geregelt:

> *Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.*

Datenschutz bezieht sich nur auf personenbezogene Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Juristische Personen sind ausgenommen.

Anonymisierung und Verschlüsselung als datenschutzrechtliche Mittel.

Hinreichende Anonymisierung (z. B. durch Verschlüsselung[3]) von personenbezogenen Daten ist als datenschutzrechtliches Mittel vorgesehen. Allerdings ist fraglich, wann eine Datenanonymisierung hinreichend ist:

> *Da es aber heute keines unverhältnismäßig großen Aufwandes an Zeit, Kosten und Arbeitskraft mehr bedarf, um durch komplexe Verknüpfungen in Netzen nicht eindeutig identifizierende Daten einer bestimmbaren Person zuzuordnen, ändert allein der Umstand einer Verarbeitung in einer Cloud an der Anwendbarkeit des Datenschutzrechtes nichts. Eine Personenbeziehbarkeit ist bei Einzeldatensätzen zu Personen regelmäßig anzunehmen. Gerade die elektronische Auswertbarkeit und die Integration in ein möglicherweise weltweites Netzwerk erhöht die Wahrscheinlichkeit des Vorliegens von Zusatzwissen, das eine Identifizierung der Betroffenen ermöglicht.*[4]

Bindend für die Verarbeitung personenbezogener Daten sind die Regelungen des Bundesdatenschutzgesetzes (BDSG) bzw. gegebenenfalls landesspezifische Besonderheiten, die in den Landesdatenschutzgesetzen (LDSG) als Erweiterungen des BDSG geregelt sind. Darüber hinaus sind verschiedene bereichsspezifische Spezialgesetze gegenüber den Regelungen des BDSG und den LDSGen vorrangig (z. B. Sozialgesetzbuch, Straßenverkehrsgesetz, Meldegesetze, Polizeigesetze).

Europäische Datenschutzrichtlinie.

Weiterhin ist die 1995 verabschiedete Europäische Datenschutzrichtlinie[5] (EU-DSRL) insbesondere im Bezug auf Auftragsdatenverarbeitung außerhalb Deutschlands von Interesse.

Grundsätzlich liegt die Verantwortung für konkrete Verarbeitung personenbezogener Daten bei der Behörde, die entweder selbst diese Daten verarbeitet oder dies durch einen Auftrag (Auftragsdatenverarbeitung) durchführen lässt. Im Bereich der öffentlich-öffentlichen Kooperationen

[3] vgl. § 3 Abs. 6 BDSGgl. § 3 Abs. 6 BDSG.

[4] (Weichert, 2010).

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

dürfen Daten weitergegeben werden, bei einem Wechsel des Rechtsträgers ist allerdings der Grundsatz der Erforderlichkeit zu berücksichtigen.

II.2.2.1 Erforderlichkeit und Zweckmäßigkeit

Elektronischer Umgang mit personenbezogenen Daten setzt entweder ein Gesetz, das dies erlaubt, oder die Zustimmung der betroffenen Person voraus.

Im Allgemeinen ist die Erhebung, Verarbeitung und Speicherung personenbezogener Daten erlaubt, wenn dies

- entweder durch ein Gesetz erlaubt ist oder
- die betroffene Person eingewilligt hat.

Allerdings muss hierbei das Ziel verfolgt werden, die Menge der erhobenen Daten auf ein für die Aufgabenerfüllung der erhebenden Behörde absolut notwendiges Minimum zu reduzieren. Nach diesem Grundsatz der **Datensparsamkeit** und **Datenvermeidung** ist eine Datenerhebung bzw. -verabeitung unzulässig, wenn sie über die unmittelbaren Erfordernisse der Aufgabenerfüllung hinausgeht.

Zweckbindung.

Persönliche Daten dürfen nur zu einem zuvor definierten Zweck erhoben und verarbeitet werden; die Speicherung solcher Daten auf den Verdacht einer zukünftigen (dann rechtmäßigen) Verarbeitung ist unzulässig. Insbesondere dürfen personenbezogene Daten zwar für die Datenschutzkontrolle, die Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage erhoben und gespeichert werden, jedoch dann ausschließlich für diesen Zweck verwendet werden.

II.2.2.2 Automatisierte Einzelentscheidungen

§ 6a Abs. 1 BDSG sieht vor, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale[6] dienen. Hierzu zählen auch besondere Datenarten wie etwa Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Bei automatisierten (Online-) Abrufverfahren trägt die abrufende Stelle die Verantwortung für die Rechtmäßigkeit des Abrufs.[7]

II.2.2.3 Vorabkontrolle

Für spezifische Daten (vgl. Abschnitt II.2.2.2) ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen.[8] Manche LDSG sehen darüber hinaus eine grundsätzliche Vorabkontrolle personenbezogener Daten vor.

[6] D. h. nach § 4d Abs. 5 BDSG seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

[7] § 10 Abs. 4 Satz 1 BDSG.

[8] § 4d Abs. 5 BDSG.

II.2.2.4 Rechte der Betroffenen

Recht auf Auskunft, Berichtigung, Löschung, Sperrung, Widerspruch und Schadensersatz.

Die Rechte der Betroffenen sind nach BDSG bzw. den landesspezifischen Datenschutzgesetzen wie folgt definiert:

- Das Recht auf Auskunft über die zu ihrer Person gespeicherten Daten. Dieses Recht schließt auch ein, dass Auskunft über die Herkunft, die Empfänger oder Kategorien von Empfängern, an die personenbezogene Daten weitergegeben wurden, und den Zweck der Speicherung erlangt werden kann.
- Das Recht auf Berichtigung, wenn unrichtige Daten gespeichert werden
- Das Recht auf Sperrung, soweit die Unrichtigkeit der Daten nachgewiesen werden kann
- Das Recht auf Löschung, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden (falls Aufbewahrungsfristen zu beachten sind, eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigen würde oder nur mit unverhältnismäßigen Aufwand durchgeführt werden kann, müssen solche Daten gesperrt werden)
- Das Recht auf Widerspruch gegen die Datenverarbeitung, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift vorgeschrieben ist
- Das Recht auf Schadensersatz wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten

II.2.3 Datensicherheit und Auftragsdatenverarbeitung

Spezifische Schutzziele, die Datensicherheit betreffen, ergeben sich u. a. aus der Pflicht der Unternehmensleitung zur Risikovorsorge[9] sowie aus spezialgesetzliche Einzelregelungen.[10]

- Vertraulichkeit: Schutz vor unbefugter Informationswahrnehmung
- Unversehrtheit: Schutz vor ungewollter Informationsänderung
- Verfügbarkeit: Schutz vor Informationsverlust, -entzug und -blockade
- Gegebenenfalls weitere Schutzrichtungen (Verbindlichkeit, Authentizitat, Zurechenbarkeit)

Auftragsdatenverarbeitung innerhalb und außerhalb von Europa.

Die EU-DSRL hat die Zielsetzung, innerhalb des europäischen Binnenmarktes grenzüberschreitende Datenverarbeitung zu ermöglichen,[11] wo-

[9] §§ 91, 93 AktG, §§ 35, 43 GmbHG.

[10] § 25 a Abs. 2 KWG, § 33 Abs. 2 WpHG.

[11] Art. 1 Abs. 2 EU-DSRL.

bei allerdings ein ausreichendes Datenschutzniveau in dem Mitgliedsstaat, in dem die mit der Datenverarbeitung beauftragte Institution ihren Sitz hat, vorausgesetzt werden muss. Entscheidend für die Anwendbarkeit der EU-DSRL ist also nicht der Ort, an dem die tatsächliche Datenverarbeitung stattfindet: *Hat die Daten verarbeitende Stelle keine Niederlassung im EU/EWR-Raum, so kann nach § 1 Abs. 5 S. 3 BDSG ein im Inland ansässiger Vertreter benannt werden, dem gegenüber das anwendbare nationale Datenschutzrecht geltend gemacht werden kann.*[12]

Auftragsdatenverarbeitung außerhalb von Europa: Ausnahmen.

Auftragsdatenverarbeitung in Drittstaaten[13] ist nach der EU-DSRL grundsätzlich nicht ausgeschlossen: Voraussetzungen ist aber ein angemessenes Datenschutzniveau beim Empfänger,[14] das von der EU für bestimmte Staaten anerkannt ist (z. B. Schweiz, Kanada, Argentinien).

Weitere Ausnahmen sind:

- US-Unternehmen, die Safe Harbor Principles unterliegen.
- Das Vorhandensein bindender Unternehmensregelung beim Empfänger.
- Das Vorhandensein von EU-Standardvertragsklauseln (inklusive aller Unterauftragnehmer)
- Das Vorhandensein von Einzelverträgen mit behördlicher Genehmigung
- Interessenabwägung nach § 28 Abs. 1 BDSG

Insgesamt ergibt sich hinsichtlich der datenschutzrechtlichen und vor Allem auch der Auftragsdatenverarbeitungsfrage eine — u. a. auch von Schulz vorgeschlagene bzw. näher spezifizierte und rechtlich nur in Teilfragen zu beanstandene Ausgestaltungsform, wenn innerhalb des öffentlich-rechtlichen Bereiches Bündelungen eigenständige Rechtspersonen erfolgen.[15] Allerdings muss dieser Konzeptansatz noch seine Akzeptanz im Ausgestaltungsbereich des Art. 91c GG beweisen.

[12] (Weichert, 2010).

[13] D. h. solche Staaten, die nicht Mitglieder der EU sind bzw. außerhalb des Europäischen Wirtschaftsraums liegen.

[14] § 4 b Abs. 2 BDSG.

[15] Vgl. (Kammer u. Schulz, 2010) sowie dort angegebenen Quellen

Teil III

Beherrschbarkeit der Risiken

KAPITEL III.1

Risiko-Management

Zusammenfassung

Um den Begriff »Cloud-spezifisches Risiko« besser eingrenzen zu können, verwenden wir die folgende Klassifikation von Schwachstellen in Cloud-Systemen: Solche Schwachstellen sind Cloud-spezifisch, wenn

1. *sie immanenter Bestandteil oder weit verbreitet in den Cloud-Basis-Technologien sind, oder*
2. *durch Cloud-Innovationen verursacht werden, die bekannte und erprobte Gegenmaßnahmen unmöglich oder schwierig implementierbar machen, oder*
3. *ihren Ursprung in einer der Charakteristiken des Cloud-Computings haben.*

Unabhängig davon gibt es eine Reihe von Argumenten dafür, dass das Sicherheitsniveau in Cloud-Infrastrukturen deutlich gesteigert werden kann:

- *Skalierungseffekte sorgen dafür, dass Systeme weniger angreifbar sind, und dass Sicherheitsrichtlinien einfacher durchgesetzt werden können.*
- *Sicherheit kann zu einem Marktfaktor werden, der zur Entwicklung robusterer Dienste wie auch zur stringenten Implementierung von Sicherheitsmanagementsystemen führen kann.*
- *Schließlich können einige Sicherheitsfunktionen selbst als Cloud-Dienst angeboten werden.*

Sicherheit ist im Zusammenhang mit Cloud-Computing zur Zeit ein kontrovers diskutiertes Thema. Während einerseits argumentiert wird, dass

Cloud-Lösungen aufgrund vereinheitlichter Technologien, Ressourcenkonsolidierung und Marktanforderungen grundsätzlich ein gegenüber klassischen IT-Infrastrukturen erhöhtes Sicherheitsniveau bieten können, werden andererseits Sicherheitsbedenken als eines der Hauptargumente gegen den Einsatz von Cloud-Technologien angegeben.

Was genau sind Cloud-spezifische Risiken?

Die Zielsetzung dieses Kapitels ist es, eine Definition und Klassifizierung von Cloud-spezifischen Risiken zu finden, die als Grundlage für einen Risikomanagement-Ansatz für Cloud-Systeme dienen kann. Einige Grundlagen hierzu werden im zugeordneten Anhang D weiter ausgeführt; insbesondere wird dort der Begriff der »Schwachstelle« weiter untersucht. Weiterhin wird exemplarisch der Risikomanagement-Ansatz des US-amerikanischen National Institute of Standards and Technology (NIST, 2002) vorgestellt; ein deutsches Äquivalent, nämlich der BSI-Standard (BSI, 2008c), wird im Zusammenhang mit Cloud-Computing bereits in der Studie (Streitberger u. Ruppel, 2009) diskutiert.

III.1.1 Cloud-Computing aus der Sicherheitsperspektive

Indikatoren Cloud-spezifischer Schwachstellen: Immanent in den Basis-Technologien, durch Cloud-Innovation verursacht oder aus den Cloud-Eigenschaften herleitbar.

(Grobauer u. a., 2010) definiert eine Cloud-spezifische Schwachstelle durch die folgenden Indikatoren, wobei wenigstens eines der Merkmale zutreffen muss:[1]

1. Sie ist immanenter Bestandteil oder weit verbreitet in den Cloud-Basis-Technologien.
2. Sie wird durch Cloud-Innovationen verursacht, die bekannte und erprobte Gegenmaßnahmen unmöglich oder schwierig implementierbar machen.
3. Sie hat ihren Ursprung in einer der Charakteristiken des Cloud-Computings (vgl. Abschnitt I.1.2).

Ausgehend von dieser Charakterisierung werden für jedes Merkmal beispielhaft Schwachstellen aufgezeigt.

III.1.1.1 Schwachstellen in Cloud-Basis-Technologien

Risiken, die sich aus Ressouren-Vitualisierung, Web-basiertem Zugang und Kryptographie ergeben.

Die Basis-Technologien, die hier wesentlich sind, sind Ressouren-Vitualisierung (*virtual machines*), Web-basierter Zugang zu Cloud-Diensten und Kryptographie.

- **Virtual machine (VM) escape**. Ressourcenvirtualisierung gehört zu den wesentlichen Bausteinen eines Cloud-Systems. Wesentlich hierbei ist, dass sich Benutzer solcher Ressourcen in einer isolierten Umgebung bewegen, d.h. eine Wechselwirkung mit Ressourcen, die

[1] (Grobauer u. a., 2010) definiert eine weitere Kategorie, nämlich solche Schwachstellen, die in marktgängigen Cloud-Systemen zu finden sind. Da solche Schwachstellen jedoch notwendigerweise zu einer der drei anderen Kategorien gehören, wollen wir sie nicht einer weiteren Kategorie zuordnen.

anderen Benutzern zugeordnet sind, ist unmöglich (Reuben, 2007). Die Schwachstelle ist vorhanden, wenn es einem Benutzer möglich ist, diese isolierte Umgebung zu verlassen und auf die physikalischen Systeme zuzugreifen, von denen die Virtualisierung abstrahiert, bzw. auf virtualisierte Ressourcen anderer Benutzer.

- **Session Riding and Hijacking**. Web-basierte Anwendung benötigen i. d. R. ein Session-Konzept, das jedoch durch das unterliegende (zustandslose) Kommunikationsprotokoll (http) nicht unterstützt wird. Ein unerlaubtes Aneignen oder Benutzen des Session-Kontexts führt dazu, dass Angreifer die Identitäten autorisierter Benutzer übernehmen können (Schreiber, 2004).

- **Unsichere oder obsolete Kryptographie**. Kryptographische Verfahren zur Nachrichten- und Datenverschlüsselung und zur Zertifizierung gehören zu den grundlegenden Sicherheitsfunktionen. Kryptographische Schwachstellen ziehen vielfältige Risiken nach sich.

III.1.1.2 Schwachstellen, die durch Cloud-spezifische Innovationen verursacht werden

Welche Verfahren und Prozesse sind in virtualisierten Umgebungen nicht oder nur erschwert umsetzbar?

Virtualisierung gehört zu den wesentlichen Charakteristiken von Cloud-Systemen. Die unterstützte Abstraktion von physikalischen Ressourcen wie Rechnern, Betriebssystemen, Kommunikationsnetzen und Eingabegeräten führt jedoch dazu, dass erprobte Kontrollmaßnahmen in Cloud-Umgebungen nicht oder nur schwer anwendbar sind.

- **Unzureichende Kontrollen in virtualisierten Netzwerken**. Administrativer Zugang zu IaaS Netzwerkinfrastrukturen und ihre Anpassung ist für den Cloud-Benutzer notwendigerweise eingeschränkt; Standard-Kontrollmaßnahmen wie »Zoning«, die in selbstverwalteten Unternehmensnetzwerken zur Verfügung stehen, können nicht oder nur eingeschränkt verwendet werden. Netzwerkanalysetechniken (*port scanning*, etc.), die von Netzwerkadministratoren zur Fehlersuche und zur Optimierung verwendet werden, können in einer Cloud-Umgebung nicht von Angriffen unterschieden werden. Schließlich führt Netzwerkvirtualisierung zu verzerrten Lastsituationen im unterliegenden physikalischen Netzwerk, da keine eindeutige Zuordnung von virtualisierten Netzwerkknoten und -links zu physikalischen existiert. Etablierte Kontrolltechniken stehen in virtualisierten Netzwerken nur gar nicht oder nur eingeschränkt zur Verfügung, woraus Schwachstellen resultieren, die in nicht-virtualisierten Umgebungen vermeidbar sind.

- **Unzureichende Schlüsselmanagement-Prozeduren**. Kryptographische Absicherung ist ein essentieller Baustein eines vertrauenswürdigen Cloud-Systems. Schlüsselerzeugung beruht vielfach auf der Verwendung von Hardware-Mechanismen und -Charakteristiken. Virtualisierung stellt eine Abstraktion von tatsächlichen Hardwareressourcen dar, so dass gängige Methoden zur Erzeugung sicherer Schlüssel nicht zur Verfügung stehen.

- **Sicherheitsmetriken sind nicht an Cloud-basierte Infrastrukturen angepasst**. Zur Zeit existieren keine standardisierten Sicherheitsmetriken für Cloud-Infrastrukturen, die eine Bewertung des Sicherheitsstatus einer Cloud und die Verwendung diesbezüglicher Kontrollmaßnahmen durch den Kunden erlauben würden.

III.1.1.3 Schwachstellen, die aus den Eigenschaften von Cloud-Systemen herleitbar sind

Welche Sicherheitsrisiken ergeben sich aus Selbstbedienung, Netzwerkzugang, Elastizität, Ressourcen-Pooling und Messbarkeit der Dienstqualität?

Die Eigenschaften von Cloud-Systemen, auf die hier Bezug genommen wird, wurden in Abschnitt I.1.2 diskutiert.

- **Nichtautorisierter Zugang zu Managementschnittstellen**. Dienstleistungen in Clouds sind für Benutzer »*on-demand*« verfügbar, d. h. Benutzer benötigen zur Anforderung und Konfiguration solcher Dienste Zugang zu Managementschnittstellen, der natürlich durch Authentisierungs- und Autorisierungsmechanismen abgesichert werden muss. Mangelnde Zugangskontrolle erlaubt es einem Angreifer, unerlaubt Cloud-Ressourcen zu verwenden und Daten einzusehen bzw. zu verändern.
- **Netzwerkschwachstellen**. Cloud-Computing erlaubt einen netzwerkbasierten Zugang zu Ressourcen bzw. Diensten. In vielen Kontexten werden hierbei nichtvertrauenswürdige Netzwerke (Intranet, Internet) eingesetzt.
- **Datenwiedergewinnung**. Elastizität und Ressourcen-Pooling bedeutet, dass physikalische Speicherbereiche nacheinander verschiedenen Benutzern zugeordnet werden. Daraus resultiert die Möglichkeit, Daten anderer Benutzer zu rekonstruieren.
- **Manipulation von Abrechnungen**. Cloud-Dienste werden nutzungsorientiert in Rechnung gestellt — der Benutzer zahlt nur für die tatsächlich in Anspruch genommenen Ressourcen. Eine Schwachstelle besteht also in der möglichen Manipulation der Rechnungsdaten und Abrechnungsmechanismen.

III.1.2 Mehr Sicherheit in der Cloud

In den vorhergehenden Abschnitten haben wir aufgezeigt, dass Cloud-spezifische Sicherheitsrisiken zwar existieren, jedoch durchaus verstehbar und analysierbar sind. Frameworks und Prozesse zur Risikoanalyse und -bewertung existieren bzw. lassen sich aus allgemeinen Ansätzen zur IT-Sicherheit ableiten. In diesem Abschnitt befassen wir uns mit der Frage, inwieweit Sicherheitsanforderungen durch Clouds besser eingelöst werden können als durch herkömmliche Formen der IT-Dienstleistung. Die ENISA-Publikation (ENISA, 2009) zählt eine Reihe von Vorteilen auf, die Cloud-Computing bietet.

III.1.2.1 Skaleneffekte

Skaleneffekte können die Sicherheit in Cloud-Systemen erhöhen.

Sicherheitsrelevante Maßnahmen wie Monitoring und Ereignisanalyse, Patch- und Konfigurations-Management, Absicherung von Hardware und Betriebssystemen, Authentifizierung und Zugangskontrolle, Hard- und Softwareredundanz, Identitätsmanagement, einheitliche Richtlinien für Systemadministratoren usw. erweisen sich als überaus kostspielig, wenn sie in kleinen Datenzentren bzw. kundenspezifisch in kleinen Teilen der Infrastruktur eines Datenzentrums angewendet werden sollen. Eine vereinheitlichte Sichtweise auf Hardware, Plattform und Software, wie sie durch Cloud-spezifische Elemente wie Virtualisierung erreicht wird, ist wesentlich besser geeignet, um einheitliche und nachvollziehbare Sicherheitsarchitekturen und -komponenten kosteneffizient und effektiv zu implementieren.

Im Einzelnen bietet hochskaliertes Cloud-Computing die folgenden Vorteile:

- **Multiple Standorte**. Große Cloud-Anbieter verteilen ihre Infrastruktur auf eine Reihe von Standorten und verfügen über Mechanismen, Daten und Prozesse schnell zu verschieben und zu vervielfältigen. Die daraus resultierende Redundanzerhöhung vermindert das Risiko, dass ein Angriff an einem kritischen Punkt katastrophale Ausfälle zur Folge haben kann.

  Erhöhte Redundanz.

- **Verteilte Datenhaltung**. Clouds sind notwendigerweise verteilte Systeme, in denen Netzwerk- und Kommunikationsaspekte eine wesentliche Rolle spielen. Ausfälle und technische Probleme auf Netzwerkebene werden — da auf entsprechende Sicherheitsmechanismen bereits bei der Definition der Systemarchitektur gesteigerter Wert gelegt wurde — weniger heftige Auswirkungen haben.

  Nutzung der Mechanismen, die verteilte Infrastrukturen zur Verfügung stellen.

- **Zeitnahe Aufdeckung von Schwachstellen** kann besser erfolgen, da Informationen über erfolgte Angriffe innerhalb der Organisation des Cloud-Anbieters schneller verbreitet und Gegenmaßnahmen einfacher durchgesetzt werden können.

  Schnellere Verbreitung sicherheitsrelevanter Informationen.

- **Bedrohungsmanagement**. Große Cloud-Anbieter verfügen im Gegensatz zu kleineren Datenzentren über die finanziellen Mittel, ein Team von Sicherheitsexperten zu unterhalten und so ihre Sicherheitskonzepte auf dem neusten Stand zu halten.

  Sicherheitsexpertenteams und aktuelle Sicherheitskonzepte.

III.1.2.2 Sicherheit als Marktfaktor

Anbieter müssen die Sicherheit ihrer Dienstleistungen glaubhaft machen können, um marktfähig zu bleiben.

Sicherheitsbedenken zählen zur Zeit zu den wesentlichen Hindernissen für die Einführung von Cloud-Computing Technologien sowohl im öffentlichen wie auch im privatwirtschaftlichen Sektor. Cloud-Anbieter (bzw. Anbieter von Cloud-Technologien) können ihre Marktchancen erhöhen, wenn sie in der Lage sind, ein umfassendes und effektives Sicherheitskonzept vorzuweisen; Sicherheit wird damit zu einem Unterscheidungsmerkmal für Cloud-Angebote.

Cloud-Anbieter müssen in weitaus größerem Maßstab die Möglichkeit von Audits und die Verwendung von SLA-Validationsmechanismen bie-

ten, um ihr Angebot für ihre Kunden attraktiv zu halten. Dadurch werden jedoch auch Schwachstellen früher aufgezeigt und Gegenmaßnahmen können schneller und gezielter in Zusammenarbeit mit Cloud-Anwendern entwickelt werden.

Dieses Argument ist auch auf die Hersteller von Dienst-Software anwendbar, die explizit für die Anwendung in Clouds entwickelt wurde.

Eine sicherere Laufzeitumgebung kann nicht vorausgesetzt werden.

- **Robustere Dienste**. Da Hersteller bei der Entwicklung von Software zur Erbringung von Dienstleistungen nicht auf einen gesicherten Unternehmenskontext (d. h. einer als sicher eingestuften Zone, die von einem Sicherheitsperimeter umgeben ist) bauen können, wird Software, die explizit für Cloud-Umgebungen entwickelt wurde, schwachstellenärmer und robuster implementiert werden müssen, um überhaupt als valide Anwendungen in einem Cloud-Kontext in Frage zu kommen.

Interoperabilität und Sicherheitsanforderungen.

- **Standardisierte Schnittstellen für Sicherheitsmanagement**. Große Cloud-Anbieter können ihren Kunden sicherheitssensitive Dienste über standardisierte Schnittstellen zur Verfügung stellen, die die Interoperabilität zwischen Clouds auch bezüglich der Definition von Sicherheitsanforderungen erhöhen kann.

Elastizität als Sicherheitsmechanismus.

- **Sofortige und adaptive Ressourcenskalierung**. Die Detektion von aktuellen Angriffen erfordert Ressourcen (etwa für *monitoring*, *filtering*,*root cause analysis*), die in klassischen Systemen extra vorgehalten werden müssen.

  Darüber hinaus beruhen bestimmte Arten von Angriffen darauf, dem angegriffenen System systematisch Ressourcen zu entziehen (*Distributed Denial-of-Service*, DDoS). Mechanismen zur dynamischen, situationsgerechten Ressourcenskalierung sind also geeignet, um sowohl Ressourcen für die Angriffsabwehr zeitnah zur Verfügung zu stellen wie auch die Auswirkungen von verteilten Angriffen abzumildern. Voraussetzung hierfür ist aber die Verfügbarkeit von automatisierten Verteidigungs- und Ressourcenoptimierungsmechanismen.

Virtualisierung als Sicherheitsmechanismus.

- **Vereinfachte Audits und Spurensicherung**. Die Virtualisierung von Ressourcen ermöglicht es, forensische Analysen nicht am laufenden System durchzuführen, sondern an einem Schnappschuss des Systems, der zum Zeitpunkt der Feststellung eines Angriffs oder Sicherheitsproblems aufgenommen wird — Systeme müssen zur Analyse nicht außer Betrieb gestellt werden. Darüber hinaus sind Schnappschüsse beliebig kopierbar: Analysen können somit wesentlich schneller durchgeführt werden, ohne dass die Gefahr bestünde, während der Analysen Spuren zu verwischen.

Aktuelle Systemkonfigurationen durch Virtualisierung.

- **Verkürzte Reaktionszeiten**. Die Verwendung einer einheitlichen Plattform für das Management virtualisierter Systeme erlaubt offensichtlich die effiziente und beschleunigte Aufbringung von Updates und Patches sowie die Verwaltung einer einheitlichen und aktuellen Konfiguration.

- **Ressourcenkonzentration** wird im Sicherheitskonzept gewöhnlich als Nachteil angesehen, da auch Schwachstellen konzentriert wer-

den und Systeme leichter angreifbar sind. Demgegenüber steht allerdings die Möglichkeit der einfacheren Verwaltung von Sicherheitsperimetern bezogen auf die tatsächlichen Hardwareressourcen eines Cloud-Zentrums und die Durchsetzung einheitlicher Sicherheitsrichtlinien (z. B. Zugangskontrollen), Wartungsprozeduren und dem Management von Zwischenfällen.

III.1.2.3 Sicherheit als Dienst

Viele Sicherheitsmechanismen können selbst als Cloud-Dienstleistungen angeboten werden.

Schließlich können Sicherheitsmanagement-Funktionen und Prozesse selbst Gegenstand einer Auslagerung in die Cloud werden. Dies beinhaltet Anwendungen einerseits von Antivirenprogrammen und Spamfiltern, die durch Drittanbieter bereitgestellt werden, andererseits von Monitoringfunktionen, Zwischenfallmanagement, forensischen Analysen usw. Eine automatisierte Verwaltung verschiedener redundanter Instanzen eines Dienstes kann dessen Verfügbarkeit erhöhen.

III.1.3 Schlussfolgerung

Sicherheitsrisiken in der Cloud sind durch geeignete Prozesse grundsätzlich beherrschbar, für die allerdings noch Maßstäbe und Richtlinien erarbeitet werden müssen. Clouds können sogar höheren Sicherheitsstandards als herkömmliche Datenzentren genügen.

Wie jede neue Technologie beinhaltet auch Cloud-Computing neue Sicherheitsrisiken. Insbesondere ist Cloud-Computing als integrativer Rahmen einer Reihe von Basistechnologien (Netzwerk, Kryptographie, Virtualisierung) sowohl mit den Schwachstellen dieser Technologien behaftet, als auch durch solche, die sich aus den Kombinationen (etwas Kryptographie und Virtualisierung) dieser Technologien ergeben. Das besagt jedoch insbesondere, dass wir mit der Sicherheitsproblematik in Clouds kein vollständiges Neuland betreten. Allgemeine Ansätze für IT-Sicherheit sind gut in den Cloud-Bereich übertragbar. Schwachstellen sind klassifizierbar. Analysen werden durch eine Reihe gut dokumentierter Beispiele und Untersuchungen unterstützt.

Darüber hinaus besteht die begründete Annahme, dass Cloud-basierte Systeme tatsächlich höheren Sicherheitsstandards genügen können als klassische Datenzentren.[2] Um die Sicherheit einer Cloud bemessen zu können, sind jedoch eindeutige Maßstäbe und Richtlinien erforderlich, die noch zu erarbeiten und Verwaltungen und Behörden an die Hand zu geben sind. Diese dienen nicht nur dazu, Cloud-Angebote zielgerichtet zu beurteilen und zu unterscheiden, sondern insbesondere auch zur Schaffung einer Diskussionsgrundlage, die Sicherheitsanforderungen aus der Verwaltung auch für Cloud-Anbieter und Hersteller entsprechender Technologien verstehbar macht.

[2] Vgl. hierzu auch (Streitberger u. Ruppel, 2009).

KAPITEL III.2

Gefahrenlage Outsourcing

Zusammenfassung

Im Vergleich zu klassischen IT-Dienstleistern ergibt sich für private Clouds ein grundsätzlich positives Gesamtbild bzgl. Sicherheitsfragestellungen, die mit Outsourcing verbunden sind. Das einzige offensichtliche Problem ist das Fehlen von Interoperabilitätsstandards, so dass Insourcing oder ein Wechsel des Dienstleisters zu einem Problem werden kann. Ein ähnliches Bild ergibt sich für Community-Clouds, wobei es hier aufgrund des Umstandes, dass die an der »Community« beteiligten Rechenzentren unterschiedliche Verwaltungsdomänen mit u. U. unterschiedlichen Richtlinien definieren, zu weiteren Schwierigkeiten kommen kann. Insgesamt ist hier ein integriertes, kollaboratives Management von Cloud-Diensten erforderlich, für das zurzeit wenige oder keine Ansätze existieren.

Öffentliche Cloud-Anbieter hingegen kommen als Kooperationspartner für Behörden aus der Sicherheitsperspektive nur bedingt in Frage. Eines der Hauptprobleme ist der Umstand, dass der Kundenstamm eines öffentlichen Anbieters nicht a-priori bekannt ist: jeder, insbesondere auch Personen mit böswilligen Absichten, könnte — aufgrund der Cloud-Eigenschaft der »Selbstbedienung« — Zugang zu ggf. kritischen Systemteilen erlangen.

Einer der Grundschutz-Bausteine des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die für die vorliegende Studie von besonderem Interesse sind, ist der Baustein B 1.11 »Outsourcing«.[1] Der Baustein ist anzuwenden, wenn IT-Funktionen oder Prozesse an externe Dienstleister ausgelagert werden, wobei die Informationssicherheit des Auftrag-

[1] Zur Zielsetzung und Strukturierung der Grundschutzkataloge des BSI vgl. Anhang E.

gebers beeinflusst wird und Aufgaben im Bereich des Informationssicherheitsmanagements auf den Auftragnehmer übergehen. B 1.11 bezieht sich hierbei auf Maßnahmen, die der Auftraggeber durchzuführen hat, d. h. im vorliegenden Fall die Behörde oder das behördliche Rechenzentrum, das IT-Dienstleistungen (z. B. an einen Cloud-Anbieter) auslagern möchte.

III.2.1 Anwendbarkeit

Die Anwendbarkeit des Bausteins wird in (BSI, 2004) genauer beschrieben:

- Die Anwendung des Bausteins ist optional, wenn die Auslagerung eine unbedeutende Gefährdung für den Untersuchungsgegenstand darstellt. Eine nur unbedeutende Gefährdung liegt dann vor, wenn nur unwesentliche Komponenten des IT-Verbunds ausgelagert sind, und die ausgelagerten Komponenten einen höchstens mittleren Schutzbedarf haben und durch kumulierte Schadensereignisse der Schutzbedarf nicht erhöht wird.

- Die Anwendung des Bausteins ist zwingend, wenn die ausgelagerten Komponenten einer bedeutenden Gefährdungen ausgesetzt sind, d. h. wenn die ausgelagerten Komponenten einen hohen oder sogar sehr hohen Schutzbedarf haben oder wesentliche Teile des IT-Verbunds ausgelagert sind.

Vertragliche Regelungen machen die Anwendung des Bausteins »Outsourcing« nicht überflüssig.

- Die Anwendung des Bausteins ist zwingend, wenn ein begrenztes Schadensausmaß angenommen werden kann, d. h. der Dienstleister verpflichtet sich vertraglich auf die Einhaltung von IT-Grundschutz. Weiterhin kann im Einflussbereich des Outsourcing-Dienstleister nur finanzieller Schaden entstehen. Schließlich sind Verstöße gegen Gesetze und Beeinträchtigungen des informationellen Selbstbestimmungsrechts ausgeschlossen. Ein möglicher Schaden lässt sich so eindeutig beschreiben (Schadensdefinition, Höhe des Schadens, Schadensfolgen usw.), dass vertraglich Schadensersatz oder eine andere Wiedergutmachung vereinbart werden kann.

Selbst ein Grundschutz-Zertifikat macht die Anwendung des Bausteins nicht überflüssig.

- Selbst wenn der Dienstanbieter selbst über ein IT-Grundschutz-Zertifikat verfügt, das sich auf die ausgelagerten Komponenten bezieht, ist der Baustein zwingend anzuwenden.

Der Begriff »IT-Verbund« ist in der Cloud schwer zu definieren.

Es ist an dieser Stelle noch zu beachten, dass sich der Begriff IT-Verbund hier lediglich auf den Untersuchungsgegenstand des Bausteins bezieht, nicht auf die gesamte IT-Landschaft des Dienstanbieters oder Auftragnehmers. Gerade im Fall von Cloud-Computing ist jedoch die Grenze zwischen solchen Systemen, die Dienste für einen bestimmte Auftragnehmer bereitstellen, und solchen, die weitere Kunden bedienen, nur schwer zu ziehen.

	Gefährdung	Öff.	Priv.	Comm.
G 1.10	Ausfall eines Weitverkehrsnetzes	☀	☁	☁
G 2.1	Fehlende oder unzureichende Regelungen	—	—	—
G 2.7	Unerlaubte Ausübung von Rechten	—	—	—
G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	🌧	☀	☀
G 2.47	Ungesicherter Akten- und Datenträgertransport	☀	☀	☀
G 2.66	Unzureichendes Sicherheitsmanagement	☀	☀	☀
G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	🌧	☁	🌧
G 2.83	Fehlerhafte Outsourcing-Strategie	Vgl. § G 2.83 auf S. 76		
G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleister	🌧	☁	☁
G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens	🌧	🌧	🌧
G 2.86	Abhängigkeit von einem Outsourcing-Dienstleister	🌧	🌧	🌧
G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben	—	—	—
G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase	☀	☀	☀
G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister	🌧	☁	☁
G 2.93	Unzureichendes Notfallvorsorgekonzept beim Outsourcing	☀	☀	☀
G 3.1	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten	—	—	—
G 4.33	Schlechte oder fehlende Authentifizierung	☀	☀	☀
G 4.34	Ausfall eines Kryptomoduls	☀	☀	☀
G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleisters	☀	☀	☀
G 5.10	Missbrauch von Fernwartungszugängen	🌧	☁	☁
G 5.20	Missbrauch von Administratorrechten	🌧	☁	☁
G 5.42	Social Engineering	—	—	—
G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	🌧	☀	🌧
G 5.85	Integritätsverlust schützenswerter Informationen	🌧	☁	☁
G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister	—	—	—

Tabelle III.2.1
Einschätzung der im Baustein B 1.11 aufgeführten Gefährdungen im Vergleich zu herkömmlichen Dienstanbietern.

Legende:
- ☀ : *vermindert,*
- 🌧 : *erhöht,*
- ☁ : *neutral,*
- — : *nicht anwendbar.*

III.2.2 Gefährdungen

Der Baustein B 1.11 identifiziert Gefährdungen auf verschiedenen Ebenen, die im Folgenden genannt werden. Wenn eine bestimmte Gefährdung in Cloud-Umgebungen besonders zutage tritt bzw. abgemindert werden kann, werden wir dies besonders diskutieren. Tab. III.2.1 gibt unsere Einschätzung des Risikopotentials für private, Community- und öffentliche Clouds (verglichen mit den entsprechenden Potentialen für klassische Dienstanbieter) wider.

III.2.2.1 Höhere Gewalt

G 1.10: Ausfall eines Weitverkehrsnetzes

Öffentliche Clouds mit Internet-basiertem Zugang sind weitestgehend immun.

Diese Gefährdung kann in Verfügbarkeitsbeeinträchtigungen resultieren, wenn ungenügende Redundanz vorliegt. Diese Gefährdung wird dann besonders immanent, wenn zur Bereitstellung einer privaten Cloud ein dediziertes physikalisches Netzwerk verwendet wird. Eine öffentliche Cloud, die einen Internet-basierten Zugang offeriert, ist gegen diese Gefährdung weitestgehend immun. Diese Gefahrenquelle ist allerdings nicht Cloud-spezifisch, da viele klassische Rechenzentren ebenfalls dedizierte Netzwerke verwenden.

III.2.2.2 Organisatorische Mängel

G 2.1: Fehlende oder unzureichende Regelungen

Die Gefährdung bezieht sich auf organisatorische Regelungen im Betrieb des Rechenzentrums (z. B. Schlüsselregelungen) und ist nicht Cloud-spezifisch.

G 2.7: Unerlaubte Ausübung von Rechten

Auch diese Gefährdung bezieht sich auf organisatorische Regelungen und steht in keinem Zusammenhang zu den verwendeten Technologien.

G 2.26: Fehlendes oder unzureichendes Test- und Freigabeverfahren

Potentiell fehlerhafte Komponenten können in das Produktionssystem eingebracht werden. Im Cloud-Kontext ist diese Gefahrenquelle bei der Inanspruchnahme von (öffentlichen oder hybriden) Plattform- bzw. Infrastrukturdiensten insbesondere immanent, da die Umgebungen, in denen die Dienste des Auftraggebers laufen, für diesen nur indirekt zugreifbar sind, so dass die Herstellung einer realistischen Testumgebung problematisch ist. Bei hybriden Modellen kommt erschwerend hinzu, dass Dienstbindungen u. U. zur Laufzeit erfolgen.

Umgekehrt können innerhalb einer privaten Cloud sehr dedizierte Testumgebungen einfach (z. B. durch Virtualisierung) aufgesetzt werden, so dass routinemäßige und umfassende Testverfahren möglich sind. Unter der Voraussetzung, dass zwischen den an einer Community-Cloud beteiligten Rechenzentren ein adäquates Maß an Zusammenarbeit erreicht werden kann, können solche Tests auch rechenzentrenübergreifend vorgenommen werden; eine Vorgehensweise, die durch die Bereitstellung von Ressourcen auf Anforderung zusätzlich unterstützt wird.

In privaten bzw. Community-Clouds können Test- und Freigabeverfahren effektiver gestaltet werden.

G 2.47: Ungesicherter Akten- und Datenträgertransport

Der vergrößerte Maßstab von Cloud-Systemen macht die Einführung von Konzepten zur Umsetzung von Rechnerressourcen unumgänglich, so dass an dieser Stelle eher mit einer Abmilderung dieser Gefährdung zu rechnen ist. Auf die Ablage sensitiver Informationen auf mobile Datenträger oder gar Akten für deren Transport wird in Cloud-basierten Rechenzentren wohl ganz und gar verzichtet werden.

G 2.66: Unzureichendes Sicherheitsmanagement

Dieser Katalogeintrag nennt eine Reihe von Beispielen:

- Mangelnde persönlich Verantwortung/fehlendes Sicherheitsteam
- Mangelnde Unterstützung durch die Leitungsebene
- Unzureichende strategische und konzeptionelle Vorgaben
- Unzureichende oder fehlgeleitete Investitionen
- Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen
- Fehlende Aktualisierung im Sicherheitsprozess

Die Diskussion in Abschnitt III.1.2 deutet allerdings darauf hin, dass ein gut strukturiertes und stringent durchgesetztes Sicherheitsmanagement im Falle von Cloud-Infrastrukturen zu erwarten ist.

G 2.67: Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Im Kontext einer öffentlichen Cloud wird diese Gefährdung besonders immanent, da sich die Menge der Benutzer, die über einen erlaubten Zugriff auf Daten und Dienste in der Cloud verfügen, ständig ändert, so dass lediglich ein rudimentäres Rollensystem angewendet werden kann. Im Gegensatz dazu kann in privaten Clouds eine wohldefinierte Rechtestruktur verwendet werden. In föderierten Infrastrukturen, d. h. Community-Clouds setzt dies allerdings voraus, dass einheitliche oder aufeinander abbildbare Sicherheitsrichtlinien verwendet bzw. durch die verwendeten Technologien unterstützt werden.

Können Zugriffsrechte mit ausreichender Granularität definiert werden?

G 2.83: Fehlerhafte Outsourcing-Strategie

Dieser Eintrag im Gefahrenkatalog ist äußerst generisch formuliert; eine konkrete Bewertung von Cloud-Computing Infrastrukturen bzw. dieser Gefährdung ist nicht möglich.

G 2.84: Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

Die umfassende Definition von SLAs spielt eine wichtige Rolle.

Dieser Katalogeintrag gibt eine Reihe von Beispielen für Probleme an, die mit unzulänglichen Verträgen einhergehen können.

- Der Dienstleister kann die Dienstleistung nicht zu den kalkulierten Kosten erbringen, was zu Einsparungen in der IT, insbesondere im Bereich Sicherheit führen kann.
- Aufgaben, Leistungsparameter und Aufwände wurden ungenügend oder missverständlich beschrieben, so dass aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden.
- Der Auftraggeber kann seiner Auskunftspflicht nicht nachkommen, wenn der Dienstleister keinen Zutritt zu seinen Räumlichkeiten oder keinen Zugang zu den notwendigen Unterlagen gewährt.
- Der Auftraggeber kann neuen Anforderungen (z. B. fachlicher Art, gesetzliche Vorschriften, Verfügbarkeit, technische Entwicklung) nicht nachkommen, wenn Änderungsmanagement und Systemanpassungen nicht ausreichend vertraglich geregelt wurden.
- Bei Outsourcing-Vorhaben ist die Behörden- bzw. Unternehmensleitung des Auftraggebers unter Umständen voll verantwortlich für die ausgelagerten Geschäftsbereiche, kann dieser Verantwortung aber wegen fehlender Kontrollmöglichkeiten nicht gerecht werden.
- Ausgelagerte Daten oder Systeme werden ungenügend geschützt, wenn ihr Schutzbedarf dem Outsourcing-Dienstleister unbekannt ist.
- Die Dienstleistungsqualität ist schlecht, und es gibt keine Eingriffsmöglichkeiten, weil keine Sanktionen vertraglich festgelegt wurden.
- Der Dienstleister zieht qualifiziertes Personal ab oder Vertreter des Stammpersonals sind nicht ausreichend vorbereitet, was zu Sicherheitsproblemen führen kann.

Fragestellungen des Auftraggebers.

Diese Bespiele decken eine Reihe von Fragestellungen ab, mit denen sich eine Behörde konfrontiert sieht, die die Auslagerung von Diensten an einen öffentlichen Cloud-Anbieter plant.

- Inwieweit sind interne Sicherheitsmaßnahmen des Anbieters für den Auftraggeber nachvollziehbar in einer Cloud, in dem Dienste und Daten u. U. auf mehrere geographisch entfernte Rechenzentren verteilt sind?

- Welche Kontrollmöglichkeiten existieren für den Auftraggeber?
- Wie werden Dienstleistungen verwaltet?
- Welches fachspezifische Know-How kann beim Dienstleister vorausgesetzt werden?

Zusammenfassend muss die Frage, wie Dienstleistungsverträge in einer öffentlichen Cloud formuliert werden können, als eines der wesentlichen Probleme für dieses Betriebsmodell angesehen werden.

Im Gegensatz dazu bestehen bzgl. der Vertragslage für private Clouds bzw. Community-Clouds weitgehend dieselben Probleme wie für herkömmliche Dienstleister. Im Falle einer Community-Cloud ist noch auf das Problem hinzuweisen, dass Vereinbarungen, die eine Behörde mit einem der an der Community-Cloud beteiligeten Dienstleistungszentren trifft, an die anderen beteiligten Zentren »durchgereicht« werden müssen.

G 2.85: Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens

Neben der Beendigung des Vertrags wegen einer anstehenden Neuausschreibung bzw. Streitigkeiten wegen unzureichender Dienstqualität oder Sicherheitsmängel ist hier insbesondere auch der Fall zu betrachten, dass der Dienstleister von einem ausländischen Unternehmen aufgekauft wird, so dass die gesetzlichen Regelungen zum Schutz personenbezogener Daten unterlaufen werden können.

Können Daten und Prozesse sicher und zeitgerecht migriert werden?

Das wesentliche Problem, nämlich die zeitgerechte und sichere Migration von Daten und Prozessen zu einem neuen Anbieter, kann nicht pauschal diskutiert werden. Besteht etwa der besagte Dienst aus einer ERM-Unterstützung, hängt die Migrationsfähigkeit von der Verfügbarkeit kompatibler Systeme beim Neuanbieter ab (und erfordert im einfachsten Fall das Kopieren von Konfigurationsinformationen bzw. das Erstellen eines Datenbankabbilds), nicht jedoch von der verwendeten Cloud-Infrastruktur selbst. Umgekehrt führt die Verwendung proprietärer oder veralteter Formate für virtuelle Maschinen beim Altanbieter dazu, dass umfangreiche Konvertierungs- bzw. Neuinstallationen beim Neuanbieter notwendig sind.

Standards zur Interoperabilität und Portabilität sind z. Z. noch nicht verfügbar.

Allerdings ergibt sich im Cloud-Kontext insbesondere das Problem, dass die Cloud-Infrastruktur des Anbieters eine weitere technologische — und z. Z. proprietäre — Schicht hinzufügt, die zu weiteren Inkompatibilitäten und damit verbundenen Migrationsschwierigkeiten führen kann. In jüngster Zeit sind jedoch eine Reihe von Bemühungen eingeleitet worden, die Portabilität und Interoperabilität von Cloud-Diensten und -Infrastrukturen zu erhöhen und entsprechende Standards zu entwickeln (vgl. hierzu auch Abschnitt III.4.6).

G 2.86: Abhängigkeit von einem Outsourcing-Dienstleister

Neben dem Verlust von Know-How, Kontrollverlust, Veränderung der Rahmenbedingungen (z. B. Eigentümerwechsel beim Outsourcing-

Dienstleister, Änderung der Gesetzeslage, Zweifel an der Zuverlässigkeit des Outsourcing-Dienstleisters) und Kosten, die bei einem Wechsel des Anbieters auftreten, ergibt sich im Cloud-Kontext noch die im vorherigen Abschnitt beschriebene technologische Abhängigkeit von der Cloud-Infrastruktur.

G 2.88: Störung des Betriebsklimas durch ein Outsourcing-Vorhaben

Diese Gefährdung ist offenbar nicht Cloud-spezifisch.

G 2.89: Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase

Unzureichende Planung, Terminprobleme und strukturelle Veränderungen sowohl beim Auftraggeber wie auch beim Dienstleister können dazu führen, dass Sicherheitsstandards nicht eingehalten werden. Im Falle einer öffentlichen Cloud ist allerdings davon auszugehen, dass zumindest auf Anbieterseite ein strukturiertes Konzept für die Einführungsphase besteht.

G 2.90: Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister

Ein Web-basierter Zugang kann Schwachstellen aufweisen.

Für private Clouds bzw. Community-Clouds kann hier ein Gefahrenniveau angenommen werden, das mit dem eines klassischer Dienstanbieters vergleichbar ist. Für öffentliche Clouds, für die ein grundsätzlich auch für Dritte offener Internet-basierter Zugang besteht, muss eine erhöhte Gefährdung angenommen werden. Allerdings kann hier umgekehrt auch so argumentiert werden, dass ein öffentlicher Cloud-Anbieter aufgrund seines Geschäftsmodells ein erhöhtes Interesse an gesicherten Anbindungen hat.

G 2.93: Unzureichendes Notfallvorsorgekonzept beim Outsourcing

Notfallvorsorge bezieht sich auf die Integration von

- IT-Systemen beim Auftraggeber
- IT-Systemen beim Outsourcing-Dienstleister
- Schnittstellen (z. B. Netzverbindung, Router, Telekommunikations-Provider) zwischen Auftraggeber und Dienstleister

Ressourcen-Pooling, Netzwerkzugang und Elastizität erleichtern die Umsetzung eines Notfallkonzepts.

Allerdings ist zu erwarten, dass Cloud-Systeme, in denen IT-Systeme virtualisiert betrieben werden und die damit leichter zu überwachen und redundant zu halten sind und die zudem für einen netzwerkbasierten Zugang entworfen wurden, die Etablierung eines Notfallkonzepts erleichtern. Insbesondere ist hierbei auf die unmittelbare bedarfsgerechte Verfügbarkeit von Ressourcen und die damit verbundene gesteigerte Redundanz hinzuweisen; dieses Argument gilt sowohl für öffentliche wie auch private bzw. Community-Clouds.

III.2.2.3 Menschliche Fehlhandlungen

G 3.1: Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten

Diese Gefährdung ist nicht Cloud-spezifisch; Fehlverhalten durch Unachtsamkeit bzw. Unwissen stellt ein allgemeines, von der Verwendung konkreter Technologien und Infrastrukturen unabhängiges Risiko dar.

III.2.2.4 Technisches Versagen

G 4.33: Schlechte oder fehlende Authentifizierung

Cloud-Infrastrukturen benötigen ein integriertes, modernes Sicherheitskonzept. Deshalb ist anzunehmen, dass eine Gefährdung für Clouds aufgrund unzureichender Authentifizierungsmechanismen zumindest ebenso hoch, jedoch nicht höher einzuschätzen ist als im Falle herkömmlicher Dienstanbieter.

G 4.34: Ausfall eines Kryptomoduls

Der Eintrag G 4.34 nennt exemplarisch die folgenden Ursachen für den Ausfall eines Kryptomoduls:

- technischer Defekt, der die Funktionsfähigkeit beeinträchtigt,
- Stromausfall, in dessen Folge die flüchtig gespeicherten kryptographischen Schlüssel gelöscht werden, so dass das Kryptomodul infolgedessen nicht mehr ordnungsgemäß verschlüsseln kann,
- unabsichtliche oder absichtliche Zerstörung durch mechanische Einwirkung, Fehlbedienung oder Ähnliches.

Zumindest bzgl. der letzten beiden Punkte ist für Cloud-Infrastrukturen eine (durch Virtualisierung bzw. Ressourcen-Pooling) höhere Redundanz zu erwarten, so dass ein geringeres Gefährdungsniveau angenommen werden kann.

G 4.48: Ausfall der Systeme eines Outsourcing-Dienstleisters

Zumindest teilweise auftretende Systemausfälle können in redundant ausgelegten Ressourcen-Pools mit dynamischen Allokationsmechanismen leichter ausgeglichen werden als in herkömmlichen Infrastrukturen.

Fehlertoleranz durch Redundanz ist in der Cloud leichter realisierbar.

G 5: Vorsätzliche Handlungen

G 5.10: Missbrauch von Fernwartungszugängen

Netzwerkzugang und Selbstbedienung können Administrationsschnittstellen angreifbar machen.

Im Fall der öffentlichen Cloud muss hier eine erhöhte Gefährdung angenommen werden, da Administrationsaufgaben (im Falle von IaaS und PaaS, und falls Kunden Konfigurationsmöglichkeiten eingeräumt werden, auch SaaS) auf den Dienstnehmer übergehen und »remote« wahrgenommen werden, so dass grundsätzlich ein weiterer Fernwartungszugang zu berücksichtigen ist. Für private Clouds und Community-Clouds besteht bezüglich dieser Gefährdung kein Unterschied zu herkömmlichen Systemen.

G 5.20: Missbrauch von Administratorrechten

Der Eintrag G 5.20 bezieht sich im Wesentlichen auf Gefährdungen, die aus unrechtmäßig erlangten Administratorrechten auf Systemen der Infrastruktur resultieren, und ist somit als »neutral« einzustufen. Allerdings existieren für Clouds u. U. Administrationszugänge bzgl. der in Anspruch genommenen Dienste (vgl. die Diskussion zu Eintrag G 5.10), für die im Falle einer öffentlichen Cloud ein gesondertes gesteigertes Risiko angenommen werden muss.

G 5.42: Social Engineering

Diese Gefährdung ist nicht Cloud-spezifisch; inwieweit für Clouds eine besondere Gefährdung durch Social Engineering — »Aushorchen« oder Manipulation geeigneter Personen — besteht, ist Gegenstand soziologischer und psychologischer Untersuchungen, die in dieser Studie nicht geleistet werden können.

G 5.71: Vertraulichkeitsverlust schützenswerter Informationen

Cloud-Computing involviert potentielle Gefährdungen, die im Grundschutzbaustein »Outsourcing« noch nicht berücksichtigt wurden.

Für verschiedene im Eintrag G 5.71 diskutierte Beispiele (Zugriff auf Festplatten, mobilen Speichermedien, Akten und Ausdrucke) ist ein deutlich geringeres Gefährdungsrisiko festzustellen als bei herkömmlichen Infrastrukturen. Allerdings muss davon ausgegangen werden, dass Risikopotentiale, die durch Internet-basierten Zugang, Selbstbedienung und dynamische Ressourcenzuweisung (und die damit verbundene Kommunikation verteilter Komponenten) bedingt werden, zumindest im Fall einer öffentlichen Cloud grundsätzlich überwiegen. Für private Clouds, in denen die Definition und Durchsetzung geeigneter Zugriffsrechte angenommen werden kann, besteht hier ein grundsätzlich geringeres Gefahrenpotential. Für Community-Clouds entsteht wiederum das Problem, dass solche Zugriffsrechte für föderierte Strukturen definiert werden müssen.

	Phase	Maßnahme
1	Strategische Planung des Outsourcing-Vorhabens	M 2.250
2	Definition der wesentlichen Sicherheitsanforderungen	M 2.251
3	Auswahl des Outsourcing-Dienstleisters	M 2.252
4	Vertragsgestaltung	M 2.253
5	Erstellung eines IT-Sicherheitskonzepts für den ausgelagerten IT-Verbund	M 2.254, M 2.83
6	Migrationsphase	M 2.255
7	Planung und Sicherstellung des laufenden Betriebs	M 2.256

Tabelle III.2.2
Phasen eines Outsourcing-Vorhabens nach (BSI, 2010a, Bausteine→Übergreifende Aspekte→B 1.11 Outsourcing).

G 5.85: Integritätsverlust schützenswerter Informationen

Integritätsverlust kann unter anderem durch unzulässigen Systemzugriff[2] kommen. Der Eintrag nennt unter anderem die folgenden Beispiele:

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

Wegen des Vorhandenseins zusätzlicher Administrationszugänge ist zumindest für öffentliche Clouds ein gesteigertes Gefährdungsniveau festzustellen.

G 5.107: Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

Die Gefährdung ist unabhängig von der Inanspruchnahme von Cloud-Dienstleistungen.

III.2.3 Maßnahmen

Betrachten wir nun die Maßnahmen, die vom BSI für ein Outsourcing-Vorhaben vorgeschlagen werden. Ein solches Verfahren wird in Phasen untergliedert, in denen generelle Maßnahmen primär berücksichtigt werden müssen (vgl. Tab. III.2.2). Daneben werden eine Reihe von spezifi-

[2] Vgl. § G 5.10 bzw. § G 5.20.

scheren Maßnahmen betrachtet. Tab. III.2.3 fasst unsere vorläufige Einschätzung der Durchsetzbarkeit des Maßnahmenkatalogs für private und öffentliche Clouds im Vergleich zur Durchsetzbarkeit analoger Maßnahmen bei herkömmlichen Anbietern zusammen.

III.2.3.1 Planung und Konzeption

M 2.40 (A): Rechtzeitige Beteiligung des Personal-/Betriebsrates

Welche Daten über die Mitarbeiter einer Behörde gelangen in die Cloud?

Die Verhaltens- und Leistungsüberwachung von Mitarbeitern bedarf der Mitbestimmung des Personal- bzw. Betriebsrates einer Institution (hier die auslagernde Behörde). Falls — z. B. bei einer öffentlichen Cloud — nicht von vornherein klar ist, inwieweit solche Daten erhoben bzw. gespeichert werden, kann sich dies erschwerend auf eine Einigung mit dem Personal- bzw. Betriebsrat auswirken.

M 2.42 (B): Festlegung der möglichen Kommunikationspartner

Die Maßnahme ist unabhängig von der Inanspruchnahme von Cloud-Dienstleistungen.

M 2.221 (A): Änderungsmanagement

Effektive Mechanismen zum Dienstmanagement in der Cloud stehen der Berücksichtigung kundenspezifischer Anforderungen an die öffentliche Cloud gegenüber.

Der Eintrag M 2.221 nennt die folgenden Beispiele für solche Änderungen:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzwerkverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware, usw.),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme Benutzergruppen),
- räumliche Änderungen, z. B. nach einem Umzug.

Inwieweit ein Cloud-Anbieter Prozesse für ein solches Änderungsmanagement unterstützt ist im Einzelfall zu klären. Für öffentliche Cloud-Anbieter, die wesentlich generischere Dienstleistungen anbieten, ist die Durchführung eines kundenspezifischen Änderungsmanagements erwartungsgemäß ein großes Problem.

Andererseits vereinfachen Cloud-Eigenschaften und -Technologien wie Ressourcen-Pooling, Monitoring bzw. Virtualisierung und zentralisierte System- und Dienstmanagementstrukturen das Aufbringen eines dedizierten Änderungsmanagements. Diese Vorteile kommen insbesondere bei privaten und Community-Clouds zum Tragen.

		Maßnahme	Öff.	Priv.	Comm.
M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates			
M 2.42	(B)	Festlegung der möglichen Kommunikationspartner	—	—	—
M 2.221	(A)	Änderungsmanagement			
M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal	—	—	—
M 2.250	(A)	Festlegung einer Outsourcing-Strategie		Vgl. § M 2.250, S. 84	
M 2.251	(A)	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben		Vgl. § M 2.251, S. 84	
M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben	Vgl. § M 2.254, S. 84		
M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters			
M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister			
M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben			
M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern			
M 5.87	(C)	Vereinbarung über die Anbindung an Netze Dritter			
M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten	—	—	—
M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb			
M 2.307	(A)	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses	Vgl. § M 2.307, S. 89		
M 6.83	(A)	Notfallvorsorge beim Outsourcing			
M 6.109	(A)	Notfallplan für den Ausfall eines VPNs			

Tabelle III.2.3
Einschätzung der Durchsetzbarkeit der im Baustein B 1.11 aufgeführten Maßnahmen im Vergleich zu herkömmlichen Dienstanbietern.

Legende:
- : *leichter,*
- : *schwieriger,*
- : *neutral,*
- — : *nicht anwendbar.*

M 2.226 (A): Regelungen für den Einsatz von Fremdpersonal

Nicht Cloud-spezifisch; die Maßnahme bezieht sich auf den Einsatz von Fremdpersonal beim Auftraggeber.

M 2.250 (A) Festlegung einer Outsourcing-Strategie

Standards zur Bewertung von Cloud-Anbietern werden benötigt.

Die Festlegung einer geeigneten Outsourcing-Strategie kann — abhängig von den Funktionen und Diensten, die ausgelagert werden sollten — eine sehr komplexe Aufgabe sein.[3] Allerdings steht die Behörde, die eine Auslagerung in Erwägung zieht, hier vor denselben Fragestellungen nach Verfügbarkeit, Sicherheit, Complience usw., unabhängig davon, ob ein Cloud- oder ein klassischer Anbieter ins Auge gefasst wird. Im Falle eines öffentlichen Cloud-Anbieters können diese Fragen nur schwer beantwortet werden, da eine detaillierte Analyse der Systeme und Organisation des Anbieters für diesen i. d. R. problematisch ist. Für private und Community-Clouds ergibt sich das Problem, dass zusätzliche Technologien zur Unterstützung der Cloud-Funktionen entsprechend ihrer Vorteile und Risiken zu untersuchen sind. Bisher fehlen dedizierte Standards und Richtlinien für eine solche Abwägung (die allerdings etwa vom BSI bereits vorbereitet werden)[4].

M 2.251 (A) Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

Sicherheitsrelevante Aspekte sind durchaus identifizierbar, allerdings fehlen entsprechende Standards.

Hier sind u. a. die in Kapitel III.1 diskutierte Klassifizierung in Verbindung mit Prozessen wie in Anhang D dargestellt zu beachten. Insgesamt lässt sich feststellen, dass zumindest im Fall einer privaten Cloud die Analyse von sicherheitsrelevanten Aspekten auf der Basis dieser Konzepte durchführbar ist. Eine vereinheitlichte Infrastruktur bzw. einheitliche und automatisierte System- und Dienstmanagementprozesse können eine solche Analyse zumindest potentiell vereinfachen; allerdings gilt hier wie auch bei der Diskussion des Eintrags M 2.250, dass aufgrund der bisher fehlenden Standards kein endgültiges Urteil getroffen werden kann.

Für öffentliche Clouds kommt erschwerend hinzu, dass Informationen über die verwendeten Systeme und Prozesse bzw. deren Integration beim Cloud-Anbieter u. U. nicht ohne weiteres verfügbar sind.

M 2.254 (A) Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

Die Maßnahme M 2.245 nennt u. a. die folgenden Elemente, die bei der Erstellung eines solchen Sicherheitskonzepts zu berücksichtigen sind; wir fügen jeweils Verweise auf die Teile der Studie hinzu, in denen diese Elemente diskutiert werden.

[3] Vgl. (Groll u. Brodnik, 2009)

[4] Vgl. (BSI, 2010b) bzw. Kapitel III.4

- Organisation:
  - Umgang mit Daten und schützenswerten Betriebsmitteln (vgl. Kapitel III.3)
- Hard-/Software (vgl. Kapitel III.4; viele der genannten Punkte sind im Zusammenhang mit Cloud-Computing von besonderem Interesse):
  - Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
  - Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
  - Einsatz von Datei-Integrität-Prüfungssystemen, um Veränderungen, z. B. nach erfolgreichen Angriffen, zu erkennen
  - Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
  - Einsatz kaskadierter Firewallsysteme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters; für öffentliche Clouds sind solche Firewalls allerdings nur bedingt einsetzbar.
  - sorgfältige Vergabe von Benutzer-Kennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters
- Kommunikation (vgl. ebenfalls Kapitel III.4):
  - Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Auftraggeber, um sensitive Daten zu schützen
  - Authentisierungsmechanismen
  - Detailregelungen für weitere Netzanbindungen (vgl. § M 5.87)
  - Detailregelungen für den Datenaustausch (vgl. § M 5.88)
- Kontrollen und Qualitätssicherung:
  - Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messungen von Sicherheit, Dienstqualität, Abläufen und organisatorischen Regelungen
- Notfallvorsorge (vgl. § M 6.83)

III.2.3.2 Beschaffung

M 2.252 (A) Wahl eines geeigneten Outsourcing-Dienstleisters

Zur Auswahl eines Outsourcing-Anbieters nennt der Eintrag M 2.252 die folgenden Elemente:

- Definition der Aufgaben und Aufgabenteilung

Messbare Dienstqualität und Protokollierungsmechanismen sprechen für die Wahl eines Cloud-Anbieters.

- Festlegung des geforderten Qualitätsniveaus sowie Sicherheitsanforderungen, insbesondere auch Kriterien zur Messung von Servicequalität und Sicherheit.

Für öffentliche Clouds, insbesondere wenn Verträge nicht unter Zugrundelegung von SLAs, sondern lediglich von AGBen geschlossen werden können, sind diese Festlegungen nur schwer zu treffen. Insbesondere Behörden, die weitreichende Garantien bzgl. Sicherheit, Datenschutz und Verfügbarkeit von Dienstleistungen benötigen (z. B. Grundschutz-Zertifizierung), können öffentliche Cloud-Anbieter nur schwer als potentielle Dienstleister in Betracht ziehen. Für private und Community-Cloud-Anbieter ergibt sich hier jedoch derselbe Schwierigkeitsgrad wie für klassische Anbieter, wobei hier die Verfügbarkeit weitreichender Monitoring- und Protokollierungsmechanismen, die als Cloud-Eigenschaft definiert wurde, im Wesentlichen für die Auswahl eines Cloud-Anbieters spricht.

III.2.3.3 Umsetzung

M 2.253 (A) Vertragsgestaltung mit dem Outsourcing-Dienstleister

Dieser Eintrag nimmt wiederum starken Bezug auf Maßnahmen, die im Detail durch andere Einträge im Katalog abgedeckt werden. Wir gehen hier nur auf die Punkte ein, die in dieser Studie an anderer Stelle nicht oder nur am Rande betrachtet werden:

Weiterführende Szenarien für Cloud-Nutzung (z. B. »Cloud bursts«) involvieren sehr komplexe vertragliche Regelungen.

- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, externe Partner grundsätzlich auszuschließen, sondern sinnvolle Regelungen festzulegen. Für private und Community-Cloud-Anbieter kann dies in derselben Art wie für klassische Anbieter geschehen. Für öffentliche Clouds hingegen, insbesondere wenn dynamische Ressourcenallokationsmodelle (»*Cloud bursts*«) betrachtet werden, bei denen Ressourcen von Drittanbietern bei Bedarf kurzfristig hinzugeschaltet werden, können derartige vertragliche Regelungen extrem komplex werden.

Probleme bei der Berücksichtigung von Eigentumsrechte und Lizenzierung.

- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist auch zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt. Wiederum ergibt sich für private und Community-Clouds dieselbe Situation wie für klassische Dienstleistungzentren, während eine Vertragsgestaltung mit öffentlichen Cloud-Anbietern problematisch werden kann. Insbesondere ist ein Vertrag, der auf AGBen beruht, an dieser Stelle ungeeignet.

Mandantenfähigkeit ist eine konstitutive Cloud-Eigenschaft.

- Mandantenfähigkeit wird im Eintrag M 2.253 explizit aufgeführt. Cloud-Systeme sind jedoch aufgrund ihrer vorausgesetzten Eigenschaften mandantenfähig.

Zusammenfassend ergibt sich für private und Community-Clouds an dieser Stelle eine eher positive Einschätzung der Durchsetzbarkeit die-

ser Maßnahme. Für öffentliche Anbieter muss wiederum ein erhöhter Schwierigkeitsgrad angenommen werden.

M 2.255 (A) Sichere Migration bei Outsourcing-Vorhaben

Migration in die Cloud erfordert eine enge Zusammenarbeit zwischen Dienstleister und Auftraggeber, die dem Selbstbedienungs-Prinzip (zumindest in öffentlichen Clouds) widerspricht.

Im Eintrag M 2.255 wird die Bildung eines gemischten Teams aus Mitarbeitern des Auftraggebers und des Dienstleisters zur Durchführung und Überwachung der Migration vorgeschlagen, das u. U. durch externe Experten ergänzt werden kann. Die Aufgaben dieses Teams sind

- Erstellung der IT-Sicherheitskonzeption
- Festlegung von Verantwortlichkeiten und Hierarchien für die Migration
- Planung und Durchführung der erforderlichen Tests
- Erstellung von Abnahmeprozeduren
- Auswahl des geeigneten Personals, Durchführung von Schulungen, etc.
- Dokumentation der relevanten Abläufe, Applikationen und IT-Systeme des Auftraggebers, sofern sie von der Migration betroffen sind
- Sicherstellung des störungsfreien Betriebs
- Anpassung von SLAs oder IT-Sicherheitsmaßnahmen, falls notwendig
- Erstellung eines Notfallvorsorgekonzepts
- Aktualisierung und Konkretisierung des Sicherheitskonzepts auch nach Abschluß der Migration.

Die aufgeführten Aufgaben zeigen, dass eine sehr enge Zusammenarbeit zwischen Dienstleister und Auftraggeber notwendig ist, die auch personelle bzw. organisatorische Aspekte auf Seiten des Dienstanbieters umfasst. Eine pauschale Selbstbedienung ohne dedizierte Verhandlungen mit dem Cloud-Anbieter steht im Widerspruch zur Umsetzung dieser Maßnahme. Für öffentliche Cloud-Anbieter ist eine solche (mit dem Betriebsmodell »öffentliche Cloud« nicht zu vereinbarende) Einflussnahme kaum akzeptabel. Für private und Community-Clouds hingegen besteht offenbar dieselbe Situation wie für klassische Anbieter.

M 3.33 (Z) Sicherheitsüberprüfung von Mitarbeitern

Im Fall einer öffentlichen Cloud wird die Durchsetzbarkeit dieser Maßnahme durch den Umstand erschwert, dass Personal nicht eindeutig einem Kunden oder einem bestimmten Kundenkreis (hier: Kunden aus dem öffentlichen Sektor) zugeordnet werden kann. Für private bzw. Community-Clouds ergibt sich ein Schwierigkeitsgrad, der dem eines klassischen Anbieters entspricht.

M 5.87 (C) Vereinbarung über die Anbindung an Netze Dritter

»Cloud-bursts« erschweren die Definition von »Data Connection Agreements«.

Falls ein öffentlicher Cloud-Anbieter im Fall von Überlastsituationen auf die Ressourcen anderer Anbieter zurückgreift (»*Cloud burst*«), können sensitive Daten außerhalb der Verträge zwischen der auslagernden Institution und dem originalen Anbieter verarbeitet oder gespeichert werden, ohne dass dies für den Auftraggeber unmittelbar ersichtlich ist, wodurch sich ein kaum überschaubares Sicherheitsrisiko ergeben kann. In privaten und Community-Clouds kann eine solche Anbindung durch »*Data Connection Agreements*« ebenso geregelt werden, wie dies für herkömmliche Anbieter möglich ist.

M 5.88 (C) Vereinbarung über Datenaustausch mit Dritten

Nicht Cloud-spezifisch: die Maßnahme bezieht sich auf die Kommunikation der auslagernden Einrichtung mit Dritten via Email oder physikalischen Datenträgern.

III.2.3.4 Betrieb

M 2.256 (A) Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb

Eine enge Zusammenarbeit zwischen Anbieter und Auftraggeber ist gefordert, die dem Selbstbedienungs-Prinzip (zumindest in öffentlichen Clouds) widerspricht.

Ähnlich zu denen im Eintrag M 2.255 aufgeführten Maßnahmen ist hier eine enge Kooperation zwischen Dienstleister und Auftraggeber erforderlich, die die folgenden Punkte adressiert:

- Aktualisierung von Dokumentationen und Richtlinien.
- Aktualität der Sicherheitskonzepte. Insbesondere muss der Outsourcing-Dienstleister den Auftraggeber über wichtige Änderungen in seinem Einflussbereich informieren.
- Kontrollen umfassen
  - Durchführung der vereinbarten Audits
  - Umsetzungsstand der vereinbarten IT-Sicherheitsmaßnahmen
  - Wartungszustand von Systemen und Anwendungen
  - Rechtezuweisung durch den Dienstleister (Missbrauch von Rechten)
  - Einsatz von Mitarbeitern, die dem Auftraggeber nicht gemeldet wurden, z. B. bei Vertretungen
  - Performance, Verfügbarkeit, Qualitätsniveau
  - Datensicherung
- Kommunikation: Regelmäßige Abstimmungsrunden zu operativen Aspekten sind abzuhalten, die u. a. organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, Probleme und Änderungsmanagement umfassen.

- Tests und Übungen, z. B.
  - Reaktion auf Systemausfälle (Teilausfall, Totalausfall)
  - Wiedereinspielen von Datensicherungen
  - Beherrschung von Sicherheitsvorfällen

Wiederum ergibt sich hier eine für einen öffentlichen Cloud-Anbieter problematische Einmischung in seine unternehmensinternen Vorgänge. Keinesfalls ist die Maßnahme durch vorkonfigurierte Dienstmuster (*templates*) umsetzbar, wie sie nach dem Selbstbedienungs-Prinzip in öffentlichen Clouds angeboten werden. Für private und Community-Cloud-Anbieter ist die Situation mit der eines klassischen Anbieters vergleichbar.

III.2.3.5 Aussonderung

M 2.307 (A) Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses

Erforderliche Standards zur Interoperabilität und Portabilität müssen erst erarbeitet werden.

Das Problem, dass Datenrückgewinnung aus Cloud-Infrastrukturen verglichen mit »klassichen« Infrastrukturen aufgrund zusätzlicher proprietärer Technologien u. U. schwierig ist, wurde bereits diskutiert. Insbesondere sind Standardisierungsgremien an dieser Stelle gefordert, um die erforderlichen Standards und Richtlinien zu interoperablen und portierbaren Daten und Prozessen zu erarbeiten, die, sobald sie verfügbar und umgesetzt sind, durchaus Erleichterungen im Insourcing bzw. in der Migration in eine neue Cloud bieten können.

Der Vollständigkeit halber seien hier nocheinmal die wesentlichen Punkte genannt, die bei der Beendigung eines Dienstleistungsverhältnisses zu beachten sind:

- Eigentumsrechte an Hard- und Software müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte oder Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln. Eine Standardisierung solcher Hilfsmittel, die zur Entstehung entsprechender Produkte bzw. Open-Source-Lösungen führt, erleichtert die Durchsetzung dieser Maßnahme.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe müssen ausreichend dokumentiert sein. Für Cloud-Infrastrukturen, in denen solche Systeme und Abläufe in hohem Maße integriert und in vielen Fällen automatisiert sind, ist eine solche Dokumentation einfacher zu erstellen als in Infrastrukturen, die manuell oder mit Hilfe von Einzellösungen verwaltet werden.
- Alle notwendigen Daten müssen vom Dienstleister an den Auftraggeber übertragen bzw. übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden.

III.2.3.6 Notfallvorsorge

M 6.83 (A) Notfallvorsorge beim Outsourcing

Obwohl für öffentliche Clouds insgesamt eine verbesserte Notfallvorsorge zu erwarten ist (vgl. G 2.93), greifen die in diesem Eintrag genannten Maßnahmen stark in die betriebsinternen Prozesse des Dienstleisters ein. Im Einzelnen:

- Zuständigkeiten, Ansprechpartner und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
- Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.

Damit ist für öffentliche Cloud-Anbieter eine erhöhte Schwierigkeit bei der Durchsetzung dieser Maßnahmen festzustellen, während sich private und Community-Cloud-Anbieter bzw. klassische Anbieter vergleichbaren Problemen gegenübergestellt sehen. Allerdings können homogenisierte Systemlandschaften und Managementansätze durchaus zu einer Erleichterung bei der Durchführung von Notfallmaßnahmen führen, so dass sich hier für die beiden »geschlossenen« Cloud-Betriebsmodelle eine Verbesserung gegenüber klassischen Anbietern feststellen lässt. Darüber hinaus erleichtern Cloud-Eigenschaften, insbesondere das Ressourcen-Pooling bzw. dynamische Skalierung, die Etablierung redundanter Systemlandschaften und erhöhen somit insgesamt die Ausfallsicherheit.

M 6.109 (A) Notfallplan für den Ausfall eines VPNs

Die Verfügbarkeit eines VPNs kann durch Standardtechnologien und -vorgehensweisen auch in der Cloud gewährleistet werden.

Notfallpläne für »*Virtual Private Networks*« (VPNs) werden durch eine gesonderte Maßnahme behandelt. Es werden die folgenden Teilmaßmahmen betrachtet:

1. Festlegung von Verantwortlichkeiten für den Notfall
2. Einrichten von Notfallnummern
3. Einrichtung redundanter Kommunikationsverbindungen
4. Redundante VPN-Komponenten
5. Erstellung eines Wiederanlaufplans
6. Überprüfung der Datenintegrität nach der Störung
7. Notfallkonfiguration eines VPNs während eines Störfalls
8. Durchführung von Notfallübungen

Da diese Maßnahmen einerseits im Wesentlichen technischer bzw. organisatorisch- generischer Natur sind (mit Ausnahme von 8.), sie an-

dererseits zu einem großen Teil von den Notfallmaßnahmen des Cloud-Betreibers abgedeckt sind, kann auch im Fall einer öffentlichen Cloud davon ausgegangen werden, dass eine Implementierung verglichen mit der Implementierung bei einem herkömmlichen Dienstleister ebenso schwer oder sogar leichter ist. Darüberhinaus sind VPNs eine etablierte Technologie, deren Absicherung in Notfallsituationen mit Standardtechnologien und -vorgehensweisen erfolgen kann.

KAPITEL III.3

Gefahrenlage Datenschutz

Zusammenfassung

Ähnlich wie bei der Untersuchung des Outsourcing kommen wir zu dem Schluß, dass private und — wiederum mit Einschränkungen — Community-Clouds valide Modelle für öffentlich-öffentliche Kooperationen sind. Wiederum schneiden öffentliche Clouds im Vergleich zu klassischen Anbeitern schlecht ab. Die Gründe hierfür liegen einerseits in dem Aufgabenprofil öffentlicher Clouds, das nicht notwendigerweise auf den Umgang mit personenbezogenen Daten abgestimmt ist, andererseits in mangelnder Transparenz, da für den Auftraggeber umfassende Informationen über die Systeme und Prozesse des Dienstanbieters und ggf. Eingriffe in diese erforderlich sind.

III.3.1 Kontrollziele

Kontrollziele zum Schutz personenbezogener Daten sind in §9 BDSG definiert:

- Zutrittskontrolle, d. h. der Schutz der Datenverarbeitungsanlagen vor Zutritt durch Unbefugte.
- Zugangskontrolle, d. h. der Schutz vor Nutzung von EDV-Systemen durch unberechtigte, externe Dritte.
- Zugriffskontrolle, d. h. der Schutz vor internen Mitarbeitern ohne Zugriffsberechtigung.
- Weitergabekontrolle, d. h. der Schutz der Daten bei Speicherung oder Weitergabe vor unbefugtem Lesen, Kopieren, Verändern oder

Entfernen. Dieses Kontrollziel erfordert offensichtlich die Dokumentation, an welche Stellen eine Weitergabe vorgesehen ist.

- Eingabekontrolle, d. h. die Dokumentation, wann, von wem und welche Daten eingegeben, verändert oder entfernt worden sind.
- Auftragskontrolle, d. h. die Gewährleistung, dass Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- Verfügbarkeitskontrolle, d. h. der Schutz gegen zufällige Zerstörung oder Verlust von Daten.
- Einhaltung der Zweckbestimmung, d. h. Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden können.

III.3.2 Gefährdungen

Tab. III.3.1 fasst unsere Einschätzung der im Baustein B 1.5 aufgeführten Gefährdungen im Bezug auf Cloud-Anbieter bzw. klassische Dienstleister zusammen.

G 6.1 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten

Diese Gefährdung ist insbesondere bei öffentlichen Betriebsmodellen immanent, die keine expliziten Dienstvereinbarungen zulassen. Auch falls dies (wie im Fall einer exklusiven Cloud) möglich ist, ist die Zulässigkeit der Datenverarbeitung durch den Auftraggeber i. d. R. schwer nachzuvollziehen. Im Falle privater oder föderierter Modelle ergibt sich hingegen ein ähnliches Gefährdungsniveau wie im Fall herkömmlicher Dienstleister.

G 6.2 Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten

Die Einhaltung der Maßgabe, dass personenbezogene Daten nur für den Zweck gespeichert bzw. verarbeitet werden dürfen, ist für öffentliche Modelle nur schwer nachvollziehbar. Da in diesem Fall grundsätzlich ein besonderes Vertrauensverhältnis zwischen Auftraggeber und Dienstleister vorausgesetzt werden kann, muss der Auftraggeber mit der Weitergabe personenbezogener Daten an Dritte bzw. der unzweckmäßigen Verarbeitung solcher Daten rechnen.

Im Fall einer privaten Cloud ist hingegen das gleiche bzw. ein verringertes Gefährdungsniveau anzunehmen, da die Gefahr des »Abwanderns« personenbezogener Daten in heterogenen Infrastrukturen mit manuell verwalteten Diensten größer ist als in konsolidierten Infrastrukturen mit einheitlichen Sicherheits- und Datenschutzkonzepts. Für Community-Clouds, in denen Geschäftsprozesse u. U. mehrere Verwaltungsdomänen durchlaufen, ist wiederum ein erhöhtes Gefahrenniveau anzunehmen.

	Gefährdung	Öff.	Priv.	Comm.
G 6.1	Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten			
G 6.2	Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten			
G 6.3	Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten			
G 6.4	Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten			
G 6.5	Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten			
G 6.6	Fehlende oder nicht ausreichende Vorabkontrolle	Vgl. § G 6.6 (S. 97)		
G 6.7	Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten			
G 6.8	Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten	Vgl. Kapitel III.2		
G 6.9	Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen			
G 6.10	Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten	Vgl. § G 6.10 (S. 99)		
G 6.11	Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland	Vgl. Abschnitt II.2.3		
G 6.12	Unzulässige automatisierte Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten			
G 6.13	Fehlende oder unzureichende Datenschutzkontrolle			

Tabelle III.3.1
Einschätzung der im Grundschutzbaustein B 1.5 aufgeführten Gefährdungen im Vergleich zu herkömmlichen Dienstanbietern.

Legende:
- : *vermindert,*
- : *erhöht,*
- : *neutral,*
- — : *nicht anwendbar.*

G 6.3 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten

Der Eintrag G 6.3 diskutiert im Einzelnen die folgenden Gefährdungen:

- Bearbeitern werden Zugriffsbefugnisse auf Datenbestände gewährt, die für die aktuelle Aufgabenerfüllung nicht erforderlich sind.
- Weit reichende Zugriffsrechte der Systemverwalter und Netzadministratoren.

Können adäquate Rechtestrukturen in öffentlichen Clouds definiert und nachweisbar durchgesetzt werden?

Die Definition eines Systems adäquater, differenzierter Zugriffsrechte kann in privaten und Community-Clouds aufgrund des vorausgesetzten homogenisierten System- und Dienstmanagements mit einem im Vergleich zu herkömmlichen Dienstleistern vergleichbaren bzw. verringerten Aufwand geleistet werden. Bei öffentlichen Cloud-Betriebsmodellen stellt sich die Frage, ob eine solche Rechtestruktur mit dem Cloud-Betreiber vereinbart werden kann und inwieweit Kontrollmechanismen vorhanden sind. Darüber hinaus ist nicht klar, inwieweit die Rechte von Administratoren und Systemverwaltern in Umgebungen, die Diens-

te für einen heterogenen, nicht a-priori definierten Kundenkreis in einem Ressourcen-Pool zur Verfügung stellen (so dass eben nicht klar ist, für welchen Administrator gerade welche Zugriffsrechte relevant sind), eingeschränkt werden können.

Stellt »Mandantenfähigkeit« eine ausreichede Funktionstrennung sicher?

Eine weitere in G 6.3 genannte Gefahrenquelle ist die

- fehlende Funktionstrennung zwischen Systemtechnik, Programmierung, Anwendung und Kontrolle und eine fehlende Abschottung von Programmen.

Gegenüber herkömmlichen Dienstleistern, die eine physikalische Trennung der Systemlandschaften ihrer Kunden betreiben, muss für Cloud-Systeme, die Ressourcen virtualisiert verwalten, generell ein erhöhtes Gefahrenniveau angenommen werden. Hier zu beachten ist aber, dass sich solche Gefährdungen aus technischen Schwachstellen der verwendeten System ergeben: Cloud-Computing wird als »mandantenfähig« angesehen, so dass Daten, die sich auf verschiedene Kunden bzw. Prozesse beziehen, sicher voneinander getrennt gehalten werden können.

Abschließend schneiden private und Community-Clouds bzgl. der ersten beiden Punkte potentiell besser ab als herkömmliche Dienstleistungsszenarien, während sich die Einschätzung des dritten Punkts aus den aktuellen technischen Gegebenheiten ergeben muss.

G 6.4 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten

Auch hier ist es hilfreich, diese Gefährdung anhand der im Eintrag G 6.4 ausgeführten Beispiele genauer zu analysieren:

- Erhebung von mehr Daten, als für den Verarbeitungszweck benötigt werden.
- Verarbeitung von Daten in größerer Detaillierung als benötigt.

Die ersten beiden Punkte sind nur dann relevant, wenn nicht nur die Speicherung und Verarbeitung, sondern auch die Erhebung personenbezogener Daten durch den Cloud-Anbieter (und nicht durch die beauftragende Behörde) vorgenommen werden. Weiterhin beziehen sie sich auf die Art, wie eine solche Erhebung vorgenommen wird, die unabhängig von der gewählten Technologie ist. Allenfalls lässt sich im Fall öffentlicher Modelle ein leicht erhöhtes Gefahrenniveau feststellen, dass sich aus eventuell mangelhaften bzw. fehlenden Kontrollmechanismen ergibt.

Das letzte Beispiel bezieht sich u. a. auch auf technische Gegebenheiten:

- Verarbeitung und Speicherung von personenbezogenen Daten über einen längeren Zeitraum als dies für den Verwendungszweck notwendig ist, z. B. Sicherheitsanalysen von Protokolldateien einer Firewall.

Da die Verwendung von Daten für derartige sekundäre Zwecke im Fall einer öffentlichen Cloud nicht unbedingt nachvollziehbar ist, muss für öffentliche bzw. hybride Modelle ein erhöhtes Gefahrenniveau angenommen werden, während sich die Situation für private und Community-

Cloud-Betriebsmodelle nicht von der eines klassischen Dienstleisters unterscheidet.

G 6.5 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten

Wie kann die Einhaltung des Datengeheimnisses kontrolliert werden?

Diese Gefährdung bezieht sich auf den Zugriff auf bzw. die Verarbeitung von personenbezogen Daten durch Personen, die dazu nicht befugt sind. Der Eintrag G 6.5 gibt Unkenntnis der entsprechenden datenschutzrechtlichen Bestimmungen als eine der Hauptursachen dieser Gefährdung an, weiterhin *[. . .] das Nichtlöschen oder Verfälschen von gespeicherten personenbezogenen Daten, die Weitergabe von Adressdateien an Werbeunternehmen, die Weitergabe von personenbezogenen Daten innerhalb der Behörde oder des Unternehmens ohne dienstlichen Anlass, die unbefugte Einsichtnahme in Personaldaten, das Erstellen unzulässiger Auswertungen, die Nutzung dienstlicher Daten für private Zwecke (z. B. Weitergabe von Bonitätsdaten eines Nachbarn durch einen Mitarbeiter einer Bank im privaten Kreis)*.

Für private und Community-Clouds ist demzufolge ein Gefahrenniveau festzustellen, dass mit dem eines klassischen Dienstleisters vergleichbar ist. Für öffentliche bzw. hybride Modelle ist wegen des Problems der mangelnden Kontrollmöglichkeiten wiederum eine gesteigerte Gefährdung festzuhalten.

G 6.6 Fehlende oder nicht ausreichende Vorabkontrolle

Aus unzureichender oder fehlender Vorabkontrolle ergibt sich u. U. eine Gefährdung für das informationelle Selbstbestimmungsrecht. Der Eintrag G 6.6 analysiert die entsprechende Gefahrensituation allerdings eher unscharf durch den Verweis auf Gefahrenquellen, die bereits in Kapitel III.2 bzw. in diesem Kapitel diskutiert werden:

- Nutzung von Datenverarbeitungssystemen durch Unbefugte; Mangelnde Zugangs- oder Zutrittskontrollen.
- Verletzung der Vertraulichkeit bzw. Integrität der Daten während der Verarbeitung bzw. Verschlüsselung.
- Verletzung der Zulässigkeit bzw. Zweckbindung der Erhebung und Verarbeitung personenbezogener Daten.

Da aufgrund der vielschichtigen Gefahrensituation die Bildung eines »Mittelwerts« über die Bewertungen der entsprechenden Einträge nicht sinnvoll möglich ist, sehen wir von einer gesonderten Bewertung für diesen Eintrag ab.

G 6.7 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten

Dieser Eintrag verweist auf technische bzw. organisatorische Gegebenheiten, die z. B. das Recht auf Auskunft, Berichtigung, Sperrung, und

Löschung personenbezogener Daten gefährden und in unzulässiger Weise verwehren. Die zugrundeliegende Problematik, nämlich dass behördliche Prozesse von den verwendeten IT-Systemen strukturiert werden, reicht offenbar über die bloße Fragestellung, ob Cloud-Computing in der öffentlichen Verwaltung eingesetzt werden kann, hinaus, und kann in dieser Studie nicht behandelt werden.

Inwieweit werden behördliche Prozesse durch die verwendeten Technologien strukturiert? In der privaten Cloud können ungewollte Strukturen zumindest schneller aufgelöst werden.

Allerdings spricht zumindest in privaten bzw. Community-Cloud-Modellen die erhöhte Flexibilität sowie ein vereinheitlichtes Management dafür, dass Systeme, die derartige Einschränkungen involvieren, schneller ausgetauscht bzw. verbessert werden können. Unter der Voraussetzung, dass ein hinreichendes Dienstmanagement-Konzept vorliegt, das dem Auftraggeber ausreichende Kontrollmöglichkeiten gewährt, gilt diese Überlegung auch für öffentliche bzw. hybride Modelle.

G 6.8 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten

Die Gefährdungen, auf die sich dieser Eintrag bezieht, wurden bereits in Kapitel III.2 diskutiert.

G 6.9 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen

Dieser Eintrag bezieht sich einerseits auf die Informierung Betroffener bzw. auf Datenschutz-Kontrollinstanzen:

- Betroffene werden nicht über die Erhebung, Verarbeitung und Speicherung von Daten und die entsprechenden Rechtsgrundlagen informiert.
- Informationen zur Einführung und Freigabe neuer Verfahren, dem Erlass von Verwaltungsvorschriften, der Einrichtung von automatisierten Abrufverfahren oder einer Vergabe von Datenverarbeitung im Auftrag werden nicht an die entsprechenden Datenschutz-Kontrollinstanzen weitergeleitet.

Derartige Probleme können nicht in Beziehung zu Cloud-Computing gesetzt werden.

Ein homogenes Dienstmanagement kann die Transparenz erhöhen.

Andererseits werden jedoch technische und organisatorische Probleme genannt:

- Fehlende oder mangelhafte Protokollierung und Dokumentation.
- Fehlende Aktualisierung bei Verfahrensänderungen.
- Unvollständige oder nicht aktualisierte Verzeichnisse der eingesetzten IT-Systeme
- Mangelhafte Konfigurationsübersichten und fehlende Verkabelungspläne.

- Fehlende oder unvollständige Meldungen zu den internen Verzeichnissen und, soweit gesetzlich vorgeschrieben, zu den öffentlichen Verzeichnissen.

Werden proprietäre Systeme oder manuelle Lösungen zum Dienstmanagement verwendet, ist hier wegen der Problematik, die bei der Implementierung eines einheitlichen Managementkonzepts auftreten, ein gesteigertes Gefahrenniveau festzustellen. Für öffentliche Clouds hängt die Bewertung dieses Eintrags ebenfalls von der Existenz eines hinreichenden Dienstmanagements ab.

G 6.10 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten

Dieser Eintrag bezieht sich auf die Möglichkeit, dass Kontrollziele durch unzureichende technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten nicht erreicht werden. Wie schon bei der Diskussion von des Eintrags G 6.6 (S. 97) fasst der Eintrag Gefährdungen zusammen, die an anderer Stelle ausführlich diskutiert werden.

G 6.11 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland

Vgl. Abschnitt II.2.3.

G 6.12 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten

Unbestritten ist, dass Cloud-Computing geeignet ist, den Automatisierungsgrad von Prozessen zu erhöhen; dies bezieht sich jedoch zunächst nur auf technische Vorgänge wie Ressourcenallokation, Monitoring, Lastverteilung, usw. Die hier behandelten Automatisierungen bezieht sich aber auf die konkreten Fachverfahren und Entscheidungsprozesse und ist somit unabhängig von der Fragestellung, ob Cloud-Technologien eingesetzt werden oder nicht.

Unzulässige Analyse und Korrelation personenbezogener Daten durch Schadprogramme in der Cloud?

Allerdings ist natürlich darauf hinzuweisen, dass diese Automatisierungsmechanismen auch zur Einbringung von expliziten Entscheidungsalgorithmen verwendet werden können (z. B. zur Korrelation von Verhaltensdaten). Zumindest potentiell ist hier für öffentliche Cloud-Modelle und — wegen fehlender Kontrollmöglichkeiten — in geringerem Maße auch für private und Community-Cloud-Modelle also ein gesteigertes Gefahrenniveau festzustellen.

G 6.13 Fehlende oder unzureichende Datenschutzkontrolle

Kein Cloud-Anbieter kann es sich leisten, Datenschutz nicht ernst zunehmen.

Wird Datenschutz durch den Dienstleister ernst genommen? Sind Datenschutzbeauftragte nebenher mit anderen Aufgaben betraut, die ihre Aufmerksamkeit erfordern und u. U. Interessenskonflikte verursachen? I. Allg. muss gelten, dass Datenschutz um so mehr adäquat behandelt

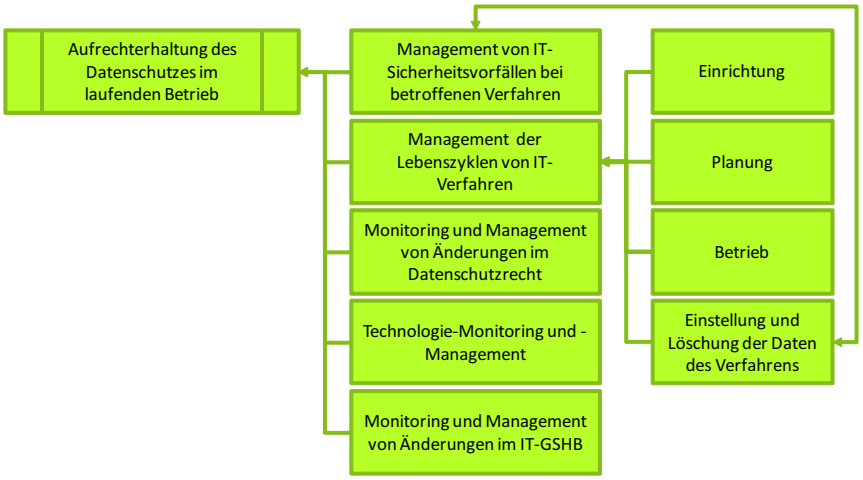


Abbildung III.3.1 *Teilprozesse des Datenschutzmanagements im laufenden Betrieb nach BSI Maßnahmenkatalog M 7.1.*

wird, je größer der Cloud-Betreiber ist. Die Bewertung dieses Eintrags fällt für öffentliche Cloud-Modelle also grundsätzlich positiv aus, da ein privatwirtschaftlicher Anbieter einer entsprechenden Größe Datenschutz als integrales Element seines Geschäftsmodells betrachten muss, wenn er als Partner für die öffentliche Verwaltung in Frage kommen möchte.

III.3.3 Maßnahmen

Unsere Analyse der vom BSI bzgl. Datenschutz vorgeschlagenen Maßnahmen wird in Tab. III.3.2 zusammengefasst.

III.3.3.1 Planung und Konzeption

M 7.1 (C) Datenschutzmanagement

Der Eintrag M 7.1 schlägt einen Prozess zur Etablierung eines Datenschutzmanagements vor, dessen detaillierte Diskussion an dieser Stelle zu weit führen würde und der zudem auf Maßnahmen verweist, die in den folgenden Abschnitten diskutiert werden.

Von besonderem Interesse für unsere Zwecke sind die in Abb. III.3.1 dargestellten Teilprozesse, die sich auf den laufenden Betrieb beziehen.

- Datenschutzmanagement von IT-Sicherheitsvorfällen zielt auf die Detektion und Bewertung von Vorfällen unter dem Gesichtspunkt des geltenden Datenschutzrechtes ab:
  - Priorisierung von technischen und organisatorischen Maßnahmen zur Problemanalyse und Problemlösung bzw. Beweissicherung unter Datenschutzgesichtspunkten
  - Behandlung juristischer Aspekte unter dem Gesichtspunkt des Datenschutzrechtes.

		Maßnahme	Öff.	Priv.	Comm.
M 7.1	(C)	Datenschutzmanagement			
M 7.2	(B)	Regelung der Verantwortlichkeiten im Bereich Datenschutz	—	—	—
M 7.3	(A)	Aspekte eines Datenschutzkonzeptes			
M 7.4	(A)	Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten			
M 7.5	(A)	Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten			
M 7.6	(A)	Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten			
M 7.7	(A)	Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten			
M 7.8	(A)	Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten			
M 7.9	(C)	Datenschutzrechtliche Freigabe			
M 7.10	(A)	Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten			
M 7.11	(A)	Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten	—	—	—
M 7.12	(A)	Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten			
M 7.13	(Z)	Dokumentation der datenschutzrechtlichen Zulässigkeit			
M 7.14	(A)	Aufrechterhaltung des Datenschutzes im laufenden Betrieb			
M 2.110	(A)	Datenschutzaspekte bei der Protokollierung			
M 7.15	(A)	Datenschutzgerechte Löschung bzw. Vernichtung	Vgl. § M 7.15 (S. 110)		

Tabelle III.3.2
Einschätzung der Durchsetzbarkeit der im Baustein B 1.5 aufgeführten Maßnahmen im Vergleich zu herkömmlichen Dienstanbietern.

Legende:
- : *leichter,*
- : *schwieriger,*
- : *neutral,*
- — : *nicht anwendbar.*

- Das Management der Lebenszyklen von IT-Verfahren unter Datenschutzgesichtspunkten wird in den folgenden Abschnitten detailliert diskutiert. Im Einzelnen:
  - In der Planung und Konzeption: Die Maßnahmen M 7.1 bis M 7.5
  - Umsetzung der Planung und Konzeption bis hin zum laufenden Betrieb: Die Maßnahmen M 7.6 bis M 7.12
  - Die Maßnahmen M 7.13 bis M 7.15 für den laufenden Betrieb
  - Nach Einstellung bis zur endgültigen Löschung des Verfahrens und aller zugehörigen Daten: Die Maßnahmen M 7.8, M 2.110 und M 7.15
- Management von Änderungen im Datenschutzrecht, die technologische Konsequenzen nach sich ziehen.
- Technologie-Monitoring unter Datenschutzgesichtspunkten verfolgt den »Stand der Technik« bezogen auf IT-Sicherheit und Datenschutz.
- Monitoring und Management von Änderungen in den IT-Grundschutz-Katalogen.

Potentiell sind Cloud-Anbieter in der Lage, ein effektives Datenschutzmanagement zu etablieren, wobei bei öffentlichen Clouds eine adäquate Protokollierung zu einem Problem werden kann.

Bereits diese oberflächliche Diskussion zeigt, dass integrierte IT-Infrastrukturen, für die ein einheitliches, konsolidiertes Dienstmanagement umgesetzt werden kann, datenschutzrechtlich besser abgesichert werden können als heterogene Infrastrukturen, die aus physikalisch und logisch getrennten Rechnern bestehen. Für alle drei untersuchten Varianten des Cloud-Computing muss deshalb bzgl. der Umsetzung eines Datenschutzmanagements generell eine Erleichterung festgestellt werden.

Allerdings können sich für öffentliche Modelle Schwierigkeiten bei der Protokollierung datenschutzrechtlich relevanter Aspekte ergeben (vgl. § 7.3).

M 7.2 (B) Regelung der Verantwortlichkeiten im Bereich Datenschutz

Diese Maßnahme bezieht sich auf personelle Maßnahmen und ist deshalb unabhängig von der Verwendung von Cloud-Computing-Technologien.

M 7.3 (A) Aspekte eines Datenschutzkonzeptes

Zur Etablierung eines Datenschutzkonzepts ist zu protokollieren, welche Aspekte der diskutierten Dienstleistungen datenschutzrechtlich relevant sind. Der Eintrag M 7.3 nennt im Einzelnen die in Tab. III.3.3 dargestellten Punkte.

Grundlegende Klassifizierung der Aspekte eines Datenschutzkonzepts.

Dabei wurden den verschiedenen Aspekten jeweils eine oder mehrere der folgenden Kategorien zugeordnet:

- Neutral — der Aspekt involviert keine Cloud-spezifischen Elemente.

Aspekt	Kategorie
Verzeichnis aller Verfahren	neutral
Umfang und Verwendung der zu verarbeitenden personenbezogenen Daten	Kontrolle
Rechtsgrundlage der Verarbeitung	neutral
Zweckbindung	Kontrolle
Berücksichtigung besonderer Datenarten	Kontrolle
Einhaltung von Datensparsamkeit und Datenvermeidung	Kontrolle
Schutzbedarf der Daten	neutral
Besonderheiten bei »Automatisierten Abrufverfahren«	Kontrolle
Verbot automatisierter Bewertungen	Kontrolle
Recht auf Auskunft, Berichtigung, Sperrung, Widerspruch, Schadensersatz und Vermeidung von Rechtsverletzungen und ihrer Folgen	Kontrolle
Löschung von Daten	Kontrolle
Protokollierung	Kontrolle
Vorabkontrolle	Kontrolle
Regelung der Verantwortlichkeiten im Datenschutz (vgl. § M 7.2)	neutral
Dokumentation und Verfahrensweise der Beteiligung des betrieblichen bzw. behördlichen Datenschutzbeauftragten	neutral
Dokumentation und Verfahrensweise der Beteiligung des Bundes- oder Landesbeauftragten für Datenschutz oder Beteiligung der Aufsichtsbehörde	Kontrolle, Ortsbindung
Vertragliche Regelungen einer Auftragsdatenverarbeitung	Vertrag
Besonderheiten einer Datenverarbeitung in Drittländern (u. a. Safe-Harbor-Regeln)	Ortsbindung
Technische und organisatorische Maßnahmen nach der Anlage zu § 9 BDSG bzw. entsprechenden Regelungen in den Landesdatenschutzgesetzen oder/und nach den spezialgesetzlichen Bestimmungen, Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge nach Zielvorgaben der Gesetze, Soll-Ist-Abgleich bei der Umsetzung und späteren Revision und datenschutzrechtlichen Kontrolle	Kontrolle, Ortsbindung
Verpflichtung auf den Datenschutz bzw. entsprechende Unterrichtung	neutral
Freigabe der Verfahren	Kontrolle
Verfahrensbeschreibung für jedes Verfahren	neutral
Meldungen an Registerstellen (vgl. § M 7.10)	Ortsbindung
Bestellung und Aufgaben eines Datenschutzbeauftragten (vgl. § M 7.2)	neutral
Berücksichtigung der unterschiedlichen datenschutzrechtlichen Zuständigkeiten (Bundesbeauftragter für Datenschutz, Landesbeauftragte für Datenschutz, Aufsichtsbehörden)	Ortsbindung

Tabelle III.3.3
Aspekte eines Datenschutzkonzeptes nach M 7.3.

- Kontrolle — der Aspekt bezieht sich auf die Kontrolle der Erhebung, Verwendung oder Speicherung personenbezogener Daten. I. Allg. schneiden private Cloud-Anbieter bzgl. solcher Maßnahmen in zu herkömmlichen Datenzentren vergleichbarer Weise ab. Für Community-Cloud-Anbieter ergibt sich aufgrund des heterogenen Kundenstamms ein leicht gesteigerter Schwierigkeitsgrad, da mehr (und möglicherweise widersprüchliche) Kontrollvorgaben zu berücksichtigen sind. Für öffentliche Anbieter muss dementsprechend ebenso ein erhöhter Schwierigkeitsgrad angenommen werden, der durch die Offenheit des Kundenstamms und den sich daraus ergebenden Sicherheitsbedenken noch gesteigert wird.
- Vertrag — Der Aspekt bezieht sich insbesondere auf vertragliche Anforderungen, d. h. auf die Möglichkeit, angepasste SLAs zu vereinbaren. Für private bzw. Community-Cloud-Anbieter sind beliebige Verträge denkbar. Entsprechend detaillierte Verträge sind mit öffentlichen Anbietern, die sich vertraglich auf AGBen zurückziehen bzw. einen großen heterogenen Kundenstamm pflegen, hingegen schwieriger zu schließen.
- Ortsbindung — Der Aspekt bezieht sich insbesondere darauf, wo personenbezogene Daten gespeichert bzw. verarbeitet werden. Sind z. B. landesspezifische Gegebenheiten zu berücksichtigen, muss der Cloud-Anbieter eine angemessene Berücksichtigung sicherstellen können. Weiterhin ist darauf zu achten, dass der jeweils zuständige Datenschutzbeauftragte beteiligt wird. Für öffentliche Cloud-Anbieter muss davon ausgegangen werden, dass eine derartig feingranulare Kontrolle des Speicher- und Verarbeitungsorts personenbezogener Daten ein Problem darstellt. Eine dynamisierte Wahl solcher Orte selbst innerhalb der Bundesrepublik ist wegen der Komplexität der zu berücksichtigenden Regelungen und der Notwendigkeit, fortlaufende Protokollierung vorzunehmen und an den zuständigen Datenschutzbeauftragten bzw. Registerstellen weiterzuleiten, nur schwer umzusetzen. Auf private bzw. Community-Cloud-Modelle ist diese Argumentation hingegen nicht anwendbar.

M 7.4 (A) Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

Hierbei sind die folgenden Aspekte zu beachten:

- Prüfung, ob personenbezogene Daten verarbeitet werden
- Zulässigkeit der Datenverarbeitung
- Erforderlichkeit der Datenverarbeitung
- Verwendung der Daten hinsichtlich der Zweckbindung
- Verwendung der Daten hinsichtlich der besonderen Zweckbindung
- Durchführung einer Vorabkontrolle

Wird ein öffentliches Cloud-Modell zugrundegelegt, sind an dieser Stelle die u. U. mangelhaften Kontrollmöglichkeiten bzgl. der Sicherstellung

der Zweckbindung der Verarbeitung personenbezogener Daten zu sehen. Weiterhin ist, falls die Datenerhebung durch den Cloud-Anbieter durchgeführt wird, eine angemessene Vorabkontrolle sicherzustellen, die sich u. a. auch auf Aspekte wie Zutrittskontrolle, Weitergabekontrolle sowie die getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten bezieht (vgl. § M 7.5). Für Community-Cloud Modelle ergibt sich gegenüber der Durchsetzbarkeit der Maßnahme durch einen klassischen Anbieter die Schwierigkeit, dass Daten in den Administrationsbereich eines anderen Rechenzentrums der »Community« gelangen und dort nicht korrekt behandelt werden. Für ein privates Cloud-Modell hingegen kann die Maßnahme aufgrund vereinheitlichter Management-Mechanismen einfacher durchgesetzt werden.

M 7.5 (A) Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Die Maßnahme M 7.5 zählt die folgenden Unterpunkte auf:

- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle,
- Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten.

Insbesondere bezüglich der Punkte Zutrittskontrolle, Zugangskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und getrennter Verarbeitung ergibt sich für öffentliche Cloud-Modelle ein gesteigerter Schwierigkeitsgrad, der abgeschwächt auch für das Community-Modell festgestellt werden muss. Für private Cloud-Anbieter, die über eine vereinheitlichte Dienstmanagement-Struktur und entsprechende technologische Unterstützung verfügen, kann die Maßnahme hingegen einfacher als durch einen klassischen Dienstleister durchgesetzt werden.

III.3.3.2 Umsetzung

M 7.6 (A) Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

Für einen öffentlichen Anbieter, dessen Mitarbeiter mit der Betreuung einer Vielzahl von Kunden beschäftigt sind, ist diese Maßnahme schwieriger als für einen klassischen Dienstleister durchzuführen. Für Community- und private Clouds ergibt sich ein vergleichbarer Schwierigkeitsgrad.

M 7.7 (A) Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

Die Maßnahme M 7.7 bezieht sich auf die Verfügbarkeit von technisch-organisatorischen Verfahren, *um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in Dateien- bzw. Verfahrensverzeichnisse [...] sicherzustellen. Diese Verfahren sollen so beschaffen sein, dass die Rechte der Betroffenen schnell und zweckmäßig umgesetzt werden können.*

Kann die Umsetzung derartiger Verfahren mit einem öffentlichen Cloud-Anbieter vereinbart werden?

Obwohl derartige Verfahren grundsätzlich auch in öffentlichen Clouds implementiert werden können, ist nicht unmittelbar klar, inwieweit ein solcher Anbieter bereit ist, entsprechende, ihrer Natur nach kundenspezifische Mechanismen zur Verfügung zu stellen. Für private und Community-Clouds kann diese Maßnahme unter der Annahme, dass solche Mechanismen in einer homogenen Management-Infrastruktur etabliert werden können, einfacher als durch einen klassischen Anbieter gewährleistet werden.

M 7.8 (A) Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten

Die IT-Systeme einer Cloud sind in ihrer Gesamtheit zu erfassen.

Die Maßnahme M 7.8 fordert, dass *[...] bei dezentraler Datenverarbeitung alle eingesetzten IT-Systeme zu erfassen [sind] [...]. Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten zugegriffen werden können.* Diesen Vorgaben sind für private Cloud-Anbieter mit heterogenem Kundenstamm kaum umsetzbar. Für private und Community-Clouds ergibt sich hingegen ein verringerter Schwierigkeitsgrad: Klassische, heterogene Infrastrukturen enthalten oftmals Mikrosysteme, die durch die Mitarbeiter in den entsprechenden Rechenzentren selbst entwickelt und nur von ihnen verwendet werden (Shell-Skripte, »kleine« Hilfsprogramme für Konfigurationsaufgaben, usw.), und die sich einer systematischen Erfassung entziehen.

M 7.9 (C) Datenschutzrechtliche Freigabe

Vgl. hierzu § G 2.26 (Seite 74). Private und Community-Clouds können umfassende Test- und Freigabeverfahren zur Verfügung stellen. Für öffentliche Anbieter ist dies nur eingeschränkt möglich, da Tests von potentiell schädlicher Software hier in eingeschränkten Umgebungen stattfinden muss (Simulationsumgebungen oder »*sand boxes*«), um den Betrieb der Produktionsumgebung nicht zu beeinträchtigen.

M 7.10 (A) Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

Können Dritte automatisiert auf personenbezogene Daten zugreifen?

Unter automatisierten Abrufverfahren werden solche Verfahren verstanden, bei denen eine datenverarbeitende Stelle Dritten automatisierten Zugang zu personenbezogenen Daten gewährt. Die Verantwortung für

einen solchen Abruf trägt dabei der Empfänger der Daten. Da auf diese Weise Dritten ein undifferenzierter Zugang zu sensiblen Daten gewährt wird, sind datenschutzrechtliche Aspekte bei solchen Verfahren besonders relevant.

Der Eintrag M 7.10 definiert eine Reihe von Maßnahmen gegen unbefugte Zugriffe, die im Wesentlichen einerseits die zu implementierenden Zugriffsmechanismen betreffen, anderseits die Protokollierung von Zugriffen, weiterhin für jeden Zugriff eine klare Zuordnung der abfragenden Stelle bzw. Person sowie die Gründe für den Zugriff.

Damit ist die Durchsetzbarkeit dieser Maßnahme für öffentliche Anbieter wiederum abhängig von den technischen Mechanismen zur Zugriffskontrolle sowie von den Protokollierungsmechanismen, die zur Verfügung gestellt werden. Mit dem Argument der homogenen Management-Infrastruktur kann für private und Community-Clouds abgeleitet werden, dass diese Maßnahme einfacher als durch einen klassischen Anbieter gewährleistet werden kann.

M 7.11 (A) Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

Dieser Eintrag betrifft die datenschutzrechtlichen Kriterien, die durch die beauftragende Behörde bei der Auslagerung von Datenverarbeitungsprozessen zu berücksichtigen sind: Welche Arten von Daten dürfen extern verarbeitet werden und welches Schutzniveau ist dafür anzusetzen? Die Maßnahme ist also unabhängig davon, ob ein Cloud- oder ein klassisches Angebot in Anspruch genommen werden soll.

M 7.12 (A) Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

Können Benutzerschnittstellen umgangen werden, um unerlaubten Zugriff auf personenbezogene Daten zu erlangen?

Dieser Eintrag bezieht sich auf die Verfügbarkeit technischer Mittel, die den Zugriff auf personenbezogene Daten unter Umgehung der Menüstruktur der dafür vorgesehenen Programme erlauben (z. B. »freie« SQL-Abfragen). Für öffentliche Cloud-Anbieter besteht das Problem, dass die Verfügbarkeit entsprechender Schutzmechanismen nicht vorausgesetzt werden kann bzw. klientenseitig implementiert ist: So kann eine generische Datenbank in der Cloud von einem versierten Mitarbeiter einer Behörde mit Hilfe eines selbstprogrammierten Werkzeugs unbefugt abgefragt werden, ohne dass für den Cloud-Anbieter eine Möglichkeit besteht, diese Abfrage von einer Befugten zu unterscheiden. Im Unterschied dazu können entsprechende Maßnahmen in einer privaten oder Community-Cloud auch auf Seiten des Anbieters etabliert werden. Da wir ein vereinheitlichtes Dienstmanagement voraussetzten, ist diese Maßnahme für private bzw. Community-Clouds leichter durchzusetzen als für klassische Dienstangebote.

III.3.3.3 Betrieb

M 7.13 (Z) Dokumentation der datenschutzrechtlichen Zulässigkeit

Jegliche Soft- und Hardware muss auf die datenschutzrechtliche Zulässigkeit geprüft werden, bevor sie zur Verarbeitung personenbezogener Daten verwendet wird. Für öffentliche Cloud-Anbieter ist diese Forderung nur schwer zu erfüllen, da Änderungen in deren Systemlandschaft jeweils vom zuständigen Datenschutzbeauftragten geprüft werden muss. Für private und Community-Clouds ergibt sich aufgrund des Arguments, dass hier eine homogene Dienstmanagement-Infrastruktur vorauszusetzen ist, eine Verbesserung der Durchsetzbarkeit dieser Maßnahme.

M 7.14 (A) Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Der Eintrag M 7.14 bezieht sich auf die Notwendigkeit der Einrichtung eines internen Prozesses zur IT-Revision und Datenschutzkontrolle. I. E. sind die folgenden Teilaufgaben genannt:

- die Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlage und der Zweckbestimmung,
- die Sicherstellung der Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz,
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- das Führen von Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen und
- die Kontrolle der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und »getrennten Verarbeitung gemäß der Zweckbestimmung«.

Aus den in den vorhergehenden Absätzen bereits genannten Gründen ergibt sich für öffentliche Cloud-Anbieter gegenüber klassischen Anbietern eine erschwerte Durchsetzbarkeit der Maßnahme, für private und Community-Cloud-Anbieter hingegen eine Erleichterung.

M 2.110 (A) Datenschutzaspekte bei der Protokollierung

Für viele technische Vorgänge ist eine detaillierte Protokollierung notwendig.

Die Bedeutung der Protokollierung interner Vorgänge beim Dienstleister wurde bereits verschiedentlich angesprochen. Der Eintrag M 2.110 definiert eine Reihe von Vorgängen, für die Protokollierung durchzuführen ist. So sind unter anderem die folgenden Aktivitäten vollständig zu protokollieren:

- Systemgenerierung und Modifikation von Systemparametern

- Einrichten von Benutzern
- Erstellung von Rechteprofilen
- Einspielen und Änderung von Anwendungssoftware
- Änderungen an der Dateiorganisation
- Durchführung von Datensicherungsmaßnahmen
- Sonstiger Aufruf von Administrations-Tools
- Versuche unbefugten Einloggens und Überschreitung von Befugnissen

Daneben sind Vorgänge beschrieben, für die (abhängig vom zugrundeliegenden Schutzniveau) ggf. eine selektive Protokollierung ausreichend ist:

- Eingabe von Daten
- Datenübermittlungen
- Benutzung von automatisierten Abrufverfahren
- Löschung von Daten
- Aufruf von Programmen

Vorgänge des Systemmanagements sind ebenfalls zu protokollieren, nicht nur kundenspezifische Dienstleistungen. Die Cloud-Eigenschaft »messbare Dienstqualität« ist nicht ausreichend.

Zu protokollierende Vorgänge beziehen sich also nicht nur auf den aktuellen Arbeitsvorgang, sondern auch auf Aktivitäten, die zur allgemeinen Aufrechterhaltung des Betriebs der IT-Infrastruktur notwendig sind. Selbst wenn mandantenfähige Dienstsoftware verwendet wird, die eine detaillierte Protokollierung von dienst- bzw. kundenspezifischen Vorgängen erlaubt, erstreckt sich die Notwendigkeit zur Protokollierung über diese hinaus. Für einen öffentlichen Cloud-Anbieter kann diese Maßnahme deshalb nur schwer umgesetzt werden.

Die Aufbewahrungsdauer von Protokolldateien ergibt sich aus der Erforderlichkeit der jeweilen Aufgabenerfüllung.

Weiterhin dürfen Protokolldateien nur für den Zweck genutzt werden, der Anlass für ihre Speicherung war, also z. B. die im Sicherheitskonzept festgelegten allgemeinen Kontrollen sowie die in den meisten Datenschutzgesetzen geforderte *Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden.* Zur Bestimmung der Aufbewahrungsdauer von Protokolldateien wird die Erforderlichkeit der jeweiligen Aufgabenerfüllung zugrunde gelegt. Da öffentliche Cloud-Anbieter u. U. einen breiten, heterogenen Kundenstamm betreuen, ergeben sich aus diesen Anforderungen möglicherweise Konflikte, welche Daten gespeichert werden dürfen und wann eine Löschung erfolgen muss. Auch für ein Community-Cloud-Modell muss aus diesem Grund hier ein erhöhter Aufwand für die Durchsetzung der Maßnahme M 2.110 festgestellt werden.

Technische und organisatorische Rahmenbedingungen zur Protokollierung

Schließlich beschreibt der Eintrag M 2.110 eine Reihe von technischen und organisatorischen Rahmenbedingungen, die zur Durchsetzung der Maßnahme etabliert werden müssen:

- Ein Revisionskonzept für Protokolle, Kontrollen und Schutzmechanismen.

- Mechanismen zur Gewährleistung der Zwangsläufigkeit, Vollständigkeit und Manipulationssicherheit.
- Zugriffsbeschränkungen entsprechend der Zweckbindung.
- Effektive, ggf. IT-unterstützte Überprüfbarkeit.
- Im Vorfeld abgestimmte Auswertungsmöglichkeiten.
- Zeitnahe Kontrollen.
- Kontrollen nach dem 4-Augen-Prinzip.
- Definierte Konsequenzen, die sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Regelmäßige, auch unangekündigte Durchführung von Kontrollen.
- Verwendung automatisierter Verfahren (*watch dogs*)

Wiederum sind diese Rahmenbedingungen durch einen öffentlichen Cloud-Anbieter kaum einzuhalten, während sich für private und Community-Cloud-Modelle verglichen mit einem klassischen Dienstleister eine erleichterte Durchsetzbarkeit ergibt.

M 7.15 (A) Datenschutzgerechte Löschung/Vernichtung

In virtualisierten Umgebungen ist die Löschung von Daten möglicherweise ein Problem, da Mechanismen fehlen, Speichermedien physikalisch zu beeinflussen. Für einen klassischen Anbieter, der ggf. keine Virtualisierungslösungen verwendet und personenbezogene Daten auf einer bestimmten definierten Festplatte hält, ist die eigentliche Durchführung einer sicheren Löschung ein geringes Problem.

Fristgerechte und sichere Löschung von Daten ist auch eine Frage des Dienst- und Datenmanagements.

Allerdings ist die Verfügbarkeit sicherer Methoden zur Datenvernichtung nicht hinreichend zur effektiven Durchsetzung der Maßnahme, wenn hierfür keine entsprechenden (ggf. automatisierten) Prozesse etabliert wurden. Diese sind in homogenen Management-Infrastrukturen leichter zu implementieren als in heterogenen Systemlandschaften. Demzufolge ist zumindest für private und Community-Clouds eine Erleichterung der Durchsetzbarkeit der Maßnahme festzustellen. Für öffentliche Clouds muss wegen u. U. mangelhafter Kontrollmöglichkeiten ein höherer Schwierigkeitsgrad angenommen werden.

KAPITEL III.4

Mindestanforderungen an die Sicherheit von Cloud-Computing

Zusammenfassung

Betrachtet man Mindestsicherheitsanforderungen an Anbieter, die Cloud-Technologien verwenden, ergibt sich für private und Community-Clouds ein durchaus deutliches Potential zur Erfüllung dieser Anforderungen, das sich aus den Cloud-Eigenschaften in Verbindung mit dem spezifischen Betriebsmodell ergibt. Für öffentliche Clouds ist dieses Potential in vielen Punkten nicht unmittelbar erkennbar — hier ist eine gesonderte Analyse des jeweiligen konkreten Angebots vorzunehmen.

In diesem Kapitel schließen wir die Analyse der Risiken des Cloud-Computings mit der Diskussion des Entwurfs eines »Eckpunktpapiers« (BSI, 2010b) des BSI ab, in dem Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter beschrieben werden. Wir beschränken uns dabei auf solche Aspekte, die für unsere Diskussion relevant sind und nicht bereits in ausreichender Form in den Kapiteln III.2 und III.3 behandelt wurden.

III.4.1 Bewertungsfaktoren

Im Gegensatz zu der in den Kapiteln III.2 und III.3 angewendeten Bewertungsmethodik, die auf dem Vergleich eines klassischen mit einem Cloud-Anbieter beruht, beziehen sich die Anforderungen, die in den folgenden Abschnitten diskutiert werden, auf Cloud-Anbieter; somit kann ein solcher Vergleichsansatz hier nicht (oder nur in Einzelfällen) Anwendung finden. Um dennoch zu einer Bewertung der Erfüllbarkeit dieser

Anforderungen zu kommen, definieren wir eine Reihe von Bestimmungsfaktoren, die einerseits auf Cloud-spezifische Technologien (und damit potentielle Schwachstellen dieser Technologien — vgl. Kapitel III.1), andererseits auf Cloud-Eigenschaften Bezug nehmen:

Verwendete Bewertungsfaktoren.

- Ressourcen-Pooling (Virtualisierung)
- Mandantenfähigkeit
- Betriebsmodell
- Identitäts- und Rechtemanagement
- Lokalität
- Protokollierung (messbare Dienstqualität, vgl. aber auch § M 2.110, S. 108)
- Portabilität und Interoperabilität

Interpretation der getroffenen Bewertungen.

Tab. III.4.1 fasst die Ergebnisse dieser Analyse zusammen. Dabei sind — da wir uns nicht auf eine konkrete Cloud-Infrastruktur beziehen können — die jeweiligen Bewertungen natürlich abstrakt und tendenziell. So sollte die Einschätzung »erfüllbar« als *grundsätzlich erfüllbar unter Ausnutzung des technologischen Potentials* gelesen werden. »Bedingt erfüllbar« bedeutet, dass das konkrete Cloud-Angebot genauer untersucht werden muss. Die Bewertung »nicht erfüllbar«, die im Übrigen nur in einem Fall vergeben wurde, bezieht sich hierbei lediglich auf das Fehlen adäquater Standards zum jetzigen Zeitpunkt.

Abschließend ist darauf hinzuweisen, dass unsere Analyse nicht die Bewertung des BSI Eckpunktpapiers zum Gegenstand hat, sondern umgekehrt die drei betrachteten Cloud-Computing-Betriebsmodelle (öffentliche, private und Community-Cloud) aus der Perspektive des Papiers kritisch beurteilt.

III.4.2 Sicherheitsmanagement beim Anbieter

Die in diesem Abschnitt genannten Anforderungen beziehen sich auf die Verfügbarkeit eines Informationssicherheitsmanagementsystems (ISMS) beim Cloud-Anbieter als Basisanforderung. Insbesondere ist gefordert, dass ein definiertes Vorgehensmodell für das Management von IT-Prozessen z. B. basierend auf ITIL[1] oder COBIT[2] beim Anbieter implementiert ist. Weiterhin wird die Verfügbarkeit eines ISMS z. B. nach (BSI, 2008b) oder (ISO, 2008) gefordert. Abschließend ist ein IT-Sicherheitskonzept zu erstellen, das den spezifischen Anforderungen des Cloud-Computings gerecht wird (wobei das Eckpunktpapier offenläßt, wie ein solches Konzept aussehen könnte).

Die Thematik »standardisiertes Dienstmanagement in der Cloud« ist nicht erschöpfend bearbeitet.

Die Anwendbarkeit eines standardisierten System- und Dienstmanage-

[1] Information Technology Infrastructure Library, vgl. (Cartlidge u. a., 2007)

[2] Control Objectives for Information and Related Technology, vgl. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

Anforderung	Bestimmungsfaktor	Öff.	Priv.	Comm.
Sicherheitsmanagement beim Anbeiter	Dienst- und Systemmanagement (vgl. Abschnitt III.4.2)	☀	☀	☀
Netzsicherheit	Netzbasierter Zugang	☁	☀	☀
Host- und Servervirtualisierung	Virtualisierung	☀	☀	☀
Plattform- und Anwendungssicherheit	Betriebsmodell	☁	☀	☀
	Mandantenfähigkeit, Virtualisierung	Vgl. Abschnitt III.4.3.3		
Datenspeicherung, Speichervirtualisierung und Datensicherheit	Mandantenfähigkeit, Virtualisierung	Vgl. Abschnitt III.4.3.4		
Verschlüsselung und Schlüsselmanagement	Kryptographie	☀	☀	☀
	Schlüsselmanagement	☁	☀	☀
Identitäts- und Rechtemanagement	Identitätsmanagement	☁	☀	☀
	Rechtemanagement	☁	☀	☁
Transparenz	Lokalität, Protokollierung	☁	☀	☀
Portabilität und Interoperabilität	Daten-Portabilität	☁	☁	☁
	Anwendungs-Portabilität	☁	☁	☁
	Cloud-Interoperabilität (vgl. aber auch Abschnitt III.4.6)	☔	☔	☔

Tabelle III.4.1
Einschätzung der im Eckpunktpapier (BSI, 2010b) des BSI aufgeführten Anforderungen zum Cloud-Computing.

Legende:
☀ : *erfüllbar,*
☔ : *nicht erfüllbar,*
☁ : *bedingt erfüllbar,*
— : *nicht anwendbar.*

ments (etwa nach ITIL/CoBIT) beim Cloud-Anbieter kann in dieser Studie nicht erschöpfend geklärt werden, wie auch die sehr allgemeine Formulierung dieser Anforderung deutlich macht, dass die genaue Beziehung solcher Standards zum Cloud-Computing noch einigen Klärungsbedarf aufweist. Dennoch zeigen sich aufgrund der Verfügbarkeit konsolidierter Mechanismen und Prozesse für Dienstüberwachung, Fehlermanagement usw. zumindest Potentiale für die Etablierung solcher Standards.

III.4.3 Sicherheitsarchitektur

Anforderungen an die Sicherheitsarchitektur eines Cloud-Anbieters werden aus verschiedenen Blickwinkeln diskutiert:

III.4.3.1 Netzsicherheit

Im Bereich Netzsicherheit, d. h. die Absicherung der Cloud-Infrastruktur gegenüber Angriffen auf Netzwerkebene, werden die folgenden Basisanforderungen gestellt:

- Schutz gegen Malware (Viren-, Trojaner-, und SPAM-Schutz)
- Sicherheitsmaßnahmen gegen netzbasierte Angriffe (»*Intrusion Prevention Systems*« (IPS) bzw. »*Intrusion Detection Systems*« (IDS))
- Abwehr von »*Distributed Denial-of-Service*« (DDoS) Attacken
- Absicherung von Fernwartungszugängen
- Physisch und logisch redundante Kommunikationsverbindungen zwischen Rechenzentren (erhöhte Verfügbarkeit)

Cloud-Basistechnologien zum netzbasierten Zugang.

Die hier zugrunde gelegten Gefährdungen beziehen sich auf potentielle Schwachstellen in Cloud-Basistechnologien, hier Netzwerkkomponenten zur Gewährleistung des »remote«-Zugangs bzw. zur Kommunikation von Rechnenzentren untereinander. Zumindest private und Community-Cloud-Anbieter, die auf dedizierte oder besonders gesicherte Netzwerke zugreifen, können diese Anforderung durch den Einsatz von Technologien erfüllen, die dem aktuellen Stand der Technik genügen. Für öffentliche Clouds sind die zugrundeliegenden Gefährdungen insbesondere auch aufgrund der Schwierigkeiten im Zusammenhang mit einer effektiven Zugriffskontrolle allerdings als schwerwiegend zu charakterisieren.

III.4.3.2 Host- und Servervirtualisierung

Weitere Basis-Technologien, die Angriffen ausgesetzt sein können, sind virtuelle Maschine (VMs) bzw. Unterstützungssysteme wie Hypervisoren. Dabei sind zunächst die physikalischen Rechner durch Maßnahmen wie dem Einsatz von IDSs bzw. IPSs, Firewalls, Integritatsüberprüfungen usw. abzusichern, um eine Manipulation von VMs und Hypervisoren auszuschließen. Sichere Default-Konfigurationen der Hosts (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.) erhöhen weiterhin das Sicherheitsniveau. Wieterhin empfiehlt das BSI für Systeme mit erhöhten Vertraulichkeits- und Verfügbarkeitsanforderungen den Einsatz zertifizierter Hypervisoren (Common Criteria EAL 4 oder größer[3]).

Besondere Anforderungen an Infrastruktur-Anbieter.

Insbesondere für Infrastruktur-Dienstanbieter wird weiterhin gefordert, dass veröffentlichte Benutzer-Richtlinien zur Absicherung von virtuellen Maschinen zur Verfügung stehen. Weiterhin muss die Möglichkeit gegeben sein, kundeneigene Images für virtuelle Maschinen einzusetzen

[3] Der internationale Standard »*Common Criteria for Information Technology Security Evaluation*« (kurz Common Criteria) definiert Kriterien zur Bewertung und Zertifizierung der Sicherheit von Computersystemen im Hinblick auf Datensicherheit. Die »*evaluation assurance level*« (EAL) definieren sieben Stufen der Vertrauenswürdigkeit bezüglich der Korrektheit der Implementierung des betrachteten Systems bzw. die Prüftiefe: EAL 4 bedeutet hierbei: *methodisch entwickelt, getestet und durchgesehen*. Vgl. auch http://www.commoncriteriaportal.org.

und qualitätsgesicherte Images zur Verfügung zu stellen. Schließlich sind die Zugänge für den Zugriff auf VMs besonders durch eine Multifaktor-Authentisierung zu sichern.

Virtualisierung ist Stand der Technik.

Wiederum beziehen sich die Anforderungen des BSI auf Schwachstellen, die sich aus Basistechnologien des Cloud-Computings (hier Virtualisierung) ergeben. Allerdings ist darauf hinzuweisen, dass Virtualisierung längst Stand der Technik ist und insbesondere auch von behördlichen Dienstleistern extensiv genutzt wird; die entsprechenden Anforderungen müssen also grundsätzlich als erfüllbar angesehen werden.

III.4.3.3 Anwendungs- und Plattformsicherheit

Sicherheit muss bereits bei der Entwicklung und dem Test von Software für die Cloud berücksichtigt werden.

Die Verfügbarkeit schwachstellenarmer Software ist eine Grundlage für Anwendungs- und Plattformsicherheit. So wird etwa verlangt, dass Sicherheit zu einem Bestandteil des Entwicklungszyklusses einer Anwendung in Form von entwicklungsbegleitenden Maßnahmen und Freigabemaßnahmen (z. B. Reviews, automatisierte Tests, Schwachstellentests usw.) wird. Für Plattform-Dienste sind solche entwicklungsbezogenen Anforderungen auch für die Cloud-Kunden (die hier als Entwickler bzw. Anwender von Softwarelösungen auftreten) relevant und müssen durch entsprechende Richtlinien fixiert werden.

Öffentliche Cloud-Anbieter (PaaS) haben keinen Einfluß auf Kundensoftware und potentiellen Gefährdungen.

Hier handelt es sich in erster Linie um eine generische Anforderung, die nicht unmittelbar mit den Spezifika des Cloud-Computings in Verbindung zu bringen ist. Öffentliche Cloud-Anbieter haben innerhalb eines Plattform-Angebots allerdings nur in geringen Umfang die Möglichkeit, die Qualität von Kundensoftware zu überprüfen oder gar Einfluss auf die entsprechenden Entwicklungsprozesse zu nehmen. Für private und Community-Cloud-Anbieter, die entweder Software selbst entwickeln, Dritte mit Entwicklungsaufgaben betrauen oder Freigabeverfahren für Standard-Software etablieren, sind derartige Anforderungen sicher erfüllbar. Darüber hinaus ist noch zu bedenken, dass Cloud-basierte Ausführungsumgebungen bereits eine Reihe von Sicherheitsmechanismen bieten (z. B. Kapselung von der physikalischen Hardware und Netzwerkschnittstellen, überwachte Lebenszyklen, usw.), die bei der Entwicklung »gehärteter« Software Verwendung finden können.

Mandantenfähigkeit auf Anwendungs- und Plattformebene ist ebenfalls von Interesse: Anwendungen müssen gekapselt ausführbar und Daten verschiedener Anwendungen und Anwendungsinstanzen isoliert voneinander gehalten werden, um Gefahren zu vermeiden, die sich aus dem unerlaubten Zugriff auf Applikationen und Daten ergeben. Eine Bewertung der Immanenz der entsprechenden Gefährdungen hängt also davon ab, inwieweit eine konkrete Cloud-Infrastruktur entsprechende Schwachstellen aufweist.

III.4.3.4 Datenspeicherung, Speichervirtualisierung und Datensicherheit

Die Anforderungen des BSI an Datenspeicherung und -sicherheit in virtualisierten Umgebungen gehen nicht über die in Kapitel III.3 diskutierten Maßnahmen hinaus.

Im Zusammenhang mit Cloud-Computing wird an dieser Stelle insbesondere die Existenz potentieller Schwachstellen problematisiert, die aus einer mangelnden Abschottung von Daten und Prozessen eines Kunden gegenüber denen anderer Kunden resultieren (Mandantenfähigkeit). Weiterhin wird auf die bereits angesprochenen Probleme im Zusammenhang mit Datenlöschung und dem Verhältnis virtualisierter zu physikalischen Speicherbereichen hingewiesen.

III.4.3.5 Verschlüsselung und Schlüsselmanagement

Kommunikation ist grundsätzlich zu verschlüsseln.

Strenge Anforderungen sind an die Kommunikation einerseits zwischen Cloud-Kunde und -Anbieter, andererseits zwischen verschiedenen Rechenzentren in der Cloud gestellt: Ein derartiger Datenaustausch ist grundsätzlich zu verschlüsseln. Das BSI unterscheidet hierbei nicht zwischen dem Austausch personenbezogener bzw. aus anderen Gründen sensibler und sonstiger Daten; für letztere ist die Notwendigkeit einer Verschlüsselung nicht unmittelbar einsichtig.

Ein gewisses Problem im Zusammenhang mit verschlüsselter Datenübertragung ergibt sich aus dem Aufwand bei der Ausführung der verwendeten kryptographischen Algorithmen, die bei der Übertragung großer Datenmengen durchaus zu Buche schlägt. Dennoch sind Mechanismen wie TLS[4] oder SSL[5] heute Stand der Technik, so dass diese Anforderung an Cloud-Anbieter grundsätzlich als erfüllbar angesehen werden muss.

Effektives Schlüsselmanagement: Best Practices.

Darüberhinaus wird auf »Best-Practices« im Bereich Schlüsselverwaltung hingewiesen:

- Administratoren sollten keinen Zugriff auf die Schlüssel haben
- Schlüssel sollten niemals im Klartext offengelegt werden
- Zugang zu Schlüsselverwaltungsfunktionen sollten eine separate Authentisierung erfordern
- Maßnahmen zum Schutz der zwischengespeicherten Schlüssel
- Sichere Archivierung von Schlüsseln
- Sichere Replizierung von Schlüsseln

Obwohl die Berechnung von Schlüsseln in virtualisierten Umgebungen mit gewissen Problemen verbunden ist (vgl. Abschnitt III.1.1.2), kann zumindest für private und Community-Clouds die Implementierung eines

[4] Transport Layer Security

[5] Secure Sockets Layer

effektiven Schlüssel-Managementsystems, das den oben genannten Anforderungen genügt, als durchaus möglich angesehen werden. Für öffentliche Clouds ist ein solches Management-System wegen des a-priori nicht feststehenden Kundenkreises nur bedingt implementierbar.

III.4.4 Identitäts- und Rechtemanagement

Die Existenz geeigneter Zugriffskontrollen ist im Kontext von Cloud-Computing aus zwei Gründen von Interesse:

- Einerseits werden Cloud-Dienstleistungen »remote« zur Verfügung gestellt. Daraus ergibt sich die Notwendigkeit, besondere Authentisierungsmechanismen zur Verfügung zu stellen, um den unerlaubten Zugriff und die Manipulation von Daten und Prozessen zu verhindern. Insbesondere in öffentlichen Clouds ergibt sich die Schwierigkeit, dass der Kundenkreis in diesem Betriebsmodell nicht a-priori definiert ist: Ein Angreifer kann i. Allg. lediglich aufgrund der Authentifizierungsinformation, die vom Cloud-Anbieter gefordert werden, von einem erlaubten Benutzer unterschieden werden. Das BSI fordert aus diesem Grund den Einsatz von Multifaktor-Authentisierungmechanismen.

  Netzwerkbasierter Zugang.

- Andererseits ergibt sich das besondere Problem, die Rechte von Mitarbeitern des Cloud-Anbieters, insbesondere Systemadministratoren, in adäquater Weise zu definieren und durchzusetzten; eine Schwierigkeit, die in Community-Cloud-Ansätzen, in denen u. U. überlappende Administrationsbereiche existieren, besonders immanent ist. In öffentlichen Clouds besteht überdies das Problem, dass Rechtestrukturen nur sehr generisch und im Einzelfall u. U. nicht differenziert genug definiert und werden können.

  Rechteverwaltung.

III.4.5 Transparenz

Anforderungen bezüglich der Offenlegung von Systemen, Software usw., die durch den Cloud-Anbieter verwendet werden, wurden bereits in Kapitel III.3 diskutiert. An dieser Stelle ist auf verschiedene Cloud-spezifische Anforderungskategorien hinzuweisen:

- Die Standorte (Land, Region) des Cloud-Anbieters, die ja als Ressource-Pools dynamisch einbezogen werden können, müssen bekannt sein, um datenschutzrechtliche Auflagen zu erfüllen.

  Ortsbezug — in welchen Bundesländern und Regionen sind die Rechenzentren des Cloud-Anbieters beheimatet?

- Ebenfalls aus rechtlichen Gründen muss offengelegt werden, ob ein Cloud-Anbieter eventuelle Subunternehmer hinzuzieht (insbesondere auch dynamisch im Sinne eines »*Cloud burst*«). Die »Vererbung« von SLAs auf Subunternehmer muss durchsetzbar und für den Kunden nachvollziehbar gestaltet werden.

  Werden Subunternehmer hinzugezogen?

- Eine aktive Validation von Sicherheitsmechanismen — etwa durch Penetrationstests durch den Kunden — muss möglich sein.

  Validation von Sicherheitsmechanismen.

Klientenseitige Konfiguration.

- Ein Aspekt, der bisher nicht diskutiert wurde, besteht in den Eingriffen, die ein Cloud-Anbieter automatisiert auf dem Klienten des Kunden vornimmt (Konfigurationsänderungen, Installation von Software und Diensten für Zugriff und Authentisierung, usw.). Das BSI verlangt hier die Berücksichtigung eines Erlaubnisvorbehalts durch den Kunden.

Grundsätzlich sind diese Anforderungen für private und Community-Cloud-Anbieter erfüllbar. Für öffentliche Anbieter ist die Erfüllbarkeit abhängig von konkreten Angeboten.

III.4.6 Interoperabilität und Portabilität von Daten und Anwendungen

Neben Sicherheits- und datenschutzbezogenen Bedenken ist die Befürchtung, sich in eine »lock-in« Situation, d. h. in die Abhängigkeit von einem bestimmten Anbieter zu begeben, einer der meistgeäußerten Vorbehalte gegen die Inanspruchnahme von Cloud-Dienstleistungen. Dies betrifft sowohl Datenformate als auch Anwendungen (nicht nur, wie im BSI-Papier eingeschränkt, SaaS-Angebote, sondern auch Plattform- und Infrastruktur-Angebote, für die sich ja ebenso Kompatibilitätsprobleme ergeben können).

Standards zur Cloud-Interoperabilität sind bisher nicht vorhanden.

Andererseits ist es zur Etablierung von Community-Clouds bzw. hybriden Betriebsmodellen notwendig, Cloud-Infrastrukturen interoperabel zu gestalten, was durch die Verwendung standardisierter Schnittstellen, Protokolle usw. erreicht werden kann. Obwohl entsprechende Standardisierungsaktivitäten bei verschiedenen Institutionen eingeleitet worden sind, befinden sich diese jedoch erst in der Anfangsphase. Diese Anforderung ist zum augenblicklichen Zeitpunkt deshalb nicht erfüllbar.

III.4.7 Zusatzanforderungen an öffentliche Cloud-Anbieter

Abschließend sei auf die Anforderungen des BSI hingewiesen, die sich aus dem Einsatz von öffentlichen Cloud-Angeboten für die Bundesverwaltung ergeben:

- Vertrag mit Gerichtsstandort Deutschland und deutsches Recht[6]
- IT-Revisionsrecht für das BSI stellvertretend für die Bundesverwaltung
- Zusammenarbeit mit dem CERT-Bund[7] und dem IT-Krisenreaktionszentrum im BSI

[6] Vgl. hierzu auch Abschnitt II.2.3: Die EU-DSRL läßt immerhin einen Gerichtsstandort innerhalb Europas vor.

[7] Computer Emergency Response Teams, vgl. https://www.bsi.bund.de/cln_174/ContentBSI/Publikationen/Faltblaetter/F22CERTBund.html.

- Berechtigung des BSI zur Durchführung von Penetrationstests in der Cloud

Mit Ausnahme des letzten Punktes sind diese Anforderungen — die hier im wesentlichen der Vollständigkeit halber genannt werden — nicht auf technischer bzw. organisatorischer Ebene angesiedelt und werden deshalb in unserer Analyse nicht weiter berücksichtigt.

KAPITEL III.5

Positionen der Anbieter

Zusammenfassung

Einige der in dieser Studie aufgeworfenen Fragen sowie — um den konkreten Stand der Technik zumindest in einigen Bereichen zu ermitteln — allgemeine Fragen zum Cloud-Computing wurden in einem weiteren Fragebogen zusammengefasst und an zwei Cloud-Dienstanbieter sowie einen Hersteller von Cloud-Technologien versandt. Aus den Antworten lässt sich schließen, dass das konkrete Angebot bereits in vielen Aspekten der Idee der Cloud entspricht (wenn auch an verschiedenen Stellen noch Nachholbedarf besteht, z. B. im Hinblick auf Elastizität). Insbesondere bestehen vielfältige Ansätze für ein integriertes System- und Dienstmanagement.

Migration und Portierung von Daten und Anwendungen in bzw. für die Cloud wird durch entsprechende Werkzeuge unterstützt. Datenschutz und Sicherheit wird als Anforderung erkannt, wobei allerdings in den Details noch ein Abgleich mit den Anforderungen des BSI vorgenommen werden muss. Insbesondere die geforderte enge Zusammenarbeit zwischen Anbieter und Auftraggeber bei Outsourcing-Projekten zur Erstellung gemeinsam Sicherheitskonzepte, die in Kapitel III.2 diskutierte wurde (und die unabhängig von einer Zertifizierung des Anbieters durchgeführt werden muss), wird nicht oder nur in Ansätzen reflektiert. Auch sind datenschutzbezogene Fragen bzgl. der Transparenz interner Vorgänge zu klären.

Einige der in dieser Studie aufgeworfenen Fragen sowie — um den konkreten Stand der Technik zumindest in einigen Bereichen zu ermitteln — allgemeine Fragen zum Cloud-Computing wurden in einem weiteren Fragebogen zusammengefasst und an zwei Cloud-Dienstanbieter sowie einen Hersteller von Cloud-Technologien versandt. Wir geben in diesem

Kapitel eine kurze Zusammenfassung der Ergebnisse der Umfrage. Eine vollständige Liste der gestellten Fragen und die (anonymisierten) eingegangenen Antworten findet sich in Anhang C.

III.5.1 Elastizität

Automatische Ressoucen-Skalierung.

Die elastische Skalierung von Ressourcen wird zumindest teilweise umgesetzt. Einerseits werden Ressourcen innerhalb von Maximalgrößen, die durch den Kunden während des Vertragsabschlusses mit dem Anbieter gewählt werden, automatisch zu skalieren. Dies geschieht unter Berücksichtigung der aktuellen Verkehrssituation, d. h. Lastspitzen werden im Rahmen dieser Maximalgrößen abgefangen. Weiterhin stehen Mechanismen zur Verfügung, Ressourcenverfügbarkeit manuell über Administrationsschnittstellen bzw. programmatisch über API's anzupassen.

Verteilung von Prozessorlast.

Die Verteilung von rechenintensiven Operationen auf mehrere Prozessoren ist grundsätzlich möglich, wobei dies bei einem der befragten Anbieter über eine spezielle Middleware automatisiert erfolgen kann. In einem anderen Fall muss dies durch den Benutzer (etwa durch die Wahl geeigneter »Instanzen« seiner Applikationen in der Cloud) gesteuert werden.

Die vielfach diskutierte Option eines »Cloud-bursts«, d. h. der temporäre Zuschaltung von Cloud-Ressourcen eines Drittanbieters, um Lastspitzen abzufangen, wird von keinem der Anbieter unterstützt. Ein ähnliches Szenario, in dem die Dienstleistungen eines Anbieters etwa im Katastrophenfall oder auch bei Insolvenz mittel- oder langfristig bzw. permanent auf einen anderen Anbieter umgelagert werden, wird ebenfalls nicht betrachtet. Allerdings verweist der Hersteller auf konkrete (namentlich genannte) Cloud-Anbieter, über deren Ressourcen ein derartiger Skalierungsmechanismus realisiert werden kann.

Obwohl Kunden hier eine grundsätzliche Option zur bedarfsgerechten Anpassung der verwendeten Ressourcen an die Hand gegeben wird, ist man noch nicht vollständig bei der »Illusion der unendlich verfügbaren« Ressourcen angelangt.

III.5.2 Dienstüberwachung und Dienstmanagement

Monitoring.

Beide Anbieter und der Hersteller offerieren weitreichende Monitoring-Mechanismen, um die Dienstausführung auf verschiedenen Ebenen zu überwachen. Einer der Anbieter stellt Monitoring-Schnittstellen plattformunabhängig als REST[1] API zur Verfügung. Der Hersteller bietet eine Unterstützung für die Verknüpfung von Lastmessungen mit Aktivitätsmessungen auf Geschäftsprozess-Ebene.

Der Hersteller bietet weiterhin verschiedene Werkzeuge für die Provisionierung, der Pflege eines Kundeninformationsmodells und eines Servicekatalogs, zum Kapazitätsmanagement, für das Metering und Billing und

[1] REpresentational State Transfer (Architektur), vgl. z. B. http://www.oio.de/public/xml/rest-webservices.htm.

für Ressourcen-Management zur Verfügung. Ein wichtiges Mittel dafür ist die Virtualisierung, gekoppelt mit einer Management-Infrastruktur, die die Bereitstellung von standardisierten Ressourcen (virtuelle Maschinen, Service-Ablaufumgebungen, Speicherplatz) regelt, sowie deren Integration in die Unternehmens-Infrastruktur im Sinne eines mess- und abrechenbaren Selbstbedienungs-Modells.

Datenbankredundanz.

Redundanzmechanismen zur Erhöhung der Verfügbarkeit eines Cloud-Dienstes werden i. d. R. zur Verfügung gestellt. Einer der Anbieter hält z. B. Datenbanken automatisch dreifach auf unterschiedlichen Maschinen in unterschiedlichen Rechenzentrumsbereichen vor, auf die im Falle eines Ausfalls automatisch umgeschaltet wird. Über gängige SQL-Schnittstellen kann der Kunde zusätzlich private Datenreplikationen durchführen. Für Applikationsinstanzen werden für die ausfallsichere Varianten dabei mindesten zwei Instanzen vorgehalten.

Weiterhin stehen dem Kunden (bei einem der beiden Anbieter) umfangreiche Statusmeldungen für die Überwachung seiner Anwendungen zur Verfügung. Dazu können mehrere Versionen von Anwendungen parallel betrieben werden, sodass der Kunde z. B. eine nicht funktionierende Anwendung gegen eine frühere Version austauschen kann. Dabei überwacht der Anbieter die Verfügbarkeit und das Laufzeitverhalten der entsprechenden Anwendungen und schaltet bei Bedarf auf eine andere Instanz um. Der befragte Hersteller offeriert Werkzeugunterstützung für ähnliche Mechanismen.

Redundante Lagerung von Benutzerdaten.

Benutzerdaten werden ebenfalls redundant gehalten. Allerdings sind die IaaS- bzw. PaaS-Dienste agnostisch gegenüber applikationsspezifischen Daten, die der Benutzerverwaltung des Cloud-Kunden (der dann als Dienstleister gegenüber Dritten auftritt) angehören.

III.5.3 Migration und Portabilität

Datenbankmigration.

Zur Migration von Datenbanken in die Cloud stehen Werkzeuge zur Verfügung (die sich allerdings lediglich auf Datenbank-Produkte eines Herstellers beziehen). Verfahren zur Datenbankmigration sind allerdings dokumentiert. Einige Anbieter limitieren darüber hinaus die Größe der Datenbanken in ihren Clouds, wobei allerdings Partitionierungs- und Kombinationsmechanismen angeboten werden.

Zur Rettung von Benutzerdaten im Fall der Beendigung des Vertragsverhältnisses stellen beide Anbieter eine Reihe vertraglichen Optionen zur Verfügung, die spezifische Fristen, eingeschränkte Zugänge zum Benutzer-Account, bis hin zur Datenübergabe über physikalische Medien (CD/DVD) umfassen.

Portierung vor Applikationen.

Applikationen können auf Tauglichkeit für die Cloud sowohl unter Verwendung von Simulationsumgebungen als auch in der realen Cloud getestet werden. I. d. R. werden gängige Programmier- und Skriptsprachen wie .NET, Java, PHP oder Ruby unterstützt. Allerdings ist die Portierung einer Anwendung in die Cloud offenbar ein u. U. komplexer Vorgang, den einer der beiden befragten Anbieter die folgt beschreibt:

Nach einer »Workload Analyse«, der Selektion des Programmiermodels, der Bestimmung des Virtualisierungskonzepts, einer Backend-Integrationsdiskussionen (Datenbank, Applikationsserver, etc.), einer Schnittstellen-Analyse und einer Sicherheitskonzept-Definition kann die in Rede stehende Anwendung durch das Kreieren eines Images (oder mehrerer Images) und der Konfiguration der Netzinfrastruktur migrierbar sein. In den meisten Fällen ist jedoch eine komplexere Analyse nötig.[2]

III.5.4 Standort

Rechenzentrumsstandorte können auf die EU beschränkt werden.

Beide Anbieter offerieren dem Benutzer die Möglichkeit, die Standorte, an denen (etwa personenbezogene) Daten gespeichert werden, auf bestimmte Rechenzentren (oder solche innerhalb bestimmter geographischer Grenzen) zu beschränken. Bei einem der Anbieter kann der Kunde Rechenzentrumsstandorte in der EU auswählen. Eine Garantie für die Speicherung an einem bestimmten Ort kann allerdings nicht gegeben werden, da Ressourcen-Pools rechenzentrumsübergreifend betrieben werden.

III.5.5 Mandantenfähigkeit

Beide Anbieter und der Hersteller offerieren Mechanismen zur mandantenfähigen Verwaltung von Benutzerdaten (d. h. zur logischen Trennung von Daten verschiedener Benutzer) zumindest auf Infrastruktur- bzw. Plattformebene.

III.5.6 Sicherheit und Datenschutz

Verschlüsselung von Benutzerdaten und Kommunikation.

Benutzerdaten zur Identifikation des Benutzers (zwecks Abrechnung etc.) werden verschlüsselt gespeichert. Für die eigentlichen Anwendungen hängt es von der konkreten Implementierung ab, ob und wie Verschlüsselung eingesetzt wird. Entwicklern stehen entsprechende Methoden zur Verfügung, um anwendungsspezifische Daten zu verschlüsseln bzw. verschlüsselt abzulegen. Mechanismen zur Verschlüsselung der Kommunikation werden grundsätzlich angewendet.

DDos-Attacken.

Eine oft diskutierte Gefahr ist die Verwendung von Cloud-Infrastrukturen zur Durchführung von »Distributed Denial-of-Service«-Attacken (DDoS). Beide Anbieter stellen Mechanismen zur Verfügung, um einem solchen Szenario entgegenzuwirken.

So gibt z. B. einer der Anbieter an, den Netzwerkverkehr innerhalb seiner Rechenzentren, zwischen seinen Rechenzentren und den ein- bzw. ausgehenden Netzverkehr zu überwachen und somit eine DDoS-Attacke feststellen und adäquat reagieren zu können. Weiterhin behält sich der

[2] Redaktionelle Änderungen zur Anonymisierung durch die Autoren.

Anbieter das Recht vor, den Online-Dienst eines Kunden auszusetzen, falls er der Ansicht ist, dass die Verwendung des Online-Dienstes eine direkte oder indirekte Gefahr für die Funktion oder Integrität des Netzwerks oder die Verwendung des Online-Dienstes durch andere darstellt. Ein ähnlicher Mechanismus dient auch zum Schutz der eigenen Cloud gegen DDoS-Angriffe. Allerdings erklärt der befragte Hersteller, dass »›*Distributed Denial-of-Service‹-Attacken [...] nur in privaten Clouds in kompletter Isolation zu vermeiden [sind], sowie bei Vergabe von Ressourcen-Quotas an berechtigte und zugelassene Teilnehmer ohne eine Weitergabe an Dritte.*«

Forensische Maßnahmen.

Beide Anbieter unterstützen forensische Maßnahmen im Rahmen der gesetzlichen Vorgaben. Kunden können über definierte Monitoring- und Managementschnittstellen auf ihre anwendungsbezogenen Daten zugreifen, um Fehleranalysen durchzuführen: Dies gilt also nur für Protokolle, die eigene Daten oder Dienste betreffen.

Notfallkonzept.

Beide Anbieter etablieren ein Notfallkonzept, auf das Kunden allerdings keinen Einfluss haben. Die Anbieter verweisen an dieser Stelle auf ihre langjährige Erfahrung als Rechenzentrumsbetreiber.

Sicherheitskonzept.

Sicherheitskonzepte können kundenspezifisch (und nur auf Dienstebene) angepasst werden, allerdings kann dies i. d. R. nur unter Verwendung vordefinierter Optionskataloge erfolgen. Einer der Anbieter bezeichnet die Erstellung eines Sicherheitskonzepts als »*verhandelbar*«.

Die Rechenzentren zumindest eines der beiden befragten Anbieter sind ISO 27001 und SAS 70 Type II zertifiziert. Wie allerdings in Kapitel III.2 (vgl. insbesondere auch Abschnitt III.2.1) dargestellt wurde, ist durch das BSI während der Durchführung von Outsourcing-Vorhaben und der Erstellung von Sicherheits- und Notfallkonzepten dennoch eine enge Zusammenarbeit mit dem Auftraggeber (d. h. der Behörde) gefordert. Entsprechende etablierte Vorgehensweisen sind aus den Antworten beider Anbieter nicht herleitbar.

Die Protokollierung von Vorgängen, die sich auf kundenspezifische bzw. durch den Kunden genutzte Dienste beziehen, ist dem Umfang nach durchaus geeignet, um datenschutzrechtlichen Anforderungen zu genügen (wobei hier natürlich nicht die Bewertung der entsprechenden Zertifizierungsstellen bzw. des BSI vorweggenommen werden soll). Allerdings sieht der Grundschutzbaustein »Datenschutz« (vgl. Kapitel III.3) auch umfassende Protokollierungen auf Systemebene vor, deren Verfügbarkeit ebenfalls fraglich ist.

III.5.7 Selbsteinschätzung: Eignung als Dienstleister für den öffentlichen Sektor

Beide Anbieter verweisen auf ihre langjähriger Erfahrung im Betrieb von Cloud-Diensten und attestieren ihre Kompetenz und Kapazität, um die rechtlichen Anforderungen für die Cloud-Umsetzung von Behördenlösungen zu erkennen und auszugestalten. Dies kann allerdings nicht in Form einer Rechtsberatung für Kunden erfolgen. Lösungen werden auf Basis der von den Kunden in Ausschreibungen niedergelegten Anforderungen erstellt.

Teil IV

Empfehlungen zur Migration in die Cloud

KAPITEL IV.1

Bedingungsrahmen für Cloud-Migrationen

Zusammenfassung

In diesem Kapitel werden drei wesentliche Bedingungen für die Inanspruchnahme von Cloud-Angeboten erarbeitet, nämlich:

- *Die Verfügbarkeit standardisierter und bereits an anderer Stelle auf Rechtssicherheit überprüfter SLA-Konstrukte für Cloud-Migrationen stellt in erster Linie eine Entlastung von Entscheidern in einzelnen Behörden dar, die den »Sonderfall« Cloud-Migration in gängige Praxis verwandeln können.*
- *Spezielles verfahrensrechtliche Regelungen und Richtlinien für Cloud-Computing als positive gesetzgeberischere Spezifikationen für die IT-technischen Auslagerung, die als konkreten Handlungsanweisungen für Entscheider vor allem Rechtssicherheit herstellen.*
- *(Externe) Anbieterzertifizierung und -aufsicht für Cloud-Anbieter, d. h. ein gesondertes Prüf-, Anerkennungs- und Aufsichtsverfahren, das an dieser Stelle insbesondere für öffentliche Cloud-Anbieter Gültigkeit hätte.*

Die ausführliche Risikendiskussion zum Cloud-Computing in Teil III dieser Studie verdeutlicht — insbesondere in ihrer Breite — die Entscheidungsprobleme, vor denen potentielle Nutzer von Cloud-Technologien stehen. Über die allgemeine Anforderung, überhaupt durch ein eigenes Risikomanagement bewertungs- und steuerungsfähig zu sein, müssen grundsätzliche Outsourcing- und Datenschutzrisiken abgesichert sein. Hinzu kommen spezielle technologische Cloud-Computing-Risiken aufgrund der virtuellen Ausgestaltung und anderer Cloud-spezifier Technologien. Schließlich ist über diese Anzahl konzeptioneller Risikokategorien auch die konkrete Auswahl eines Marktpartners bzw. die Vergabe der

Services mit eigenständigen Anbieterrisiken behaftet. Allerdings zeigt die Studie jeweils im Zusammenhang mit der Diskussion der einzelnen Risikoarten die zielführenden Risikostrategien bzw. risikominimierenden Ausgestaltungen auf. Damit wird nachgewiesen, dass bei einer Gesamtbetrachtung die Risiken von Cloud Migrationen mit einem entsprechenden Set von Entscheidungen und Ausgestaltungen gut beherrschbar sind.

Migrationsentscheidungen sind durch die explizite Prüfung aller rechtlichen Rahmenbedingungen zu rechtfertigen.

Unter den besonderen Entscheidungsbedingungen des öffentlichen Sektors stellt jedoch allein der gezeigte Umfang von Risiken und die Komplexität des Gesamtrisikos eine besondere Herausforderung dar. Denn speziell die weit über Datenschutzbestimmungen herausreichende Verrechtlichung bei Verwaltungsentscheidungen über Cloud-Migrationen erzwingt bei den Entscheidungsträgern eine jeweils explizite und im Ergebnis positive Prüfung aller rechtlichen Rahmenbestimmungen.

Cloud-Computing ist rechtlich nicht explizit berücksichtigt: Die Ausgestaltung von SLAs ist in der Praxis eine komplexe Aufgabe.

In der Praxis erfolgt dieses im Rahmen der Anbieter- und Partnerauswahl und mit — als einzigem Instrument — der Ausgestaltung der SLAs unter der Maßgabe, dass die kontrahierende Behörde auch durch geeignete Risikomanagemtstrukturen und -kapazitäten in der Lage ist, die SLA-Regelungen zu überwachen und für deren Nachhaltigkeit zu sorgen. Entsprechende Ausgestaltungen, Verhandlungen und Umsetzungen von SLAs sind dabei auch deshalb sehr aufwendig, weil der bestehende rechtliche Regelungsrahmen — z. B. im Verwaltungsverfahrensrecht — Konstrukte wie »Shared Services« oder Cloud-Computing nicht speziell regelt, sondern der vorhandene rechtliche Rahmen regelmäßig generalisiert sowie üblicherweise auf traditionelle (nicht-arbeitsteilige) Verfahrensabläufe abgestellt ist.

Dilemma der Singularität: Bei jeder Cloud Migration stehen einzelne entstehen einzigartige umfassende Gestaltungs- und Risikobegrenzungsaufgaben.

Vergleichbar zu dem bereits an anderem Ort dargestellten »Dilemma der Singularität« bei der Ausgestaltung innovativer eGovernment-Lösungen (vgl. »Shared Service«-Problematik in Kapitel II.1 und dort genannte weiterführende Quellen), stehen Entscheider bei der Bewertung und Anbahnung von Cloud-Computing-Ansätzen vor der anspruchsvollen Aufgabe, zusätzlich zur fachlich-technologisch adäquaten Lösung eine rechtliche Ausgestaltung zu entwickeln, die der Risikosituation angemessen ist, die sich bei der Umsetzung ergibt. In realen Entscheidungssituation stellt diese Aufgabe eine außerordentliche Barriere dar. Nicht nur stellt jede singuläre außerordentliche Ausgestaltung von Aufgabenwahrnehmung ein Risiko per se dar. Auch das mehrdimensionale und damit nur schwer überschaubare Ausgestaltungsproblem und dessen Umsetzung in SLA's ist eine zusätzliche Arbeitsaufgabe und Belastung für die Entscheidungsträger.

Sofern das beschriebene Dilemma fortbesteht und für jeden einzelnen Anwendungsfall einer Cloud-Migration die Entscheidungsträger einzelner Behörde vor umfassende Gestaltungs- und Risikobegrenzungsaufgaben gestellt werden, dürften die Potentiale für breitere Cloud-Computing-Migrationen im öffentlichen Sektor faktisch begrenzt und weitgehend ungenutzt bleiben. Insoweit erscheint es geboten durch Verbesserung der Rahmenbedingungen eine Governance zu schaffen, innerhalb derer Administrationen unterstützt werden, Cloud-Migrationen zu bewilligen und umzusetzen.

Dafür erscheinen aus heutiger Sicht vor allem drei Wege zielführend zu sein:

IV.1.1 SLA-Standards

Standardvorlagen zur vereinfachten Vertragsgestaltung erlauben Anbietern eine adäquate Angebotsformulierung.

Die Verfügbarkeit standardisierter und bereits an anderer Stelle auf Rechtssicherheit überprüfter SLA-Konstrukte für Cloud-Migrationen stellen in erster Linie eine Entlastung der Entscheidungsträger in einzelnen Behörden dar. Abhängig von der Instanz, die entsprechende Standards formuliert und/oder aus vorliegenden Anwendungserfahrungen entwickelt und vorlegt, können Entscheider auf die Vollständigkeit und die Problemadäquanz entsprechender SLA-Detailregelungen vertrauen. Bei einer breiteren Verwendung entsprechender Standardausgestaltungen ist einer über eine Mehrzahl von Behörden angewandten »üblichen« Praxis zu vertrauen. Insoweit können auch die in vorliegender Studie herausgearbeiteten Anwendungsspezifika und speziell die zu berücksichtigenden Risiken als Items für die Formulierung entsprechender Standardvorlagen zu Cloud-Migrationen verstanden werden. Nicht zuletzt wird durch diese Standards auch privatwirtschaftlichen Cloud-Anbietern ein Mittel in die Hand gelegt, Angebote zielgerichteter zu formulieren und sich damit als Partner für eine Zusammenarbeit mit öffentlichen Institutionen zu qualifizieren.

IV.1.2 Spezielles Verfahrensrecht und -richtlinien für Cloud-Computing

Gegebenenfalls in einem weiteren Entwicklungsschritt zur Herausarbeitung von Standard-SLAs zu Cloud-Migrationen ist eine noch gefestigtere Herstellung von Rechtssicherheit durch spezielle, gesetzliche Rahmenregelungen vorstellbar. Im Rahmen der durch den IT-Planungsrat in der Bundesrepublik abgedeckten Ordnungsbereich ist es insoweit denkbar, eine positive gesetzgeberischere Spezifikation der IT-technischen Auslagerung nicht nur von Daten, sondern auch von Infrastrukturen und Diensten auszugestalten. Entsprechende Rahmenregelungen hätten den Vorteil, durch Angabe von konkreten Handlungsanweisungen für Entscheidungsträger vor allem Rechtssicherheit herzustellen.

IV.1.3 Externe Anbieterzertifizierung und -aufsicht

Spezielles Prüf-, Anerkennungs- und Aufsichtsverfahren für Cloud-Anbieter.

Ergänzend zur Anwendung von Standard-SLAs oder speziellen verfahrensrechtlichen Regelungen — oder ggf. in solchen verfahrensrechtlichen Rahmen mit enthalten — ist aus heutiger Sicht vorstellbar, dass aus dem öffentlichen Sektor heraus (und hier ggf. durch auf eGovernment- und e-Risiken spezialisierte Institutionen wie z. B. dem BSI) für Cloud-Anbieter ein gesondertes Prüf-, Anerkennungs- und Aufsichtsverfahren entwickelt wird, welches die besonderen rechtlichen Anforderungen (und die Risikoüberwachung) aus den einzelnen Verträgen herauszulösen und an dritte Stellen zu übertragen zum Gegenstand hat. Dieses wäre ein zielführender Ansatz einer Arbeitsteilung, die die Potentiale von Cloud-Migrationen über eine große Anzahl von Anwendungsfällen unterstützen und befördern könnte.

KAPITEL IV.2

Ausgestaltungsszenarien

Zusammenfassung

In diesem Kapitel soll abschließend präzisiert werden, wie Clouds im Einzelnen für Verwaltungen nutzbar werden können, und wo die Probleme bei der Umsetzung derartiger Ausgestaltungsvarianten liegen. Wir betrachten zunächst private Clouds, die sich unmittelbar als Umsetzungsszenario anbieten. Community-Clouds sind — aufgrund der im Teil III dargestellten Probleme — nicht unmittelbar verwendbar, wobei allerdings die zu erwartenden Konsolidierungseffekte und Kompetenzbündellungen, die dien Sicherheit und Beherrschbarkeit solcher Strukturen erhöhen, einen unmittelbaren Anreiz zur Umsetzung solcher Modelle bilden. Wir betrachten hier insbesondere zwei Modellierungsansätze, nämlich einerseits einen übergreifenden Ansatz, der auf der gemeinschaftlichen Erbringung von Dienstleistungen durch die beteiligten Rechenzentren beruht, und einen Kompetenz-basierten Ansatz, in dem Community-Clouds als Zusammenschluß von Kompetenzzentren aufgefasst werden.

Schließlich betrachten wir auch die Einbeziehung von öffentlichen Cloud-Anbietern bzw. hybride Ausgestaltungsmodelle mit öffentlichem Cloud-Anteil. Wenn datenschutzrechtliche Fragestellungen unberührt bleiben, stellen solche Modelle u. U. einen gangbaren Weg zur Umsetzung öffentlicher-privater Partnerschaften dar.

IV.2.1 Private Clouds

Unter den heutigen Bedingungen, die in den Kapiteln III.2, III.3 und III.4 unter den Blickwinkeln Outsourcing, Datenschutz und Sicherheits-Mindestanforderungen dargestellt wurden, kommt für die öffentliche

Verwaltung in einer ersten Stufe nur die private Cloud als Nutzungsszenario in Betracht.[1] Die meisten Landes- und kommunalen Rechenzentren agieren schon heute als »Shared Service Center« und bieten ihren Kunden, den Verwaltungen, Dienstleistungen aus einer Hand an. Allerdings sind diese Dienstleistungen auf die regionalen und kundenspezifischen Bedürfnisse ausgerichtet.

Dienstorientierte Archtiekturen und Virtualisierung als Schritte in Richtung privater Clouds.

Diese Rechenzentren haben für ihre Kunden, die Verwaltungen, in der Regel schon Virtualisierung vorgenommen, d. h. ihre Infrastruktur konsolidiert, und wenn möglich, auch spezifische Angebote von Dienstleistungen bereitgestellt, die auf SOA-Prinzipien beruhen. SOA-basierte Dienste stellen einen ersten Schritt in Richtung einer Konsolidierung von eGovernment-Prozessen und einer Harmonisierung fachspezifischer IT-Verfahren dar. Vereinheitlichte Dienstmanagement-Ansätze, die auf SOA-Infrastrukturen aufsetzen, erlauben die vereinheitlichte und nachprüfbare Berücksichtigung von Sicherheits- und Datenschuztanforderungen und sind, anders als heterogene Managementansätze, leichter ISO- bzw. BSI-zertifizierbar.

Die sogenannten »Shared Service Center« haben somit bereits einen Teil des Weges zu einem Cloud-Provider für den öffentlichen Sektor zurückgelegt. Ansätze in Richtung der drei Cloud-Arten (Infrastruktur, Plattform und Dienste) sind erkennbar:

Infrastruktur als Dienst, allerdings ohne elastische Skalierbarkeit.

- Infrastrukturen werden auf Anforderung bereitgestellt, d. h. Kunden bekommen Ressourcen wie Speicher und Server transparent als Dienste zur Verfügung gestellt. Bisher ist dies allerdings nur eingeschränkt möglich: die Ressourcen sind begrenzt. Dynamische Erweiterungen können bei Bedarf nicht automatisiert vorgenommen werden — es müssen Kapazitäten für den Mehrverbrauch bei Höchstlast vorgehalten und gegenüber dem Kunden abgerechnet werden.[2]

PaaS z. B. für Geodaten.

- PaaS wird beispielsweise von einigen Dienstleistungszentren für IT-Fachverfahren aus dem Bereich der Geodaten angeboten und genutzt. Kunden, in diesem Fall Vermessungsämter und Behörden für Stadtentwicklung, können eine gemeinsame Plattform für die Entwicklung von speziellen Diensten nutzen. Auch halten viele Dienstleistungszentren Verzeichnisdienste vor, die dezentrale Datenhoheit berücksichtigt und insbesondere Ausfallsicherheit gewährleistet.

SaaS: »Thin clients« und Fachverfahren.

- SaaS ist ebenfalls vertreten. Hierbei handelt es sich u. a. um Arbeitsplätze und Fachverfahren. Z. B. beziehen Kunden durch Virtualisierung von Arbeitsplätzen, d. h. dem Einsatz von sog. »*Thin Cients*«, ihre gesamte Arbeitsumgebung aus der Infrastruktur des IT-Dienstleisters. Dadurch werden Fachverfahren zentralisiert zur

[1] Diese Einschätzung wird von den Verantwortlichen vieler Dienstleister der öffentlichen Hand geteilt, vgl. (Harnisch, 2010).

[2] Ein Beispiel für einen IaaS-Anbieter im öffentlichen Sektor ist das IT-Systemhaus der Bundesagentur für Arbeit, vgl. (Deeg, 2010).

Verfügung gestellt. Die Dienste werden netzwerkbasiert zur Verfügung gestellt und können bedarfsgerecht abgewickelt werden.[3]

Die Vorteile solcher Ansätze sind u. a.:

- Konstenreduzierung durch Virtualisierung und dynamische Ressourcenallokation, sowie hohe Verfügbarkeit
- Konsolidiertes Dienstmanagement etwa nach ITIL (Cartlidge u. a., 2007)
- Einhaltung von Sicherheitsgrundsätzen, die sich aus gesetzlichen Regelungen zur Datensicherheit und zum Datenschutz ergeben; darüber hinaus können Sicherheitsrichtlinien einfacher durchgesetzt und auf dem neusten Stand gehalten werden
- Energieeinsparungen, d. h. wirtschaftlicher und ökologischer Betrieb[4]

IV.2.2 Community-Clouds

Zur Zeit[5] existieren in Deutschland mehr als 1400 unabhängige Rechenzentren. Die bloße Verwendung von Cloud-Technologien im Sinne privater, durch diese Rechenzentren betriebener Clouds würde dementsprechend nur einen geringen Konsolidierungseffekt mit sich bringen. Rechenzentrumsübergreifende Konsolidierungen sind allerdings aus verschiedenen Gründen notwendig:

Treiber für IT-Kooperationen.

- Demographischer Wandel: Im kommunalen Bereich ist davon auszugehen, dass sich in den nächsten 10 Jahren die Anzahl qualifizierter Mitarbeiter halbieren wird.
- Mittelfristige Prognosen zur Entwicklung der kommunalen Haushaltsdefizite ergeben, dass bis zum Jahr 2014 mit einem Defizit von insgesamt 60 Mrd. € zu rechnen ist.[6]

Hemmnisse bei der Umsetzung von IT-Kooperationen.

Demgegenüber stehen eine Reihe von Argumenten, die einer rechenzentrumsübergreifenden Kooperation widersprechen: Fachverfahren, insbesondere auf kommunaler Ebene, sind häufig sehr spezifisch auf die konkreten Bedürfnisse der einzelnen Landkreise und Bezirke angepasst. Softwarelösungen werden proprietär für sehr spezifische Aufgaben erstellt. Die Verwendung standardisierter Verfahren ist nicht ohne weiteres möglich.

Im Einzelnen sind aber die folgenden Fragestellungen zu beachten:

Konfigurierbarkeit anstelle von maßgeschneiderter Software.

- Ist die Verwendung spezifischer Verfahren wirklich notwendig oder

[3] Der norddeutsche IT-Dienstleister Dataport stellt u. a. Fachverfahren zur Finanzbuchhaltung für verschiedene Bundesländer und Kommunen zur Verfügung.

[4] Vgl. (Keusekotten, 2010).

[5] Stand: November 2010

[6] Innenministerium des Landes Nordrhein-Westfalen, Bezirksregierung Detmold, Deutscher Landkreistag, zitiert nach (Harnisch, 2010).

kann — bei entsprechender Konfigurierbarkeit (vorgenommen entweder durch die Behörde oder den IT-Dienstleister) der mandantenfähigen Software — das entsprechende Verfahren durch eine »generische« Standardlösung ebenso abgebildet werden?[7] Insbesondere die Anwendung dienstorientierter Architekturprinzipien, die die Umsetzung von Dienstkonfigurationen auf der Basis allgemeiner Bausteine erlauben, müssen hier als Alternativen untersucht werden.

Identifikation generischer Anteile.

- Selbst wenn einzelne Fachverfahren nur durch Speziallösungen auf der Dienstebene unterstützt werden können, bleiben immerhin noch eine Reihe generischer Anteile wie etwa Datenbanken, Infrastruktur, Kommunikation, Web-basierte Oberflächengestaltung oder Dienstmanagement-Werkzeuge, die durch einen Cloud-Anbieter zur Verfügung gestellt werden können. Hier ist es allerdings notwendig, dass traditionelle monolithische Silo-Anwendungen aufgebrochen und in flexiblere Architekturen überführt werden.

Der Vorschlag, IT-Dienstleistungen von »fremden« Rechenzentren in Anspruch zu nehmen, wird von vielen Verwaltungen sowohl auf kommunaler wie auch auf Länderebene mit Misstrauen betrachtet. Schließlich funktionieren die eigenen Lösungen; Kompetenzen und spezielle Verfahren sowie eingefahrene (nicht notwendigerweise dokumentierte) Prozesse, die aus langjähriger Erfahrung der Systemadministratoren erwachsen sind, garantieren einen reibungslosen Betrieb.

Insbesondere die Überlegungen zum demographischen Wandel lassen dieses Argument aber fragwürdig erscheinen. Salopp ausgedrückt: Wenn die alte Garde in Rente geht, wer blickt dann noch durch?

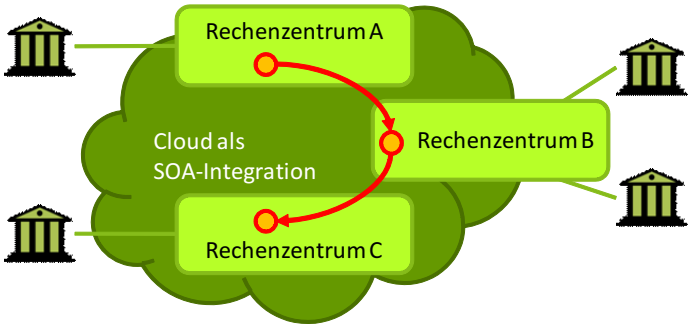
Das Community-Cloud-Betriebsmodell weist, wie in den Kapiteln III.3 – III.4 dargestellt, einige Schwierigkeiten als Dienstleistungsansatz für die öffentliche Verwaltung auf. Es muss jedoch darauf hingewiesen werden, dass sich diese Probleme im Wesentlichen auf die Verfügbarkeit föderierter System- und Dienstmanagement-Ansätze reduzieren lassen, die zumindest durch Cloud-Computing-Technologien (automatisierte Ressourcenallokation, integriertes Monitoring usw.) unterstützt werden. Andererseits bestehen diese Probleme ebenso für Konsolidierungsansätzte, die nicht auf Cloud-Technologien zurückgreifen. Wie stellen deshalb die These auf, *dass System- und Dienstmanagement in föderierten Infrastrukturen, die aus einer rechenzentrumsübergreifenden Ressourcenkonsolidierung entstehen, durch Cloud-Technologien besser umgesetzt werden können*.

These: Cloud-Technologien erlauben verbessertes System- und Dienstmanagement.

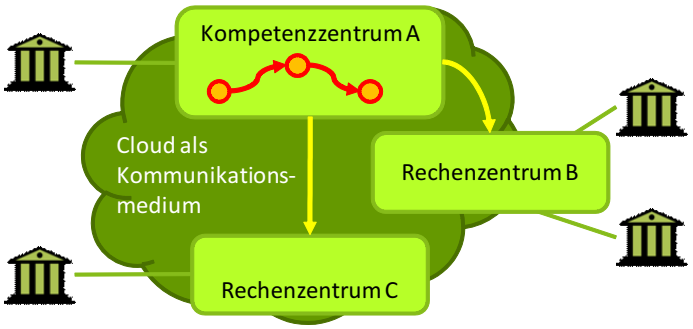
Eine Verwaltungsprozessoptimierung und die Identifikation und Definition standardisierter Kernprozesse würde eine grenzenübergreifende, interkommunale Zusammenarbeit stärken und Möglichkeiten schaffen, Fachverfahren anzubieten, die nicht nur über kommunale, sondern auch Landesgrenzen hinaus genutzt werden können. Der IT-Planungsrat als Steuerungs- und Governance-Stelle könnte die notwendigen gesetzlichen Rahmenbedingungen für die öffentliche Dienstleistung vorantreiben.

Rolle des IT-Planungsrats.

[7] Der norddeutsche IT-Dienstleister Dataport stellt z. B. einen »Master« für ERP-Anwendung für verschiedene Landesbetriebe zur Verfügung.



IV.2.1 (a): Übergreifender Ansatz.



IV.2.1 (b): Kompetenzbasierter Ansatz.

Abbildung IV.2.1
Community-Cloud-basierte Modelle zur rechenzentrumsübergreifenden Kooperation.

Wie können Gestaltungsszenarien für den Einsatz von Community-Clouds für die Verwaltung im Einzelnen aussehen? Im Wesentliche ergeben sich zwei Exteme, nämlich der **übergreifende Ansatz** und der **kompentenzbasierte Ansatz**.

IV.2.2.1 Übergreifende Kooperationen

Gemeinschaftliche Erbringung von Dienstleistungen durch rechenzentrumsübergreifende Kooperation.

In diesem Ausgestaltungsszenario werden Dienstleistungen gemeinschaftlich durch verschiedene Rechenzentren unter Verwendung einer Cloud-Infrastruktur als verbindendes Medium erbracht (Abb. IV.2.1). Funktionale Teilaspekte dieser Dienste werden u. U. von verschiedenen Rechenzentren betrieben und unter Zugrundelegung einer dienstorientierten Architektur integriert. Tatsächlich bieten viele Dienstleistungszentren bereits heute unterstützende Dienste an, die als Komponenten für eine solche übergreifende Kooperation dienen können, z. B.

- Datensicherung und Datenwiederherstellung
- Notfallmanagement
- Systemmanagement und zentrale Monitoringtools

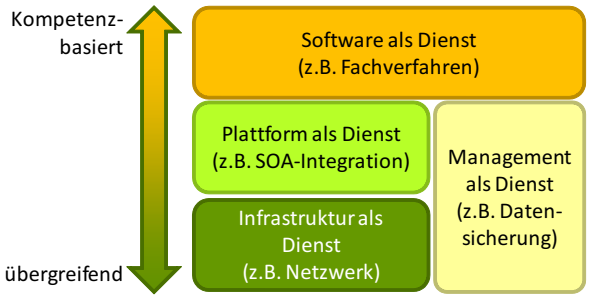


Abbildung IV.2.2
Beziehung der Kooperationsmodelle zur Art der Cloud-Dienstleistung.

IV.2.2.2 Kompetenzbasierte Kooperation

Rechenzentren treten als Kompetenzzentren für spezifische Anwendungen auf.

Während der übergreifende Kooperationsansatz auf der Idee der vollständigen Integration der beteiligten Rechenzentren in einer übergreifenden Cloud basiert, kann ein alternatives Modell darin bestehen, Rechenzentren als Kompetenzzentren zu verstehen, die verschiedene Dienstleistungen, z. B. Unterstützung für Fachverfahren, eigenständig betreiben und unter Zuhilfenahme der Cloud, die hier als Kommunikationselement verwendet wird, zur Verfügung stellen (Abb. IV.2.1).

In beiden Modellen treten einzelne Rechenzentren als Dienstleister gegenüber den beauftragenden Behörden auf. Keinesfalls sollten diese Modelle so verstanden werden, dass Behörden direkten Zugriff auf die technischen Systeme der Cloud erlangen.

Anwendung der kooperativen Ausgestaltungsszenarien.

Offenbar ist die Trennlinie zwischen beiden Modellen fließend: Kompetenzbasierte Koopertionen für Fachverfahren kann auf eine integrierte Kooperation für Dienstintegration, Speicher, Server und Kommunikationsinfrastruktur zurückgreifen. Kompetenzbasierte Kooperationen haben den Vorteil, das spezifische Lösungen, die detailiertes Domänenwissen erfordern, durch ein konsolidiertes Expertenteam unter Verwendung dedizierter Werkzeuge und Prozesse erbracht werden können. Übergreifende Kooperationen bieten sich hingegen für generische, ressourcenintensive Aufgaben wie die Erbringung von Rechenressourcen (in einer virtualisierten Umgebung), Kommunikation, aber auch allgemeine Aufgaben, die dem Dienstmanagement zuzurechnen sind (Fehler-, Ereignis- und Sicherheitsmanagement, Konfigurationsmanagement, Datensicherung und -wiederherstellung usw.) an. Abb. IV.2.2 setzt die beiden Modelle in Beziehung zu den verschiedenen Arten der Cloud-Dienstleistungen. »Management als Dienst« steht hier für Dienste, die unterstützend zum Dienst- und Systemmanagement verwendet werden.

Vorteile kooperativer Ausgestaltungen.

Unabhängig davon, welches Modell im konkreten Fall gewählt wird, ergeben sich die folgenden Vorteile:

- Dynamische Skalierung unter optimierter Nutzung der physikalischen Ressourcen der beteiligten Rechenzentren
- Übergreifende, föderierte Management-Prozesse, d. h. hohe, validierbare Dienstqualität

- Harmonisierung von fachspezifischen Verfahren (allerdings werden hier Standards benötigt, die heute nicht oder nur teilweise verfügbar und implementiert sind)
- Abmilderung der sich aus dem demographischen Wandel ergebenden Personal- und Kompetenzprobleme

Abschließend ist noch darauf hinzuweisen, dass Kooperationsbereitschaft auf allen Ebenen vorhanden ist (vgl. Abschnitt I.2.3). Allerdings ist noch zu untersuchen, inwieweit der gesetzliche Rahmen derartige Kooperationsmodelle zuläßt bzw. ob entsprechende Anpassungen vorgenommen werden können — Fragestellungen, die in dieser Studie nicht umfassend behandelt werden können. Dem IT-Planungsrat fällt hierbei die Rolle des Koordinators und Motors solcher Entwicklungen zu.

IV.2.3 Öffentliche Clouds und hybride Modelle

Eine öffentlich-private Zusammenarbeit basierend auf öffentlichen Cloud-Modellen sind, wie die Analyse in den Kapitels III.3 – III.4 zeigt, momentan für die Verwaltungen in der vorhandenen Form nicht realisierbar. Die wesentlichen Probleme sind:

Probleme bei der Beauftragung öffentlicher Clouds.

- Datenschutz
- Mangelnde Transparenz
- Fehlende Kontrollmechanismen

Option: Auslagerung öffentlicher Daten in öffentliche Clouds.

Andererseits besteht seitens privatwirtschaftlicher Anbieter ein großes Potential an Ressourcen, Dienstleistungen und Know-How, das die öffentlichen Verwaltungen nicht ungenutzt lassen sollten. Eine Möglichkeit, die anhand konkreter Szenarien und Projekte näher untersucht werden sollte, ist die Auslagerung öffentlicher Daten in öffentliche Clouds.[8] Der öffentliche Sektor ist einer der größten Produzenten von Informationen in Form öffentlicher Daten wie etwa Verkehrsinformationen, Wetterdaten, Wirtschaftsdaten, Finanzdaten oder digitale Karten. Nach EU-Recht/-Dienstleistungsrichtlinie[9] müssen diese Daten öffentlich zugänglich sein.

Der eSafe.

Perspektivisch für die sichere Ablage von Daten und Dokumenten für Bürger kann der elektronische Safe (Breitenstrom u. a., 2008), der am Fraunhofer Institut für offene Kommuikationssystem (FOKUS) entwickelt wurde, als sicherer Ort in einer Cloud gesehen werden. Der »eSafe« ist ein sicherer Container, der es Bürgern nicht nur erlaubt, elektronische Dokumente in der Cloud abzulegen, sondern auch die elektronische Abwicklung von Online-Diensten mit Behörden ermöglicht. Der Bürger als Eigentümer der Dokumente hat die alleinige Kontrolle über den eSafe und kann Behörden und Unternehmen dedizierten Zugriff auf spezielle Dokumente erlauben. Daten und Dokumente werden verschlüsselt und

[8] Vgl. (Schieferdecker u. a., 2010)

[9] PSI Directive, vgl. http://ec.europa.eu /information_society /policy /psi /actions_eu /policy_actions /index_en.htm

zudem fragmentiert und verteilt gespeichert. Damit besteht die Aussicht, dass das Verfahren datenschutzrechtlich konform ist.

Anforderungen an öffentliche Clouds.

Nichtsdestoweniger haben privatwirtschaftliche Anbieter einige Anforderungen zu erfüllen, um als geeignete Partner für eine öffentlich-private Zusammenarbeit in Frage zu kommen:

- Mechanismen müssen vorhanden sein, die externe IT-Audits und andere Kontrollen durch den Auftraggeber ermöglichen. Insbesondere ist hier auf die weitreichenden Protokollierungs- und Zusammenarbeitsanforderungen hinzuweisen, die durch die BSI-Grundschutzkataloge gefordert werden.
- Portabilität zwischen verschiedenen Clouds muss gewährleistet sein, um »*lock-in*«-Situationen zu vermeiden. Dies bedeutet insbesondere, dass eine Fortsetzung des Betriebs im Falle einer Insolvenz des Cloud-Anbieters sichergestellt sein muss.
- Ein transparentes, standardkonformes Dienst- und Systemmanagement muss gewährleistet und nachweisbar sein.
- Transparenz bezüglich der Standorte ist ebenso notwendig wie die Offenlegung von Subunternehmern und den entsprechenden vertraglichen Gegebenheiten.
- Identitäts- und Rechtemanagement, Sicherheitsmanagement nach BSI, offene Standards der Cloud-Service-Schnittstellen.

KAPITEL IV.3

Zusammenfassung und weiterführende Arbeiten

Zusammenfassend lässt sich feststellen, dass Cloud-Technologien bereits heute für Rechenzentren und Dienstleister ein Potential zur Ressourcen- und Kompetenz-Konsolidierung bedeuten. Aus der rechtlich/organisatorischen Perspektive bestehen hier insbesondere Defizite in den Bereichen SLA-Standards und Verfahrensrecht. Weiterhin sind insbesondere Ansätze zur Zertifizierung und zur Anbieteraufsicht zu konkretisieren.

Ausgestaltungsszenarien beinhalten private Clouds als technologische Weiterentwicklung oder Erneuerung der behördeninternen Rechenzentren und externen Dienstleister. Als mittelfristiges Zielszenario ist der Zusammenschluss verschiedener Dienstleister zu Commutiy-Clouds (mit verschiedenen Teilmodellen) von besonderem Interesse. Öffentliche Clouds bzw. hybride Modelle in Form als Grundlage einer öffentlich-privaten Kooperation können ebenfalls in Betracht gezogen werden, wenn es um Daten geht, die außerhalb des Datenschutzrechts liegen, und privatwirtschaftliche Cloud-Anbieter eine Reihe von Bedingungen erfüllen, die sie als grundsätzliche Partner für eine solche Kooperation qualifizieren.

Schwerpunktthemen für weiterführende Forschung.

Im Einzelnen lassen sich eine Reihe von Schwerpunktthemen identifizieren, die als Orientierungspunkte für zukünftige Arbeiten gelten können:

ITIL für die Cloud?

- **Dienstmanagement** für die Cloud, z. B. nach ITIL, ist zur Zeit nicht ausreichend betrachtet. Die Notwendigkeit, interne Geschäfts- und Verwaltungsprozesse für dem Kunden transparent, validierbar, und in bestimmten Umfang beeinflussbar zu machen, lässt dies als besonderes Defizit heutiger Cloud-ComputingAnsätze erscheinen.

Wie können föderierte Cloud-Modelle effektiv umgesetzt werden?

- **Cloud-Interoperabilität** ist eine Grundbedingung für die Bildung föderierter Infrastrukturen. Interoperabilität lässt sich auf verschiedenen Ebenen betrachten, z. B. in Bezug auf Daten, Prozesse und Technologie (d. h. Protokolle bzw. Schnittstellen).

Open Data Clouds als Option für ÖPP.

- **Open Data Clouds** und ihre Integration in hybride Cloud-Infrastrukturen stellt die zur Zeit aussichtsreichste Form einer öffentlich-privaten Partnerschaft im Bereich Cloud-Computing dar.

Standardisierung.

- Die Notwendigkeit, **Standardisierung** im Cloud-Bereich voranzutreiben, ist längst erkannt worden. So gut wie jedes Standardisierungsgremium im IT-Sektor unterhält mittlerweile eine Arbeitsgruppe, die relevante Aspekte untersucht. Allein im Bereich Interoperabilität lassen sich eine Vielzahl von Aktivitäten verzeichnen:
  - DIN (NIA-01-38) bzw. ISO (JTC 1/SC 38)
  - Distributed Management Task Force: Open Cloud Standards Incubator[1]
  - ETSI STF on ICT GRID Technologies Interoperability and Standardization[2]
  - NIST Cloud Computing Project[3]
  - Global Inter-Cloud Technology Forum[4]
  - Cloud Computing Use Cases Group[5]
  - Open Cloud Consortium[6]
  - OMG - Cloud Standards Coordination[7]
  - Cloud Security Alliance[8]

  Darüber hinaus hat das BSI mit dem in Kapitel III.4 diskutierten Papier einen ersten Schritt in Richtung einer Richtlinie zur Sicherheitszertifizierung von Cloud-Anbietern getan, der jedoch weiterer Konkretisierung bedarf.

Zertifizierung.

- Eine **Sicherheitszertifizierung** von Cloud-Anbietern — im Sinne der genannten und fortlaufenden andauernden BSI-Arbeiten — wäre ein besonders zu begrüßender Schritt, um die Risikoposition von Cloud Computing-Anwendungspartnern und Auftraggebern im Bereich der öffentlichen Verwaltung auf ein akzeptables Maß zu begrenzen. Damit könnte anwendungsübergreifende Risikokriterien breit abgedeckt werden. Dies ist nicht nur für die Be-

[1] http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf

[2] http://portal.etsi.org/STFs/STF_HomePages/STF331/STF331.asp

[3] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[4] http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf

[5] http://groups.google.com/group/cloud-computing-use-cases

[6] http://opencloudconsortium.org/testbed

[7] http://www.omg.org/news/meetings/GOV-WS/css/css-pdf/OMG.pdf

[8] http://www.cloudsecurityalliance.org/csaguide.pdf

hörden im Rahmen ihres IT-Risikomanagements besonders wichtig. Auch für die Anbieter von Cloud Computing-Diensten hätte eine solche Zertifizierung den großen Vorteil, in hinreichender Transparenz die sicherheitsbezogenen Anforderungen der öffentlichen Verwaltung am Cloud-Computing zu kennen und in ihre Produktgestaltungen einfließen zu lassen. Dies schließt allgemeine verfahrensbezogene und -rechtliche Ausgestaltungen ein. In diesem Sinne ließe sich das heute bestehende und als Barriere für Cloud-Migrationen einzuordnende Regelungsdefizit baukastenartig zweiteilen in einen solchen allgemeinen Sicherheitsrahmen — der durch eine Sicherheitszertifizierung abdeckt wird — und durch Muster- bzw. Standard-SLAs, die die dann noch gegebenen und anwendungsbezogenen Risiko-Barrieren durch entsprechende bilaterale Vereinbarungen der Cloud-Computing-Partner regeln.

Teil V

Anhänge

ANHANG A

Meinungsspiegel: Was ist Cloud-Computing?

Die folgende Liste von Cloud-»Definition« wurde aus verschiedenen Online-Quellen zusammengetragen — ein Anspruch auf Vollständigkeit besteht allerdings nicht. Diese Meinungen wurden bzgl. ihrer Kompatibilität mit der Definition des NIST[1] (vgl. Kapitel I.1) bzw. abgeleiteten Eigenschaften (vgl. Abschnitt I.1.6) analysiert.

1. **Markus Klems, Karlsruhe Institute of Technology**:

   Elastizität, messbare Dienstqualität

   What is cloud computing all about? Amazon has coined the word «elasticity» which gives a good idea about the key features: you can scale your infrastructure on demand within minutes or even seconds, instead of days or weeks, thereby avoiding under-utilization (idle servers) and over-utilization (blue screen) of in-house resources. With monitoring and increasing automation of resource provisioning we might one day wake up in a world where we don't have to care about scaling our Web applications because they can do it alone.[2]

2. **Reuven Cohen, Enomaly Inc.**:

   Netzwerkzugang, Mandantenfähigkeit, Elastizität

   For me the simplest explanation for cloud computing is describing it as, «internet centric software». This new cloud computing software model is a shift from the traditional single tenant approach to software development to that of a scalable, multi-tenant, multi-platform, multi-network, and global. This could be as simple as your web based email service or as complex as a globally distributed load balanced content delivery environment. I think drawing a distinction on whether its, PaaS, SaaS, HaaS is completely secondary, ultimately all these approaches are attempting to solve the same problems (scale). As software transitions from a traditional desktop deployment model to that of a network & data centric one, «the cloud» will

[1] (Mell u. Grance, 2009)

[2] http://markusklems.wordpress.com/2008/07/07/wow-is-a-cloud/

be the key way in which you develop, deploy and manage applications in this new computing paradigm.[3]

Bedarfsgerechte Abrechnung, Netzwerkzugang

3. **Jeff Kaplan, THINK IT Services, Cisco**:

   I view cloud computing as a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a ‹pay-as-you-go› basis that previously required tremendous hardware/software investments and professional skills to acquire. Cloud computing is the realization of the earlier ideals of utility computing without the technical complexities or complicated deployment worries.[4]

Ressourcen-Pooling (Virtualisierung)

4. **Douglas Gourlay**:

   People are coming to grips with Virtualization and how it reshapes IT, creates service and software based models, and in many ways changes a lot of the physical layer we are used to. Clouds will be the next transformation over the next several years, building off of the software models that virtualization enabled.[5]

Ressourcen-Pooling, Netzwerkzugang

5. **Praising Gaw, Fortiva**:

   The way I understand it, «cloud computing» refers to the bigger picture . . . basically the broad concept of using the internet to allow people to access technology-enabled services. According to Gartner[6], those services must be ‹massively scalable› to qualify as true ‹cloud computing›. So according to that definition, every time I log into Facebook, or search for flights online, I am taking advantage of cloud computing.[7]

Ressourcen-Pooling, SaaS, PaaS, IaaS

6. **Damon Edwards, dev2ops**:

   The «Cloud» concept is finally wrapping peoples' minds around what is possible when you leverage web-scale infrastructure (application and physical) in an on-demand way. «Managed Services», «ASP», «Grid Computing», «Software as a Service», «Platform as a Service», «Anything as a Service» . . . all terms that couldn't get it done. Call it a «Cloud» and everyone goes bonkers. Go figure.[8]

SaaS, PaaS

7. **Brian de Haaff, Paglo**:

   There sure is a lot of confusion when it comes to talking about cloud computing. Yet, it does not need to be so complicated. There really are only three types of services that are cloud based: SaaS, PaaS, and Cloud Computing Platforms. I am not sure being massively scalable is a requirement to fit into any one category.[9]

SaaS

8. **Ben Kepes**:

   SaaS is one consumer facing usage of cloud computing. While it's something of a semantic discussion it is important for people inside to have an

[3] http://www.elasticvapor.com/2008/06/describing-cloud.html

[4] http://www.thinkstrategies.com/blog/

[5] http://blogs.cisco.com/datacenter/comments/simon_crosby_on_gigaom/

[6] Gaw verweist hier auf die Definition des Gartner-Instituts, vgl. Def. 20

[7] http://cloudcomputing.sys-con.com/node/612033

[8] http://www.johnmwillis.com/cloud-computing/is-guitar-hero-a-cloud-the-cloud-wars/#comment-9506

[9] http://cloudcomputing.sys-con.com/node/612033#feedback

understanding of what it all means. Put simply cloud computing is the infrastructural paradigm shift that enables the ascension of SaaS.[10]

9. **Kirill Sheynkman**: *Ressourcen-Pooling, IaaS*

   The ‹cloud› model initially has focused on making the hardware layer consumable as on-demand compute and storage capacity. This is an important first step, but for companies to harness the power of the cloud, complete application infrastructure needs to be easily configured, deployed, dynamically-scaled and managed in these virtualized hardware environments.[11]

10. **Omar Sultan, Cisco**: *Selbstbedienung*

    In a fully implemented Data Center 3.0 environment, you can decide if an app is run locally [...], in someone else's data center [...] and you can change your mind on the fly in case you are short on data center resources [...], or you having environmental/facilities issues [...]. In fact, with automation, a lot of this can be done with policy and real-time triggers. For example, during month end processing, you might always shift non-critical apps offsite, or if you pass a certain cooling threshold, you might ship certain processing offsite.[12]

11. **Kevin Hartig, Sun Microsystems**: *Elastizität, Selbstbedienung*

    Cloud computing overlaps some of the concepts of distributed, grid and utility computing, however it does have its own meaning if contextually used correctly. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needs. An application or service developer requests access from the cloud rather than a specific endpoint or named resource. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlaid on top of the infrastructures tying them together. The cloud is a virtualization of resources that maintains and manages itself.[13]

12. **Jan Pritzker, CohesiveFT**: *Selbstbedienung*

    Clouds are vast resource pools with on-demand resource allocation. The degree of on-demandness can vary from phone calls to web forms to actual APIs that directly requisition servers. I *tend* to consider slow forms of requisitioning to be more like traditional datacenters, and the quicker ones to be more cloudy. A public facing API is a must for true clouds. Clouds are virtualized. On-demand requisitioning implies the ability to dynamically resize resource allocation or moving customers from one physical server to another transparently. This is all difficult or impossible without virtualization. Clouds tend to be priced like utilities (hourly, rather than per-resource), and I think we'll see this model catching on more and more as computing resources become as cheap and ubiquitous as water, electricity, and gas (well, maybe not gas). However, I think this is a trend, not a requirement. You can certainly have clouds that are priced like pizza, per slice.[14]

13. **Trevor Doerksen, MoboVivo**: *Ressoucen-Pooling*

[10] Zitiert nach http://cloudcomputing.sys-con.com/node/612375?page=0,1

[11] http://cloudcomputing.sys-con.com/node/612375?page=0,1

[12] http://cloudcomputing.sys-con.com/node/592855

[13] http://cloudcomputing.sys-con.com/node/579826

[14] http://virtualization.sys-con.com/node/595685, Hervorhebungen im Original.

Cloud computing is said to be the user-friendly version of grid computing. We know grid computing brought together the high performance computers, the middleware, and strategies to utilize hundreds and thousands of computers linked by advanced networks.[15]

Selbstbedienung, Netzwerkzugang

14. **Thorsten von Eicken, RightScale**:

    Most computer savvy folks actually have a pretty good idea of what the term «cloud computing» means: outsourced, pay-as-you-go, on-demand, somewhere in the Internet, etc.[16]

SaaS, PaaS, IaaS

15. **Michael Sheehan, GoGrid**:

    I would like to propose a ‹Cloud Pyramid› to help differentiate the various Cloud offerings out there. [At the top of the pyramind] users are truly restricted to only what the application is and can do. Some of the notable companies here are the public email providers (Gmail, Hotmail, Quicken Online, etc.). Almost any Software as a Service (SaaS) provider can be lumped into this group. As you move further down the pyramid, you gain increased flexibility and control but your a still fairly restricted to what you can and cannot do. Within this Category things get more complicated to achieve. Products and companies like Google App Engine, Heroku, Mosso, Engine Yard, Joyent or force.com (SalesForce platform) fall into this segment. At the bottom of the pyramid are the infrastructure providers like Amazon's EC2, GoGrid, RightScale and Linode. Companies providing infrastructure enable Cloud Platforms and Cloud Applications. Most companies within this segment operate their own infrastructure, allowing them to provide more features, services and control than others within the pyramid.[17]

Ressourcen-Pooling

16. **Irving Wladawsky Berger, IBM**:

    When virtualizing applications to be used by people who care nothing about computers or technology—as is mostly the case with Clouds—the key thing we want to virtualize or hide from the user is complexity. Most people want to deal with an application or a service, not software. . . . The more intelligent we want [computers and computer applications] to be—that is, intuitive, exhibiting common sense and not making us have to constantly take care of them—the more smart software it will take. But with cloud computing, our expectation is that all that software will be virtualized or hidden from us and taken care of by systems and/or professionals that are somewhere else—out there in The Cloud.[18]

Selbstbedienung, Netzwerkzugang

17. **Ben Kepes**:

    I view cloud computing as a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a ‹pay-as-you-go› basis that previously required tremendous hardware/software investments and professional skills to acquire. Cloud computing is the realization of the earlier ideals of utility computing without the technical complexities or complicated deployment worries.[19]

Selbstbedienung, Netzwerkzugang

18. **Bill Martin, Nonlinear Thinking**:

    Cloud computing really comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly

[15] http://cloudcomputing.sys-con.com/node/593313

[16] http://cloudcomputing.sys-con.com/node/581961

[17] http://cloudcomputing.sys-con.com/node/609938

[18] http://alwayson.goingon.com/permalink/post/28058

[19] http://diversity.net.nz/cloud-computing-and-saas/2008/07/16/

without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.[20]

19. **Tom Bittman, Gartner**: *Elastizität, Netzwerkzugang*

    Cloud Computing: A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies.[21]

20. **Frank Gens, IDC**: *Netzwerkzugang*

    When most people talk about «cloud computing», they usually refer to online delivery and consumption models for business and consumer services. These services include IT services—like software-as-a-service (SaaS) and storage or server capacity as a service—but also many, many «non-IT» business and consumer services. [...] And so, in our definitional framework, we distinguish between:

    - Cloud Services = Consumer and Business products, services and solutions that are delivered and consumed in real-time over the Internet.
    - Cloud Computing = an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services). *In short, a cloud service is virtually any business or consumer service that is delivered and consumed over the Internet in real-time*. [22]

21. **James Staten, Forrester/Jupiter Research**: *SaaS, PaaS, IaaS, Selbstbedienung, Netzwerkzugang*

    A standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way.[23]

22. **The 451 Group**: *SaaS, Ressourcen-Pooling*

    ‹Cloud computing› describes a service model that combines a general organizing principle for IT delivery, infrastructure components, an architectural approach and an economic model—basically, a confluence of grid computing, virtualization, utility computing, hosting and software as a service (SaaS). Or, put more simply, the cloud is IT, presented as a service to the user, delivered by virtualized resources that are independent of location.[24]

23. **Bruce Richardson, AMR Research**: *SaaS, Selbstbedienung*

    Cloud computing is the next-generation of software as a service, in which a complete software environment is licensed as a subscription from a software vendor and low-cost, secure, and dependable IT hardware infrastructure is ‹rented› from a utility-computing provider on demand. The customer has complete control over its own secure and private IT environment at a very low cost and without the hassle of procuring and managing its own data center. It can quickly scale IT resources up or down as computing needs

[20] http://nonlinearthinking.typepad.com/nonlinear_thinking/2008/08/cloud-computing-i-know-it-when-i-see-it.html

[21] http://www.gartner.com/it/summits/851712/str25_b2/index.html

[22] http://blogs.idc.com/ie/?p=190, Hervorhebung im Original

[23] http://blogs.forrester.com/it_infrastructure/2009/10/assessing-the-maturity-of-cloud-computing-services.html

[24] http://www.the451group.com/ice/ice_detail.php?icid=619

change. And [the customer] has complete freedom to customize the solution as it sees fit and complete control over upgrade cycles and all other aspects of its IT environment.[25]

Selbstbedienung

24. **Burton Group**:

    The set of disciplines, technologies, and business models used to render IT capabilities as on-demand services.[26]

Elastizität, Ressourcen-Pooling, Selbstbedienung

25. **Agatha Poon, Yankee Group**:

    In essence, we define cloud computing as «dynamically scalable, virtualized information services delivered on demand over the Internet with multitenant capability, service-level agreements (SLAs) and usage-based pricing.»[27]

Elastizität, Ressoucen-Pooling, Netzwerkzugang

26. **Mark Bowker, Enterprise Strategy Group**:

    ‹Cloud computing› is nothing more than a service model where business workloads are deployed, transparently executed internally or somewhere on the Internet, and businesses only pay for what they consume. Rather than purchase servers, storage and other pieces of IT equipment, businesses simply purchase a set of dials and indicators that finely-tune and adjust IT performance, availability, data protection, and security based on business requirements regardless of the actual physical location of the applications and data.[28]

Elastizität, Ressoucen-Pooling, SaaS

27. **Dale Vile, Freeform Dynamics**:

    Cloud computing ... is about the evolution of dynamic virtualised infrastructure that allows us to think more in terms of resource pools than individual IT components. This in turn opens the door to delivering computing resource on a utility basis, which is equally applicable both internally (i.e. with regard to the way you use your data centre) and externally—which takes you into the realm of utility computing and software as a service.[29]

Elastizität, Selbstbedienung, messbare Dienstqualität, SaaS, PaaS, IaaS

28. **Judith Hurwitz, Hurwitz & Associates**:

    The cloud has several key characteristics: elasticity and scalability, self-service provisioning, standardized APIs, billing and metering of services, performance monitoring and measuring, and security. There are three models for Cloud: Infrastructure as a Service, Platform as a Service, and Software as a service.[30]

Selbstbedienung, Ressourcen-Pooling, Elastizität, IaaS, PaaS, SaaS

29. **Peter Mell und Tim Grace, NIST**:

    Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg. Networks, services, storage, applications, and services], that can be rapidly provisioned and released with minimal management effort or service provider interaction.[31]

[25] http://blogs.amrresearch.com/enterprisesoftware/2009/03/the-cloud-versus-saas-compieres-don-klaiss-weighs-in.html

[26] http://www.burtongroup.com/Consulting/CloudComputingConsulting.aspx

[27] http://blogs.yankeegroup.com/2009/08/25/when-is-a-cloud/

[28] http://esgblogs.typepad.com/marks_blog/2009/03/cloud-a-picture-says-a-thousand-words.html

[29] http://freeformcomment.blogspot.com/2008/04/cloud-computing-and-web-20.html

[30] Zitiert nach http://jameskaskade.com/?p=594

[31] (Mell u. Grance, 2009)

30. **Open Cloud Computing Manifesto**: *Elastizität*

    The ability to scale and provision computing power dynamically in a cost-efficient way and the ability of the consumer (end user, organization, or IT staff) to make the most of that power without having to manage the underlying complexity of the technology.[32]

31. **BITKOM**: *Selbstbedienung, Netzwerkzugang*

    Cloud Computing ist eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand.[33]

[32](Open Cloud Manifesto, 2009)

[33](BITKOM, 2009)

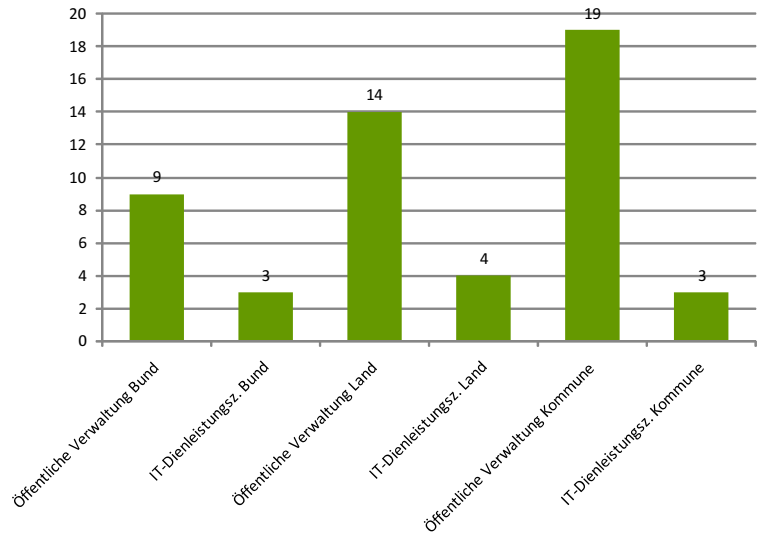
ANHANG B

Umfrage

B.1 Beteiligung

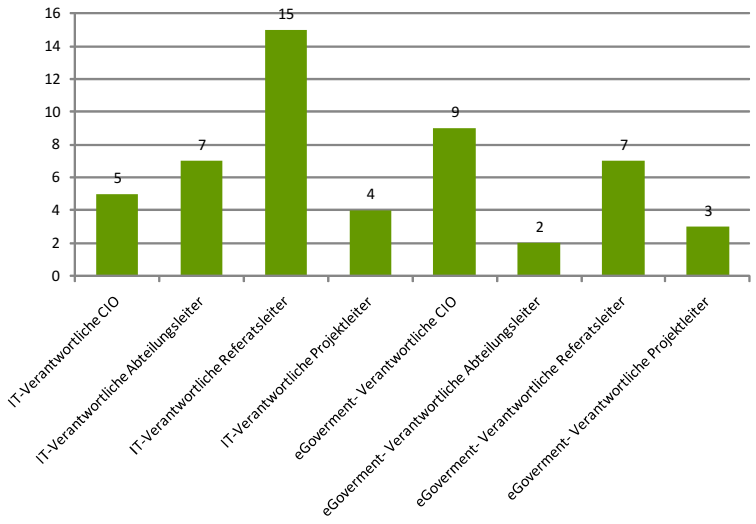
- 512 ausgesendete Fragebögen.[1]
- 52 Antworten.

Zur Auswertung des Fragebogens geben Sie bitte an, welcher Einrichtung der öffentlichen Hand Sie angehören.



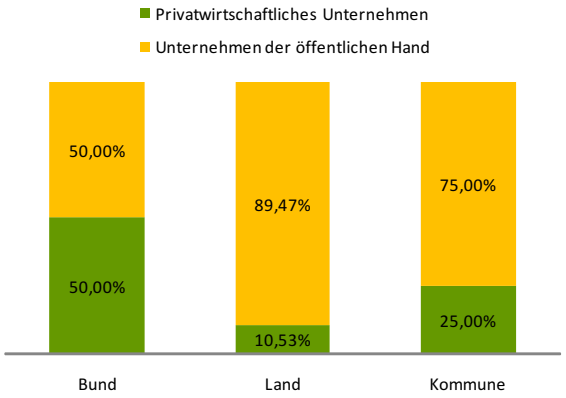
[1] Der Versandt des Fragebogens erfolgte per Email. Nicht gerechnet sind hier Fragebögen, die aufgrund von ungültigen Adressen nicht zugestellt werden konnten.

Weiterhin bitten wir Sie, eine Einordnung Ihrer Position vorzunehmen.



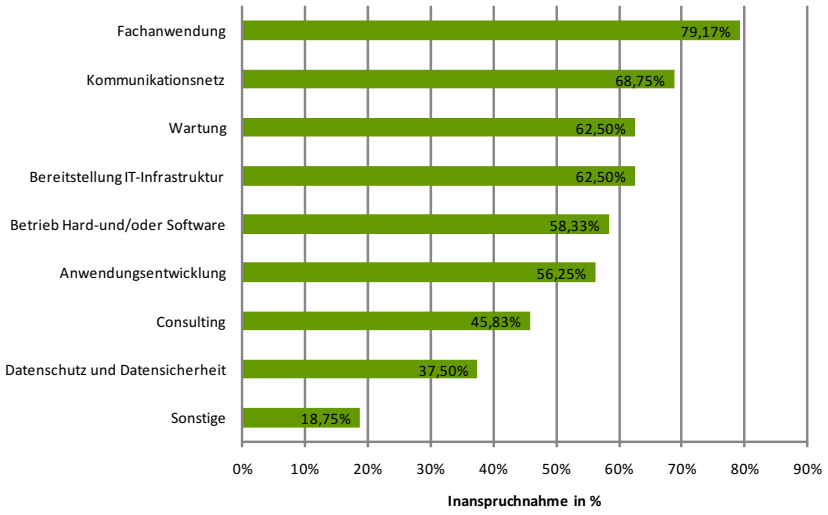
B.2 Auslagern von Dienstleistungen

Frage 1: An wen haben Sie Dienstleistungen ausgelagert?



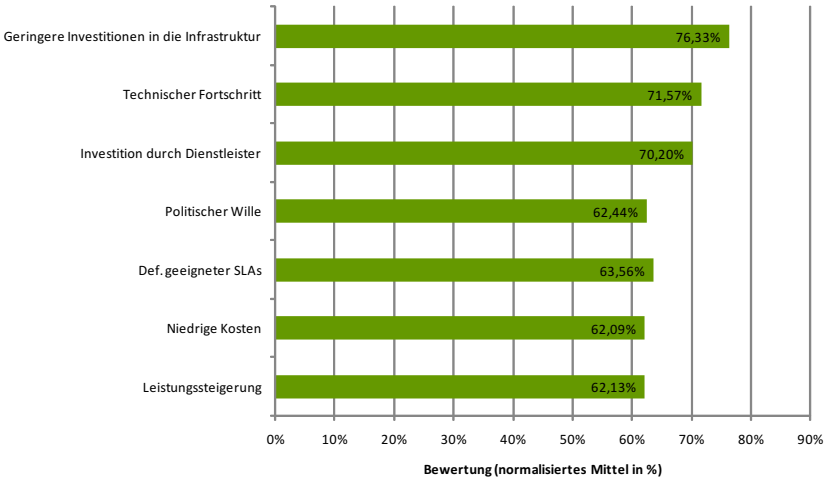
- $N = 49$

Frage 2: Welche Dienstleistungen nehmen Sie in Anspruch?



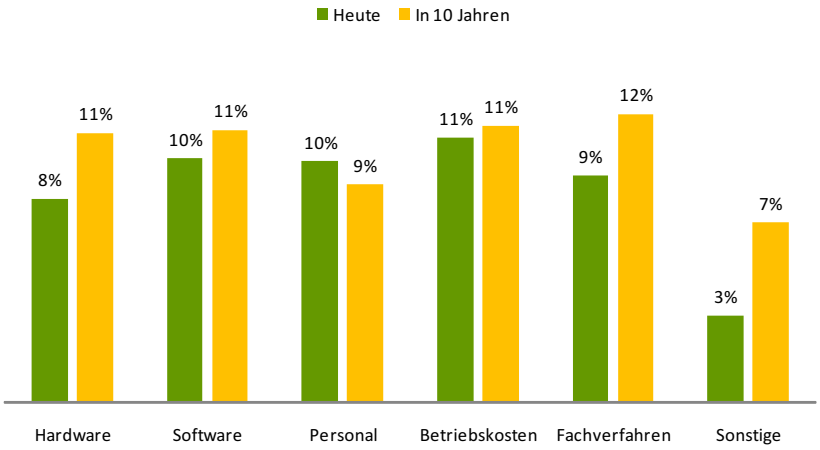
- $N = 48$

Frage 3: Was sind Ihrer Meinung nach die größten Vorteile, IT-Dienstleistung auszulagern?



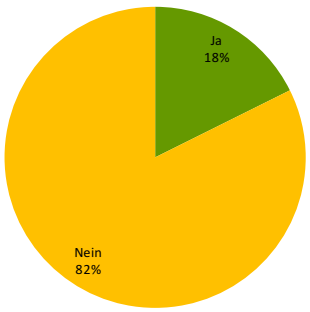
- $N = 52$

Frage 4: Bitte schätzen Sie ab, welches Einsparpotential Sie durch die IT-Leistungserbringung durch ein Dienstleistungszentrum haben bzw. erwarten.



- $N = 44$
- Bewertungsskala von 1 bis 6

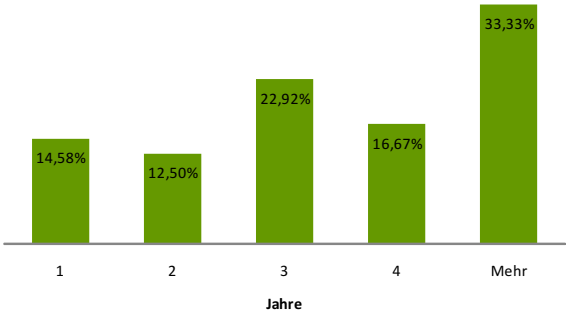
Frage 5: Haben Sie schon einmal zuvor ausgelagerte IT-Dienstleistung zurückgeholt?



- $N = 51$

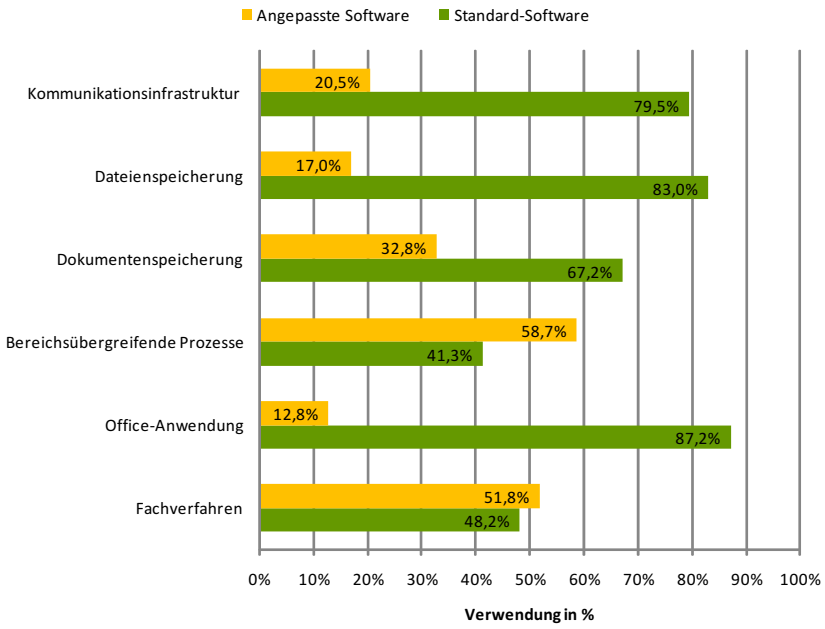
B.3 Rahmenverträge

Frage 6: Über welchen Zeitraum binden Sie sich (z. B. durch geregelte Rahmenverträge) an Ihren strategischen IT-Partner?



- $N = 48$
- Bewertungsoptionen: 1 Jahr, 2 Jahre, 3 Jahre, 4 Jahre, längerer Zeitraum.

Frage 7: Können Sie das Verhältnis zwischen Standardsoftware und Software, die an Ihre Anforderungen speziell angepasst werden muss, angeben?

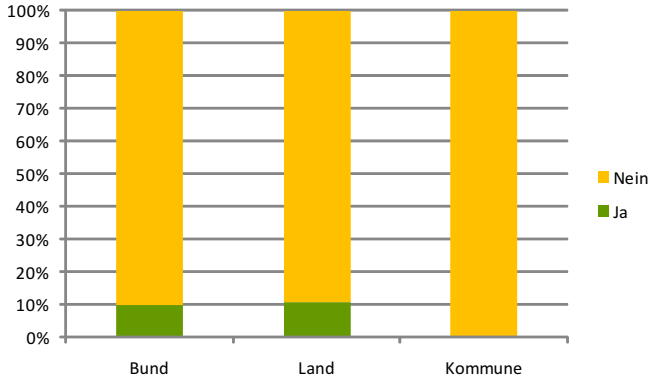


- Rücklauf N für die verschiedenen Frageoptionen:

Option	Rücklauf
Fachverfahren	$N = 46$
Office-Anwendung	$N = 46$
Bereichsübergreifende-Prozesse	$N = 35$
Dokumentenspeicherung	$N = 38$
Dateienspeicherung	$N = 40$
Kommunikationsinfrastruktur	$N = 42$

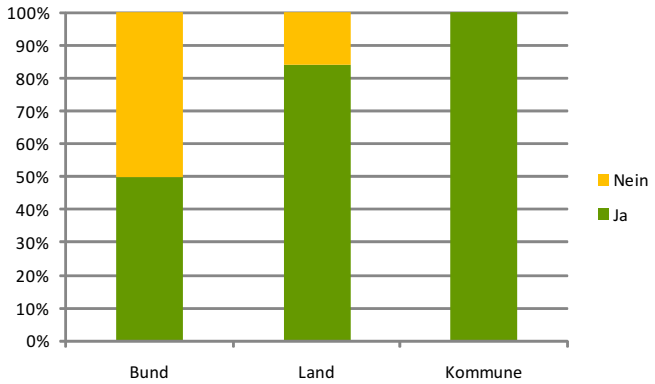
B.4 Verwaltungsübergreifendes Handeln

Frage 8: Haben Sie Hardware angeschafft, die nur für Lastspitzen vorgehalten wird?



- $N = 50$

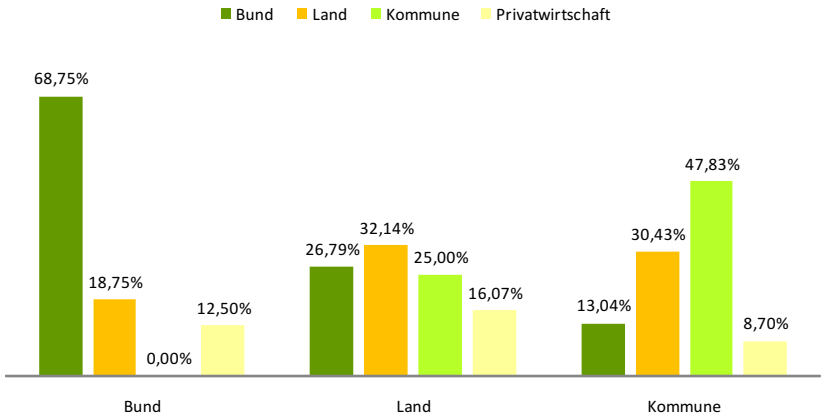
Frage 9: Können Sie sich vorstellen, Hardware und Server, die in Ihrem Dienstleistungszentrum für Sie zur Verfügung stehen oder die Sie lokal vorhalten, auch anderen Verwaltungen zugängig zu machen, sofern Sie Überkapazitäten haben und Sicherheit und Mandantenfähigkeit gewährleistet werden?



- $N = 50$

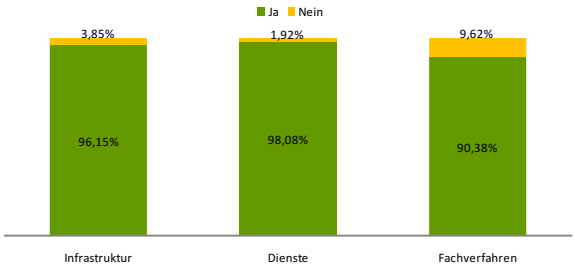
Kooperationen in der öffentlichen Verwaltung zwischen Bund, Ländern und Kommunen sind seit 2009 durch die Änderung von Art. 91 c im Grundgesetz gesetzlich verankert und sollen durch den IT-Planungsrat strategisch vorangetrieben werden. Dadurch entstehen Chancen für eine neue Qualität der Zusammenarbeit. Man hat erkannt, dass das Potential des IKT-Einsatzes nicht in monolithischen IT-Lösungen, sondern im vernetzten Arbeiten über Fach-, Ressort- und Ländergrenzen hinweg liegt.

Frage 10: Können Sie Sich vorstellen, IT-Leistungen mit Kooperationspartnern gemeinsam umzusetzen?



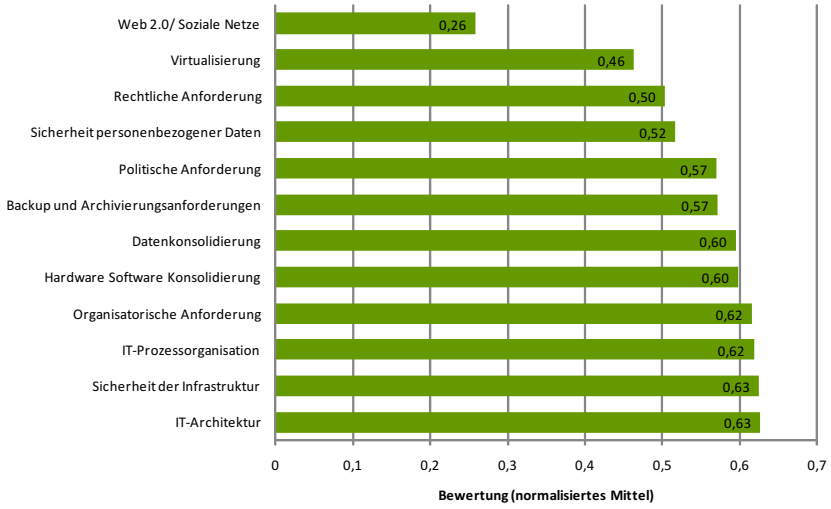
- $N = 46$

Frage 11: Können Sie sich vorstellen, bei Kooperationen innerhalb der öffentlichen Hand ressortübergreifend gemeinsam zu nutzen?



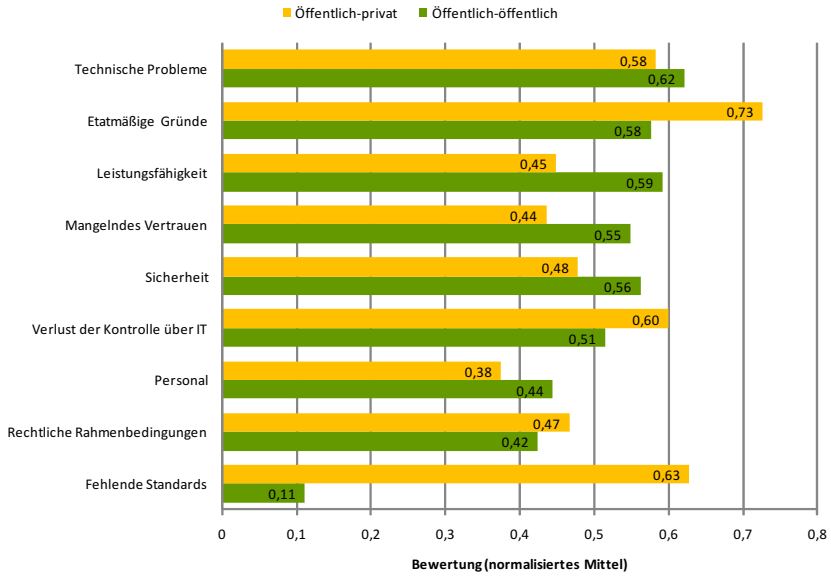
- $N = 52$

Frage 12: Was sind Ihrer Meinung nach die größten Treiber für IT-Kooperationen?



- $N = 50$
- Bewertungsskala von 1 bis 12

Frage 13: Wo sehen Sie die größten Hemmnisse für IT-Kooperationen?

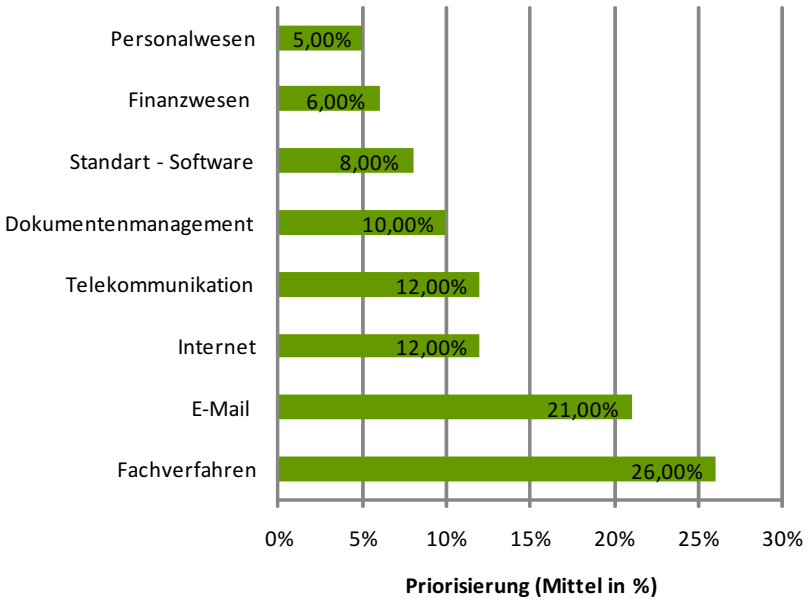


- $N = 49$
- Bewertungsskala von 1 bis 9

B.5 Verfügbarkeit und Zuverlässigkeit

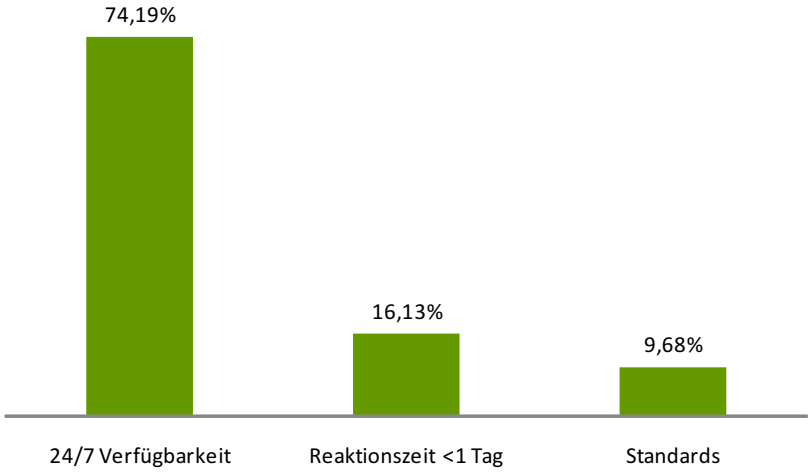
Mit dem zunehmenden Einzug von Informationstechnologien in die Verwaltungen steigt die Abhängigkeit von den Funktionen der eingesetzten Systeme. These: Daher sind eine zuverlässige Infrastruktur und die damit verbundene Verfügbarkeit der Applikationen von zentraler Bedeutung.

Frage 14: Welche Anwendungen haben für Sie die höchsten Anforderungen an Zuverlässigkeit und Verfügbarkeit?



- $N = 52$
- 56 verschiedene Anwendungen wurden genannt und in die gezeigten Kategorien unterteilt

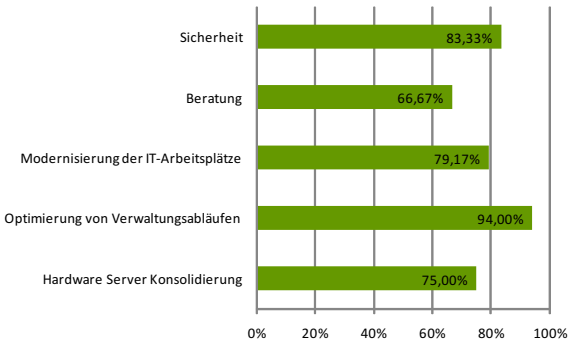
Frage 15: Welche SLAs bezüglich Verfügbarkeit und Zuverlässigkeit muss ein Drittanbieter erbringen, um Teile Ihrer Anwendungen zu betreiben?



- $N = 31$

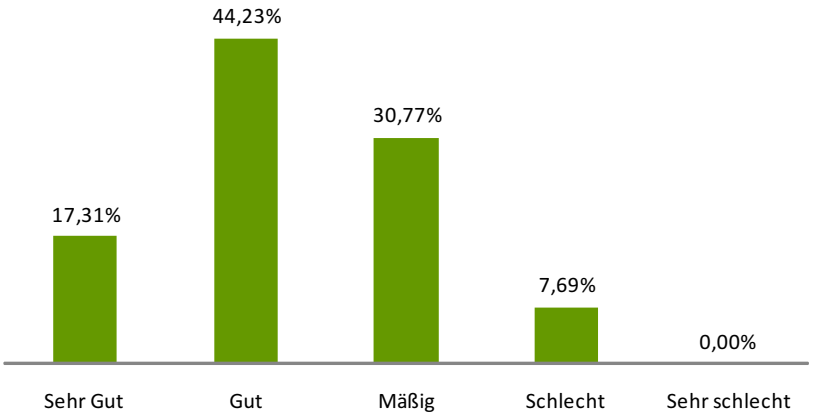
B.6 Allgemeine Fragen

Frage 16: In welche Bereiche wollen Sie in den nächsten Jahren investieren?



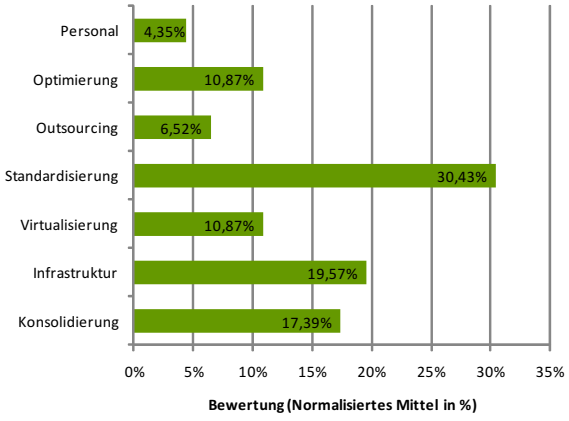
- $N = 50$

Frage 17: Wie zufrieden sind Sie insgesamt mit der IT-Landschaft in Ihrer öffentlichen Verwaltung?



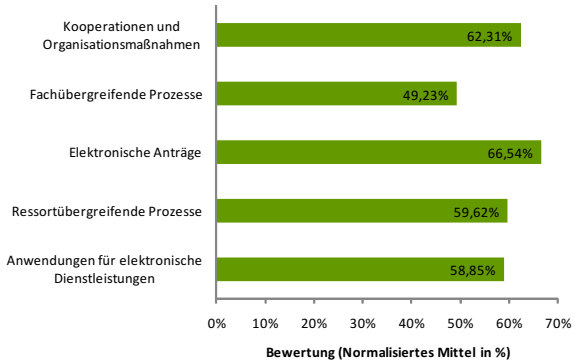
- $N = 52$
- 6-stufige Bewertungsskala

Frage 18: Sie erhalten die Möglichkeit, kurzfristig eine Veränderung der Struktur Ihrer IT-Landschaft durchzuführen. Was sollte Ihrer Meinung nach als Erstes umgesetzt bzw. verändert werden?



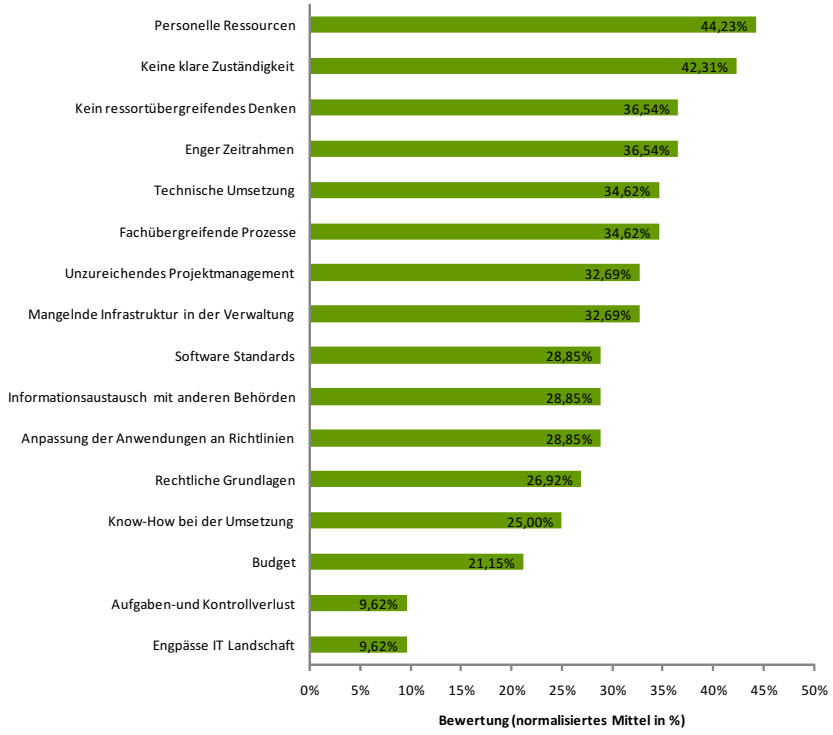
- $N = 46$

Frage 19: In welchen Bereichen sehen Sie das größte Potential zur Effizienzsteigerung?



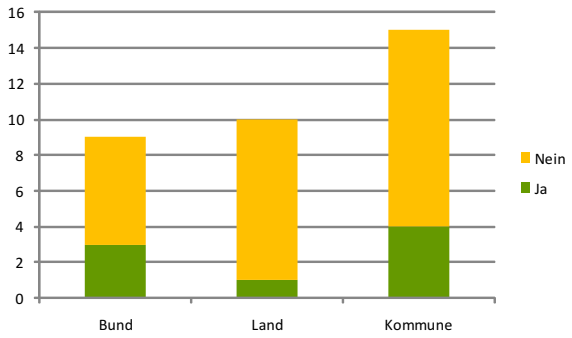
- $N = 52$
- 5-stufige Bewertungsskala

Frage 20: Bei der Einführung der EU-Dienstleistungsrichtlinie gab es viele Probleme. Trotzdem gibt es einige erfolgreiche Umsetzungen. Welches waren bzw. sind für Sie die größten Hindernisse?



- $N = 52$

Frage 21: Sind sie als IT-Dienstleistungszentrum ein Shared Service Center?

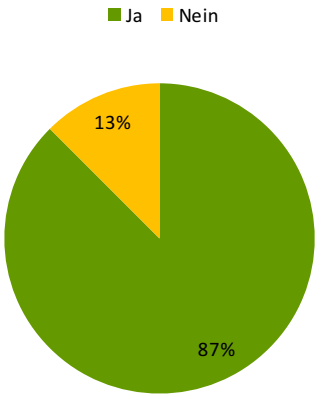


- $N = 34$

Frage 22: Welche Shared Services bieten Sie an?

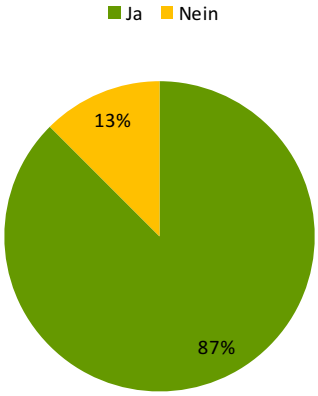
- Die folgende Auflistung ist eine Auswahl der genannten Beispiele
  - Mailserver
  - Fachanwendungen: Reise- und Umzugskosten, Entgelte Besoldung, Familienkasse, Personalverwaltung, Buchhaltung, Beschaffung usw.
  - Archivierung
  - Internet-Auftritte
  - IT-Arbeitsplatzausstattung einschl. Service/Betreuung
  - IT-Infrastruktur für Fachanwendungen
  - Storage und Sicherung
  - Helpdesk
  - Backup und Recovery
  - Sicherheitsinfrastruktur
  - Desktop-Service
  - Telekommunikation
- $N = 9$

Frage 23: Entwickeln Sie bereits Anwendungen nach dem Prinzip der Dienstorientierung (SOA, Web-Services)?



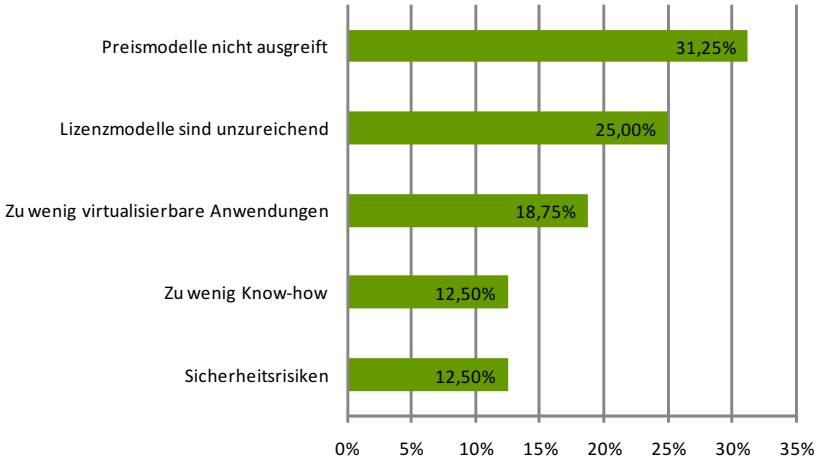
- $N = 48$

Frage 24: Verwenden Sie bereits Virtualisierungslösungen?



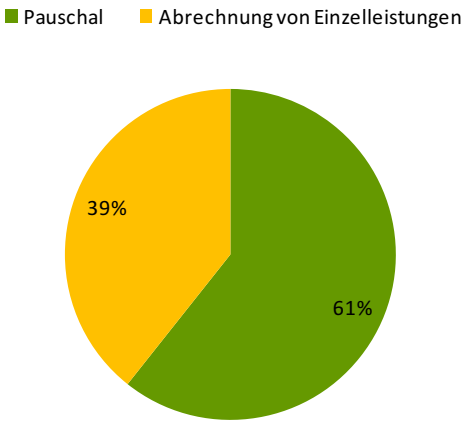
- $N = 48$

Frage 25: Was steht dem Einsatz von Virtualisierungslösungen am stärksten im Weg?



- $N = 16$

Frage 26: Nach welchen Preismodellen rechnen Sie mit ihrem IT-Dienstleistungszentrum ab?



- $N = 52$

ANHANG C

Anbieter- und Herstellerposition

Einige der in dieser Studie aufgeworfenen Fragen sowie allgemeine Fragen zum Cloud-Computing wurden in einem weiteren Fragebogen zusammengefasst und an zwei Cloud-Dienstanbieter (im Folgenden mit A_1 und A_2 bezeichnet) sowie einen Hersteller[1] von Cloud-Technologien (mit H bezeichnet) versandt. Dabei wird A_1 in den Bereichen PaaS und SaaS aktiv, während A_2 Dienstleistungen auf allen drei Ebenen (IaaS, PaaS und SaaS) offeriert. Wir geben im Folgenden die eingegangenen Antworten anonymisiert und mit entsprechenden kleineren redaktionellen Änderungen wieder.

C.1 Fragen zu IaaS

Frage 1. Werden Lastspitzen bei Ihnen automatisiert oder durch manuellen Eingriff der Systemadministratoren abgefangen? Sind darüber hinaus Maßnahmen seitens des Kunden erforderlich?

A_1: Beim Anlegen einer Applikation legt der Kunde den maximalen Skalierungsgrad fest (z. B. Anzahl der maximalen Instanzen, Größe der Instanzen, etc.). Die Anwendung skaliert innerhalb dieser Grenzen automatisch. Der Kunde kann dies manuell oder programmatisch jederzeit überschreiben.

[1] Der Fragebogen war im primär auf Cloud-Dienstanbieter zugeschnitten. Mit dem Hersteller wurde vereinbart, dass Antworten seine Antworten aus der Perspektive des Technologie-Lieferanten erfolgen sollen, d. h. das aufgezeigt werden sollte, was potentiell unter Verwendung solcher Technologien möglich ist.

A_2: Der Infrastruktur-Basisdienst[2] wird ohne automatische Lastspitzenbehandlung angeboten, kann jedoch durch den Kunden um Automatisierungsmaßnahmen erweitert werden (API Nutzung).

H: Lastspitzen werden automatisiert abgefangen. Je nach vereinbartem SLA kann ein manueller Eingriff seitens der Systemadministratoren erfolgen.

Frage 2. Wie werden Lastspitzen überhaupt festgestellt? Sind Monitoring- und Prädiktionsmechanismen verfügbar?

A_1: Es sind umfangreiche Monitoring- und Performance-Programmierschnittstelle verfügbar, die Anwender in ihre eigenen Programme bzw. Überwachungstools einbinden können. Die Schnittstellen stehen plattformunabhängig als REST[3] API zur Verfügung.

A_2: Monitoring ist als Ergänzung zum Basis-Service verfügbar, die der Kunde entweder hinzufügen kann.

H: Lastspitzen werden über Monitoring-Werkzeuge sichtbar; eine Verknüpfung dieser Informationen mit Aktivitätsmessungen auf Geschäftsprozess-Ebene ist möglich. Zusätzlich stehen in der Management-Anwendung mehrere Werkzeuge für die Provisionierung, Wartung eines Kundeninformationsmodells, Wartung eines Servicekatalogs, das Kapazitätsmanagement, Metering & Billing sowie Ressourcen-Management zur Verfügung.

Ein wichtiges Werkzeug dafür ist die Virtualisierung, gekoppelt mit einer Management-Infrastruktur, die die Bereitstellung von standardisierten Ressourcen (virtuelle Maschinen, Service-Ablaufumgebungen, Speicherplatz) regelt, sowie deren Integration in die Unternehmens-Infrastruktur im Sinne eines mess- und abrechenbaren Selbstbedienungsmodells.

Frage 3. Wie viel Zeit benötigen Sie, um dem Kunden weitere Ressourcen zur Verfügung zu stellen (z. B. die volle Rechenleistung einer neuen virtuellen Maschine)?

A_1: Der Kunde kann manuell oder programmatisch auf Lastspitzen reagieren und neue Instanzen anlegen lassen. Es werden keine minimalen bzw. maximalen Zeitspannen für das Anlegen von neuen Ressourcen garantiert. Es laufen in der Regel jedoch bereits zusätzliche Reserveinstanzen automatisch mit, um eine hohe Ausfallsicherheit zu gewährleisten, die zunächst auch für den Lastspitzenfall genutzt werden.

[2] Anbieter A_2 stellt einen Infrastruktur-Dienst in einer Standard-Konfiguration zur Verfügung, der nach entsprechenden Vereinbarungen jedoch erweitert und angepasst werden kann.

[3] REpresentational State Transfer (Architektur), vgl. z. B. http://www.oio.de/public/xml/rest-webservices.htm.

A_2: Je nach Image-Größe (kundenspezifsch) bis zu 33 Minuten für eine virtuelle Maschine.

H: Der Nutzer beauftragt die benötigten Ressourcen und fordert diese über eine Selbstbedienungs-Benutzerschnittstelle an. Über den Servicekatalog werden die bereitgestellten Ressourcen mit dem entsprechenden SLA ausgewählt und die Nutzung kann innerhalb weniger Minuten zur Verfügung stehen. Dies kann durch optimale Hardware-Auswahl sowie verschiedene integrierte Systeme umgesetzt werden.

Frage 4. Unterstützen Sie automatisierte Fehlertoleranz-Mechanismen? Wie reagieren Sie z. B. auf den Ausfall einer virtuellen Maschine oder eines physikalischen Servers? Wie charakterisieren Sie Ihre Ausfallzeiten?

A_1: Ein Kunde hat die Wahl, fehlertolerante Dienste zu beziehen. Dies ist z. B. Standard für Datenbankdienste. Datenbanken werden dabei automatisch dreifach auf unterschiedlichen Maschinen in unterschiedlichen Rechenzentrumsbereichen vorgehalten und im Falle eines Ausfalls automatisch umgeschaltet. Für Applikationsinstanzen werden für die ausfallsichere Varianten dabei mindesten zwei Instanzen vorgehalten, die genaue Anzahl wird dabei u. a. durch die gewählte Höchstgrenze des Kunden bestimmt.

A_2: Im Basisdienst wird 99.5 % Verfügbarkeit garantiert. Im Standard-IaaS werden die »basisphysischen« Server nach einem Ausfall neu aufgesetzt. Fehlertoleranz für die virtuellen Maschinen müssen vom Kunden gewährleistet werden. Weitreichendere SLAs und Mechanismen sind verhandelbar. Es werden noch Unterschiede bzgl. der Verfügbarkeit der Instanz und der Management-Plattform gemacht.

H: Der Ausfall einer virtuellen Maschine oder eines physikalischen Servers wird durch ausgefeilte Hochverfügbarkeitskonzepte abgefangen. Die Ausfallzeiten innerhalb von IaaS-Angeboten können sich zwischen 99.99% und 99.999% bewegen.

Frage 5. Werden Benutzerdaten redundant gehalten, um Datenverluste im Fehlerfall zu vermeiden?

A_1: Ja (s. Frage 4).

A_2: Im Basisdienst liegt es in der Verantwortung des Kunden, vorhandene Mechanismen auszulösen. Weitreichendere SLAs mit expliziter Absicherung von Benutzerdaten sind verhandelbar.

H: Ja, entsprechend der vereinbarten SLAs stehen automatisierte IT-Prozesse wie Provisionierung, »Snapshotting«, »Backup & Restore« und »Disaster Recovery« zur Verfügung, so dass die Benutzerdaten abgesichert werden.

C.2 Fragen zu PaaS

PaaS stellt Dienste für den Softwareentwickler bereit, um Anwendungen für die Cloud-Plattform zu entwickeln. Die Verwaltung der zugrunde liegende IT-Infrastruktur sowie die Administration und die Aktualisierung der Hardware obliegt dem Cloud-Betreiber. Durch PaaS werden potentielle Kosten bei der Administration und Wartung eingespart.

Cloud-Datenbanksysteme Im digitalen Zeitalter steigt die Flut an Daten, die von Unternehmen, Behörden und Privatpersonen erstellt werden, immer mehr an. Alle modernen Banken und Versicherungen arbeiten heute mit relationalen Datenbanksystemen als zentrale Bestandteile der Unternehmen. Die Verfügbarkeit, Vollständigkeit und Richtigkeit von Daten sind wichtige (auch gesetzlich vorgeschriebene) Anforderungen an die IT von Behörden und Unternehmen. Ein weiter wichtiger Schritt zur Erhöhung der Ausfallsicherheit und Verfügbarkeit der eigenen Datenbanken ist die Nutzung von Datenbanksystemen (DBS) in der Cloud.

Frage 6. Ein Unternehmen oder Behörde betreibt ein DBS im eigenen Rechenzentrum und möchte nun dieses in Ihre Cloud migrieren. Welche Schritte sind notwendig, um das eigene DBS auf die Cloud-Lösung umzustellen?

A_1: Es stehen kostenlose Werkzeugen für die Migration von Datenbanken und Datenbankservern zur Verfügung, die allerdings produktspezifisch sind (d. h. Start- und Zielsystem des Migrationsvorhabens müssen dieselbe Software — letzteres in der »Cloud-Edition« — verwenden).

A_2: Es wird die Infrastruktur für ein DBS als Standard-Cloud-Service angeboten. Je nach Anwendungsdesign kann das Anlegen einer einfachen Kopie ausreichend sein. In anderen Fällen kann das Redesign der Anwendung auf Grund spezifischer Anwendungsarchitekturen und Performance-Anforderungen erforderlich sein.

H: Der Nutzer beauftragt die benötigten Ressourcen (relationales Datenbanksystem) und fordert diese über eine Selbstbedienungsschnittstelle an. Über einen Servicekatalog werden die bereitgestellten Ressourcen mit dem entsprechenden SLA´s ausgewählt. Verfahren zur Datenmigration sind dokumentiert.

Frage 7. Limitieren Sie die Größe der verfügbaren Datenbanken? Wenn ja, welche Kapazitätsgrenzen hat Ihre Datenbank?

A_1: Anwendungsdaten skalieren bis zu mehreren Terabytes. Einzelne Datenbanken können dabei je nach Typ zwischen 5 und 50 GB groß werden. Dies beinhaltet nicht den Platzbedarf für weitere Kopien, die automatisch aus Verfügbarkeitsgründen angelegt werden, sowie den Platzbedarf für Protokolldateien.

A_2: Es gelten die üblichen Limitationen des gewählten Datenbank-Produktes und der darunterliegenden Infrastruktur.

H: Nein, die Größe der Datenbanken ist nicht limitiert.

Frage 8. Welche Möglichkeiten zum Backup sind vorhanden, wenn die primäre Datenbank in der Cloud ausfällt? Haben Sie ein Sicherheitskonzept, um sicherzustellen, dass weiter auf die Daten zugegriffen werden kann?

A_1: Datenbanken werden automatisch dreifach repliziert und in physisch unterschiedlichen Rechenzentrumsbereichen gespeichert, um einen Serviceausfall bei Hardwareausfällen zu vermeiden. Über gängige SQL-Schnittstellen kann der Kunde zusätzlich private Datenreplikationen durchführen.

A_2: Im Basisdienst liegt dies in der Kundenverantwortung, ist aber verhandelbar.

H: Es sind Konzepte für die Datenbank/RAC in den Bereichen »Disaster Recovery«, »Backup & Recovery«, Hochverfügbarkeit und Replikation vorhanden, die auch im Fehlerfall einen Zugriff auf die Daten erlauben.

C.3 Entwicklung von Cloud-Umgebungen

Die Programmierbarkeit der Plattform ist eine notwendige Voraussetzung dafür, dass Unternehmen und Behörden nicht nur E-Mail und Office-Anwendungen aus der Cloud nutzen können, sondern auch in der Lage sind, Geschäftsanwendungen in der Cloud betreiben.

Frage 9. Welche Schritte müssen unternommen werden, um bereits bestehende Services und Anwendungen, die etwa im eigenen Rechenzentrum »gehostet« werden, in Ihre Cloud-Umgebung migrieren zu können?

A_1: Eine Hilfestellung in Form eines Werkzeugs ist vorhanden, um Applikationen auf Tauglichkeit für die Cloud zu testen. In der Regel können entsprechende Backend-Anwendungen teilweise sogar ohne weitere Anpassungen migriert werden.

Nach dem Anlegen einer Kundenkennung können Programmierer mit einem »Software Developer Kit« bereits vorhandenen Quellcode direkt aus Standard-Programmierumgebung auf die Cloud aufbringen bzw. in diese Umgebung migrieren.

A_2: Nach einer »Workload Analyse«, der Selektion des Programmiermodels, der Bestimmung des Virtualisierungskonzepts, einer Backend-Integrationsdiskussionen (Datenbank, Applikationsserver, etc.), einer Schnittstellen-Analyse und einer Sicherheitskonzept-Definition kann die in Rede stehende Anwendung durch das Kreieren eines Images (oder mehrerer Images)

und der Konfiguration der Netzinfrastruktur migrierbar sein. In den meisten Fällen ist jedoch eine komplexere Analyse nötig.

H: Der Nutzer beauftragt die benötigten Ressourcen und fordert diese über eine Selbstbedienungsschnittstelle an. Über einen Servicekatalog werden die bereitgestellten Ressourcen mit dem entsprechenden SLAs ausgewählt. Anforderungen an die verwendeten Produkte bei einer Migration sind dokumentiert

Frage 10. In welchen Programmiersprachen kann für Ihre Cloud-Umgebung entwickelt werden (.Net, Java, PHP, C++ etc.)?

- Infrastruktur-Dienste sind vielfach unabhängig von konkreten Programmiersprachen. Auf Plattform- und Dienstebene werden gängige Programmiersprachen wie .NET, Java, PHP und Ruby werden unterstützt.

Frage 11. Wie können Fehler auch zur Laufzeit des Services oder der Applikation behoben werden oder müssen für Updates alle virtuellen Maschinen heruntergefahren werden?

A_1: Dem Kunden stehen umfangreiche Statusmeldungen für die Überwachung ihrer Anwendungen zur Verfügung. Dazu können mehrere Versionen von Anwendungen parallel ausgeführt werden, so dass der Kunde z. B. eine nicht funktionierende Anwendung gegen eine frühere Version austauschen kann.

Hat der Kunde sich für ein redundantes Lösungsangebot entschieden, überwacht der Anbieter die Verfügbarkeit und das Laufzeitverhalten der entsprechenden Anwendungen und schaltet bei Bedarf innerhalb von 2 Minuten auf eine andere Instanz um.

A_2: Das hängt von der Fehlersituation ab. Fehler sind auf Basis der virtuellen Maschinen voneinander isoliert, wobei virtuelle Maschinen kundenindividuell verwaltet werden können. Allerdings ist hier offen, ob man Fehlerbehandlung im Sinne der Fragestellungen durch das Herunterfahren der entsprechenden virtuellen Maschine realisieren würde.

H: Mit Hilfe der Management-Anwendung können Fehler auch zur Laufzeit des Dienstes oder der Applikation festgestellt werden. Mit der Verteilung von VM Images können einzelne virtuelle Maschinen geändert werden. Dabei werden Konfigurationen verwendet, die aus mehreren Komponenten (Applikationsserver, Datenbank, Web-Server, »Java Virtual Machines«, Betriebssystem) und Metadaten bestehen.

Frage 12. Kann eine Applikation oder ein Service Offline getestet werden, bevor sie in der Cloud gestellt wird? Gibt es eine Simulationsumgebung?

A_1: Programmierer entwickeln in ihrer vertrauten Entwicklungsumgebung und erproben ihre Projekte in der Regel zunächst Offline in einer lokalen Simulationsumgebung. Im Anschluss kann die Lösung direkt in die gehostete Umgebung geladen werden.

A_2: Das hängt von dem jeweiligen Testprozess ab. Tests in der Cloud sind grundsätzlich möglich.

H: Applikationen oder Dienste können in einer Referenzumgebung zur Simulation getestet werden.

Frage 13. Wenn zur Laufzeit der Cloud-Anwendung ein großer Benutzeranstieg zu verzeichnen ist, kann die Anwendung automatisch ohne menschliches Eingreifen auf neue Ressourcen zugreifen und somit die Lastspitzen abfangen? Welche Programmierhilfsmittel stehen hierfür zur Verfügung?

A_1: Die Entscheidung des Automatisierungsgrad liegt beim Kunden. Dieser legt die Obergrenze für die Anzahl von Instanzen und Datenbankgrößen fest. Über die angebotene Management-API kann dies auch automatisiert werden und programmatisch erfolgen.

A_2: Vgl. Frage 1; zusätzliche Dienstmanagementschnittstellen sind für den Benutzer vorhanden. Das der Fragestellung zugrundeliegende Szenario ist allerdings nicht auf den angebotenen Plattform-Service anwendbar, der die spezifischen Anforderungen der Anwendung nicht berücksichtigt.

H: Die Anwendung kann automatisch ohne menschliches Eingreifen auf neue Ressourcen zugreifen, wenn die Managementumgebung vollständig automatisiert wurde. Eine Überwachung der Auslastung und — je nach Konfiguration — die Bereitstellung neuer Ressourcen kann erfolgen.

Frage 14. Ist das Verteilen von rechenintensiven Operationen auf mehrere Prozessoren möglich?

A_1: Dies kann durch den Kunden durch die Wahl der Anzahl und Art der Instanzen kontrolliert werden.

A_2: Ja, gesteuert durch Hypervisor. Die Nutzung einer PC-Middleware möglich.

H: Ja, durch Überwachung der Auslastung mit neuer Verteilung, Partitionierung und mit »multi-core«-gesteuerten Algorithmen.

C.4 Datenspeicherung

Frage 15. Wie groß ist der maximale Speicher an Daten, der pro Account bei ihnen hinterlegen werden kann?

A_1: Der Speicherplatz pro Instanz ist auf 2040 GB begrenzt. Die maximale Datenbankgröße beträgt 50 GB pro Datenbank. Je nach Bedarf kann in beiden Fällen eine entsprechende Anzahl von Instanzen kombiniert werden.

A_2: Details variieren je nach angestrebten Konzept (Archivierung, Online Storage, Mailboxen, usw.). Verschiedene Ansätze mit jeweils verhandelbaren sinnvollen Speicherklassen können verfolgt werden.

H: Kein Limit vorhanden, da dies von den vereinbarten SLAs abhängt.

Frage 16. Welche Größe kann maximal eine Datei besitzen, die in die Cloud gestellt werden kann?

A_1: Unstrukturierte Daten ohne können ohne Größenbegrenzung gespeichert werden. Wenn strukturierte Daten transaktionssicher gespeichert werden sollen, dann wird eine Datenbank mit bis zu 50 GB Speicherplatz angeboten. Mit bekannten Datenbankwerkzeugen können größere Datenbanken entsprechend partitioniert werden, um auch mehrere Datenbanken im Terabyte-Bereich ablegen zu können.

A_2: Ergibt sich aus der gewählten Dateisystem-Technik je nach Service.

H: Kein Limit vorhanden, da dies von den vereinbarten SLAs abhängt.

C.5 Datenhaltung

Behörden, die gesetzlich verpflichtet sind, personenbezogene Daten nur in Deutschland bzw. in der EU zu speichern, müssen wissen, wo diese hinterlegt werden. Auch große Unternehmen legen viel Wert auf den Schutz ihrer Geschäftsdaten. Insbesondere Finanz- und Forschungsbereiche solcher Unternehmen arbeiten mit äußerst sensiblen Daten, die nicht nach außen kommuniziert werden dürfen.

Frage 17. Übernehmen Sie Garantien bezüglich des Speicherorts von Benutzerdaten? Kann der Speicherort z. B. auf ein speziellen Rechenzentrum oder ein beliebiges Rechenzentrum irgendwo in Deutschland oder dem Europäischen Wirtschaftsraum eingeschränkt werden

A_1: Die Wirtschaftlichkeit und die Ausfallsicherheit der Cloud begründet sich mit globaler Redundanz und automatisiertem Betrieb der Plattform. Der Kunde definiert bei Anwendungen die Region selbst, in der seine Anwendungen laufen bzw. Daten gespeichert werden.

Insbesondere kann der Kunde Rechenzentrumsstandorte in der EU auswählen. Eine Garantie für die Speicherung an einem bestimmten Ort kann aufgrund der oben angeführten Gründe nicht gegeben werden.

A_2: Ja!

H: Aus Herstellerperspektive nicht beantwortbar.

Frage 18. Stellen Sie Ihren Kunden Mechanismen zur Verfügung, die es erlauben, Daten logisch oder physikalisch von Daten anderer Kunden zu trennen?

A_1: Für PaaS werden Kundendaten automatisch logisch von anderen Kunden getrennt. Für SaaS ist die Möglichkeit einer physikalischen Trennung in bestimmten Fällen gegeben.

A_2: Nach Definition des Dienstbegriffs in der Cloud sind Daten getrennt.

H: Ja, durch Isolierung werden Daten logisch und physikalisch von denen anderer Kunden getrennt, sodass dadurch mandantenfähige Umgebungen bereitgestellt werden. Die Mechanismen beziehen Hardware und Software in die Mandantenfähigkeit ein.

Frage 19. Werden Benutzerdaten verschlüsselt gespeichert?

A_1: Benutzerdaten zur Identifikation des Benutzers (zwecks Abrechnung etc.) werden verschlüsselt gespeichert. Für die eigentlichen Anwendungen hängt die Verwendung von Verschlüsselung von den konkreten Implementierungen ab. Entwicklern stehen entsprechende Methoden zur Verfügung, um anwendungsspezifische Daten zu verschlüsseln bzw. verschlüsselt abzulegen.

A_2: Kunden können ihre Daten verschlüsseln, wobei die genauen Modalitäten verhandelt werden müssen.

H: Ja, je nach vereinbartem SLA.

C.6 Fragen zu SaaS

SaaS ist die oberste Schicht der »Cloud-Pyramide«: Software wird als Dienstleistung bereitgestellt. Anwendungs- und Geschäftslogiken werden in Form von Diensten angeboten, auf die »remote« über ein Netzwerk zugegriffen werden kann. Solche Cloud-Anwendungen sind in vielen verschiedenen Bereichen zu finden, z. B. Groupware, CRM, ERM, Online-Shopsysteme, Blogs, Newsletters.

C.6.1 Kommunikation

Ein wesentlicher Aspekt ist hierbei die Verfügbarkeit der Daten, auf die mobil von den meisten Standorten auf der Erde mit Internet-Zugang zugegriffen werden kann.

Frage 20. Wie hoch ist die Verfügbarkeitsgarantie sowohl für Services als auch für Daten?

A_1: Je nach ausgewähltem Service mindestens 99,9 %ige Verfügbarkeit gemessen über das Jahr.

A_2: 99,9%

H: Die ist abhängig von den vereinbarten SLA´s, und kann von 99.99% bis 99.999% betragen.

Frage 21. Besteht für den Benutzer die Möglichkeit, die Kommunikation zur Cloud zu verschlüsseln?

A_1: Ja, der Kunde kann z. B. HTTPS/SSL Technologien nutzen.

A_2: Ja, 128 Bit Verschlüsselung wird standardmäßig verwendet.

H: Ja, je nach vereinbartem SLA für die Kommunikationsverbindung.

C.6.2 Betreibermodell

Frage 22. Hosten Sie alle Cloud-Dienste exklusiv? Ist es für Ihre Kunden möglich, auf Basis der von Ihnen entwickelten Cloud-Technologien eigene (private oder spezialisierte) Clouds zu betreiben?

- Cloud-Dienste werden exklusiv betrieben. Wünschen Kunden eine »private Cloud«, so kann diese mit den entsprechenden Cloud-Technologien implementiert und betrieben werden. Dazu werden verschiedene Produkte, Dokumentationen und Dienstleistungen zur Verfügung gestellt.

A_2: »Exklusivität« ist wählbar; grundsätzlich sind eigene private Clouds implementierbar

H: Als Technologie-Lieferant werden Lösungen zum Betrieb einer eigenen Cloud bereitgestellt.

Frage 23. Falls Lastspitzen auftreten, die Sie selbst nicht in der Lage sind abzufangen, wäre es möglich, dass Sie auf Angebote anderer Cloud-Anbieter zurückgreifen?

A_1: Als einer der größten privaten Rechenzentrumsbetreiber weltweit ist A_1 sicher, hinreichende Kapazitäten für seine Kunden anbieten zu können.

A_2: Denkbar, ist augenblicklich allerdings nicht angedacht.

H: Ja, spezifische Cloud-Anbieter werden von H benannt.

C.7 Überwachung der Cloud

Frage 24. Können Sie verhindern, dass Ihre Cloud als Basis für eine DDoS-Attacke verwendet wird?

A_1: Für SaaS werden alle notwendigen Maßnahmen getroffen, um solche Attacken zu verhindern. Diese Maßnahmen sind dokumentiert und werden den Kunden mit dem Service-Vertrag zur Verfügung gestellt. Für PaaS ist A_1 nicht in der Lage, auf die Daten und Anwendungen des Kunden zuzugreifen, um präventiv eine DDoS Attacke abwehren zu können. Allerdings wird der Netzwerkverkehr innerhalb sowie in und aus seinen Rechenzentren überwacht. Es ist somit möglich, auf DDoS Attacken zu reagieren. Dazu behält sich A_1 das Recht vor, den Online-Dienst eines Kunden auszusetzen, falls A_1 der Ansicht ist, dass die Verwendung des Online-Dienstes eine direkte oder indirekte Gefahr für die Funktion oder Integrität des Netzwerks oder die Verwendung des Online-Dienstes durch andere darstellt.

A_2: Die von A_2 zur Verfügung gestellten Lösungen sorgen für eine höchstmögliche Isolation aller Instanzen gemäß Servicevereinbarung. Benutzer sind authentifiziert. DDoS-Attacken werden aktiv analysiert und bei Erkennung bekämpft.

H: »Distributed Denial-of-Service«-Attacken sind nur bei in privaten Clouds in kompletter Isolation zu vermeiden, unter Vergabe von Ressourcen-Quotas an berechtigte und zugelassene Teilnehmer und ohne deren Weitergabe an Dritte.

Frage 25. Nehmen wir umgekehrt an, einer Ihrer Kunden würde zum Opfer einer DoS-Attacke. Stellen Sie für diesen Fall Detektions- und Schutzmechanismen zur Verfügung?

A_1: Sowohl eingehender, ausgehender und rechenzentrumsinterner Netzwerkverkehr wird kontinuierlich überwacht. A_1 ist somit in der Lage, auf DoS Attacken zu reagieren.

A_2: Ja, bereits in der Basis-Dienstkonfiguration.

H: Hierfür stehen automatisierte Verfahren zur Lastminderung und Drosselung unter Berücksichtigung bestimmter Richtlinien zur Verfügung. Die Erkennung erfolgt durch die vorhandenen Monitoringwerkzeuge.

Frage 26. Unterstützen Sie forensische Maßnahmen? Können Ihre Kunden z. B. Log-Files einsehen, die ihre Daten oder Dienste betreffen, um Fehleranalysen zu betreiben?

A_1: Forensische Maßnahmen werden im Rahmen der gesetzlichen Vorgaben unterstützt. Kunden können über definierte Monitoring- und Managementschnittstellen auf ihre anwendungsbezogenen Daten zugreifen.

A_2: Ja, nach Absprache und gemäß Privacy- & Compliance-Richtlinien

H: Je nach Isolationsgrad können Kunden nur ihre eigenen Daten oder Dienste einsehen um Fehleranalysen zu betreiben.

Frage 27. Stellen Sie Monitoring-Mechanismen zur Verfügung, die es dem Kunden erlauben, SLAs zu validieren?

A_1: Ja, die Daten können vom Kunden eingesehen werden oder durch eigene Überwachungen über die genannten Monitorings- und Managementschnittstellen erfasst werden.

A_2: Ja, mit unterschiedlicher Granularität (bei Bedarf und abhängig vom Service)

H: Ja, mit dem Cloud-Management stehen Monitoring-Mechanismen zur Verfügung, die es dem Nutzer erlauben, seine SLAs zu validieren.

Frage 28. Wie genau ist der Ausfall von Diensten definiert? Sieht der Anbieter die vorübergehende Abschaltung von Diensten zu Wartungszwecken vor?

A_1: Sofern nicht anders beschrieben, ist die garantierte Verfügbarkeit über das Jahr definiert und beinhaltet keine zusätzlichen Abschaltungen zu Wartungszwecken. Eine detaillierte Beschreibung ist aus Platzgründen nicht möglich.

A_2: Wartungszeiten sind im SLA beschrieben. Der Ausfallbegriff wird nach Diensten (IaaS, PaaS, SaaS) unterschiedlich beschrieben und in verschiedene »Severity Classes« eingeteilt.

H: Der Ausfall von Diensten muss explizit im SLA definiert sein. Dies kann die vorübergehende Abschaltung von Diensten zu Wartungszwecken vorsehen.

Frage 29. Gibt es im Falle der vorübergehenden oder permanenten Nichterreichbarkeit einen alternativen Anbieter, der die entstehende Arbeitslast übernimmt? Wie sichern sie den Datentransfer für Backups in/aus der Cloud?

A_1: Es wird ein eigenes Netzwerk sowie georedundante Rechenzentren angeboten, um einer permanenten Nichterreichbarkeit vorzubeugen.

A_2: Nein, es gibt keine Alternativanbieter in der Basis-Dienstkonfiguration. Allerdings sind Export- und Import-Funktionen definiert.

H: Dies kann durch verschiedene (von H namentlich genannte) Anbieter geschehen. Der Datentransfer für Backups kann im »Disaster Recovery Konzept« spezifiziert werden, beispielsweise durch Echtzeit-Datenreplikation oder anderen Verfahren.

Frage 30. Wie kann die Schwere eines Dienstausfalls bemessen werden. Stehen hierfür Werkzeuge oder Prozeduren zur Verfügung.

A_1: Hier erfolgt ein Verweis auf Online-Dokumentationen.

A_2: Abhängig von den vereinbarten Kategorien von Leistungsmerkmalen (z. B.: Verfügbarkeit, Durchsatz, Sicherheitskonzept) unterschiedlich.

H: Ja, innerhalb der Management-Anwendung stehen geeignete Werkzeuge für Monitoring, Kapazitätsmanagement, Metering & Billing und Ressourcen Management zur Verfügung.

Frage 31. Wie wird der Kunde für Einbußen kompensiert, die durch einen Dienstausfall entstehen?

A_1: Sollte es zu Dienstausfällen kommen, die die vereinbarten SLAs mit dem Kunden überschreiten, werden dem Kunden automatisch Gutschriften in Form von »Credits« ausgestellt.

A_2: Der Basis-Service bietet keine Kompensation über das Äquivalent in gleichen »Service-Units« hinaus.

H: In der Management-Anwendung können im Rahmen von SLAs »Chargebacks« definiert werden.

Frage 32. Wird der Grad der Redundanz geregelt, die der Anbieter aufbringt, um Ausfallzeiten zu vermeiden?

A_1: Je nach gewähltem Online-Service werden Daten mehrfach auf unterschiedlichen Maschinen in unterschiedlichen Rechenzentrumsbereichen vorgehalten. Je nach Kundenregion werden unterschiedliche georedundante Rechenzentren sowie eigene Netzwerke zwischen den Rechenzentren und auch Anbindungen an das öffentliche Internet angeboten.

A_2: Wird über SLAs geregelt.

A_2: Wird über SLAs geregelt.

Frage 33. Für IaaS/PaaS-Anbieter: Können Ihre Kunden Tests der Software, die sie in Ihre Cloud auslagern möchten, in Ihrer Produktionsumgebung durchführen?

- Ja. Entwicklern wird die Möglichkeit geboten, lokale Instanzen für Test- und Entwicklungsaufgaben lokal zu betreiben.

Frage 34. Welche vertraglichen Möglichkeiten zur Beendigung des Dienstvertrags bieten Sie (z. B. Löschen von Daten, Aufbereitung der bei Ihnen gespeicherten Daten in externe Formate, usw.)

A_1: Kunden können bei Plattform-Diensten jederzeit ihre Anwendungen, Datenbanken und Daten über definierte Standardschnittstellen lokal replizieren. Bei Beendigung des Dienstvertrags hat der Kunde die Möglichkeit zu entscheiden, ob sein Account deaktiviert und anschließend die Abonnentendaten gelöscht werden oder die Abonnentendaten mindestens 90 Tage lang nach dem Ablauf oder der Kündigung des Abonnements (der »Aufbewahrungszeitraum«) in einem Account mit eingeschränkter Funktionalität aufbewahren werden sollen, damit die Daten extrahiert werden können. Nach Ablauf des Aufbewahrungszeitraums wird der Account deaktiviert und anschließend die Abonnentendaten gelöscht.

Bei Software-Diensten wird dem Kunden eine Frist gewährt, innerhalb der die Daten migriert werden können.

A_2: Verhandelbar (Das Löschen von Daten wird standardmäßig durchgeführt; eine Auslagern von Daten auf CD/DVD ist möglich).

H: Dies muss gesondert vereinbart werden.

Frage 35. Wie sieht Ihr Notfallvorsorgekonzept aus? Haben Ihre Kunden hier Möglichkeiten zur Einflussnahme?

A_1: Kunden können keinen Einfluss auf das Notfallvorsorgekonzept von A_1 nehmen. Der Anbieter informiert aber ausführlich über die Konzepte im Internet.

A_2: Das Notfallkonzept wird aus den verhandelten SLAs ableitet. A_2 ist ein langjähriger Betreiber weltweiter Rechenzentrum mit höchster Verfügbarkeit und Sicherheit.

H: Dies ist über SLA´s zu definieren und muss gesondert vereinbart werden.

Frage 36. Können Ihre Kunden mit Ihnen zusammen ein angepasstes Sicherheitskonzept erstellen?

A_1: Kunden können anhand von ausführlichen Dokumentationen ihr eigenes Sicherheitskonzept erstellen, um ihre Anwendungen bestmöglich zu schützen. Auf das Sicherheitskonzept von A_1 können Kunden im Rahmen des normalen Kundenfeedbacks Einfluss nehmen.

A_2: In der Basis-Dienstkonfiguration gibt es hier keine Anpassungsmöglichkeiten. Bei privaten Cloud-Diensten können Dienstklassen mit entsprechenden Sicherheitskonzepten verhandelt werden.

H: Ja, in Zusammenarbeit mit weiteren Hosting-Providern (von H namentlich angegeben).

C.8 Datenschutz

Anmerkung A_1. Da die gestellten Fragen vom Umfang her sehr ausführliche Antworten verlangen, wird auf weitere Informationen im Internet verwiesen. Die gegebenen Antworten sind somit lediglich als Hinweise zu verstehen.

Frage 37. Wie werden Daten verschlüsselt?

A_1: Kunden können bei Plattform- und Software-Diensten Standardverschlüsselungsalgorithmen verwenden (SSL, TLS)

A_2: Ja nach Service und SLA wird mit dem Kunden die Datenverschlüsselung durch den Anbieter oder den Kunden definiert.

Frage 38. Welche Abstufungen von Zugangsberechtigungen gibt es?

A_1: Je nach Dienst kann der Kunde unterschiedliche Zugriffberechtigungen (in der Regel mindestens Administrator, Anwender) vergeben. Dies gilt für Plattform- und Software-Dienste.

A_2: Gemäß des im Service definierte Rollenkonzepts unterschiedlich. A_2 hat Zugang nur nach Aufforderung und Abstimmung mit Kunden bzw. Institutionen, die einen Audit vornehmen.

Frage 39. Dürfen Daten ausgelagert und durch Dritte bearbeitet werden?

A_1: Für PaaS ist dies nicht der Fall. Für SaaS ist das vom jeweiligen Dienst abhängig.

A_2: Nein.

H: Nein.

Frage 40. Wo werden Sicherheitskopien schutzwürdiger Daten gespeichert?

A_1: Ausschließlich in eigenen Rechenzentren und für PaaS in den vom Kunden ausgewählten Regionen.

A_2: Unter Nutzung weltweiter Standards eines führenden Rechenzentrumbetreibers (getrenntes Rechenzentrum)

H: Im Rahmen vom privaten Plattform-Diensten in der privater Cloud bzw. einem Rechenzentrum mit angegliedertem Ausfallrechenzentrum.

Frage 41. In welcher Weise sind beteiligte Datenzentren gegen Angriffe abgesichert?

- Gesamte Palette von physischer Abschottung über digitale Überwachung bis hin zu Virenschutz. Im Grunde gibt es keinen Unterschied zu klassischen[4] Outsourcing-Rechenzentren.

Frage 42. Was geschieht, wenn Verträge neu vergeben werden?

- Wenn die Dienste in der Cloud bleiben, dann werden die Dienste einfach weiter betrieben. Bei einer Beendigung der Dienste gelten die obigen Antworten zur Vertragsbeendigung.

Frage 43. Wie sind die Prozesse definiert, mit denen Kundennachfragen oder -beschwerden zur Datensicherheit behandelt werden?

- Es werden über »Severity Codes« abgestuft Prozesse verwendet, um die Reaktionszeit der Kritikalität anzupassen.

Frage 44. Wie oft werden Audits durchgeführt und welche Werkzeuge kommen dabei zum Einsatz?

A_1: Die Rechenzentren des Anbieters A_1 sind ISO 27001 und SAS 70 Type II zertifiziert.

A_2: Unterschiedlich, ja nach Dienstleistung.

Frage 45. Wie wird die Löschung von Daten behandelt?

A_1: Siehe hierzu die Antwort auf Frage 34.

A_2: Löschung ist unumkehrbar und endgültig.

C.9 Kosten

Frage 46. Welches Abrechnungsmodell wird verwendet (basierend auf Nutzung, Verkehr, Speicher, usw.)

A_1: Je nach Dienst (Datenbank, Anwendungsplattform) werden unterschiedliche Abrechnungsmodelle verwendet.

[4] Im Original wurde der Begriff »herkömmlich« verwendet.

A_2: Abhängig vom Service, z. B. Anzahl der Benutzer pro Monat, Größeneinheiten pro Monat.

H: Das Abrechnungsmodell vom Cloud-Service Anbieter kann entsprechend der Nutzung (SaaS, PaaS, IaaS) definiert werden. Der Hosting-Provider kann seine Ressourcen auf Basis von CPU oder Nutzern intern taxieren und mit seinen eigenen Metriken auf die Nutzung der einzelnen Cloud-Schichten entsprechend umlegen.

Frage 47. Wie werden Steuern und externe Kosten wie etwa Lizenzgebühren verrechnet?

A_1: In der Regel kommen keine weiteren Lizenzgebühren hinzu. Gebühren für Plattform-Komponenten sind bereits in den Nutzungsgebühren enthalten. Für SaaS-Angebote gelten gesonderte Bedingungen

A_2: Kunden können eigene Lizenzen mitbringen oder bei Anbieter A_2 erwerben.

Frage 48. Gibt es versteckte Kosten oder zusätzliche Kosten für Schulung, Wartung, usw.?

A_1: Der Anbieter geht davon aus, dass keine weiteren versteckten Kosten auftreten. Anwendungsentwickler können für die Cloud mit den gleichen Tools wie für klassische Applikationsserver entwickeln und müssen somit nicht umfangreich geschult werden. Auch Datenbankadministratoren können innerhalb und außerhalb der Cloud identische Tools verwenden.

A_2: es gibt keine »versteckten« Kosten. Zusätzliche Kosten können je nach Kundenwunsch oder eigenen Kundenfähigkeiten anfallen, sind aber transparent.

Frage 49. Gibt es für Reseller ein Bonus-Programm, wenn sie sich für ihre Cloud Plattform entscheiden?

A_1: Ja.

A_2: Ist der Reseller ein Endkunde, wird er wie jeder andere Kunden behandelt. Wenn der Reseller einen »Channel« für einen Cloud-Service repräsentiert, ist eine Teilnahme an einem Partnerschaftsprogramm möglich.

C.10 Ihre Kunden der öffentlichen Verwaltung

Frage 50. Verfügt Ihr Unternehmen selbst über Kompetenzen und Kapazitäten, um die rechtlichen Anforderungen für die Cloud-Umsetzung von Behördenlösungen zu erkennen und auszugestalten, oder basieren entsprechende Ausgestaltung (allein) auf Pflichtenheft-Anforderungen des Kunden?

- Beide Anbieter haben aufgrund langjähriger Erfahrung im Betrieb von Cloud-Diensten sowohl die Kompetenz als auch die Kapazität, um die rechtlichen Anforderungen für die Cloud-Umsetzung von Behördenlösungen zu erkennen und auszugestalten. Dies kann allerdings nicht in Form einer Rechtsberatung für Kunden erfolgen. Lösungen werden auf Basis der von den Kunden in Ausschreibungen niedergelegten Anforderungen erstellt.

ANHANG D

Grundlagen Risiko-Management

D.1 Was sind Risiken?

Die Entwicklung von Verfahren zur Risikoabschätzung des Einsatzes von Cloud-Technologien bedarf zunächst der Begriffsschärfung: Was ist unter Begriffen wie »Schwachstelle«, »Bedrohung«, »Schadensgrößenordnung« usw. eigentlich zu verstehen?

Definition: Risiko.

Der ISO Standard 27005 (ISO, 2007) definiert ein **Risiko** als das Potential, dass eine existierende Bedrohung ausgehend von einem Bedrohungsfaktor Schwachstellen ausnutzt, die ein Vermögensgegenstand oder eine Gruppe von Vermögensgegenständen[1] aufweist und somit einer Organisation Schaden zufügt.

Die Open Group hat hierzu eine Taxonomie entwickelt (The Open Group, 2009), die den Begriff »Risiko« in weitere Faktoren aufschlüsselt: Einerseits in die Häufigkeit, in der ein spezifisches Schadensereignis auftritt, und andererseits in die wahrscheinliche Größenordnung des Verlusts (vgl. Abb. D.1).

Wahrscheinlichkeit des Auftretens eines Schadensereignisses.

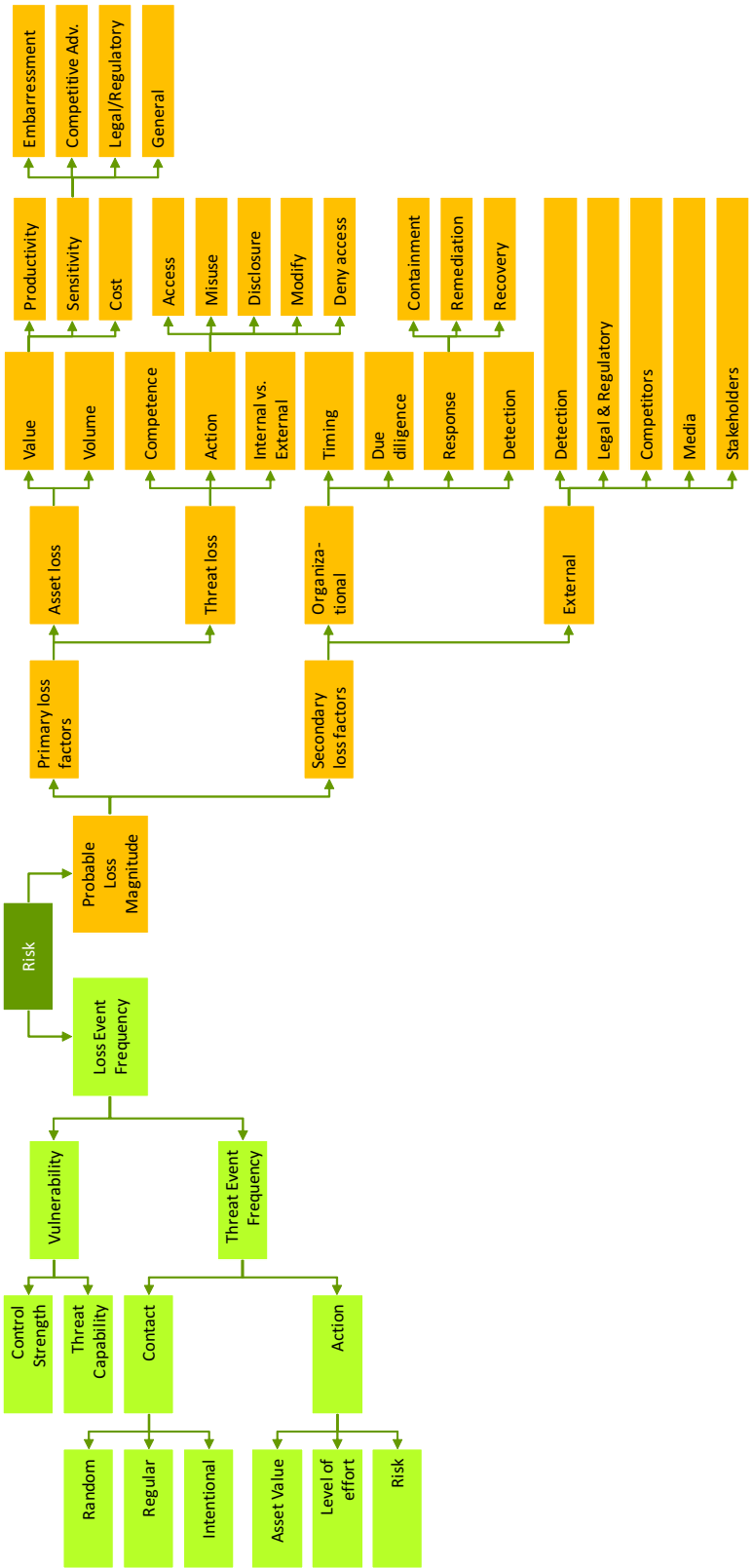
Die **Wahrscheinlichkeit des Auftretens** bezeichnet die Wahrscheinlichkeit, dass innerhalb eines spezifischen Zeitrahmens einem Vermögenswert durch einen Angreifer Schaden zugefügt wird, und wird durch zwei weitere Teilfaktoren bestimmt: Die Existenz einer Schwachstelle und die Häufigkeit, in der ein (möglicherweise erfolgloser) Angriff auf einen Vermögenswert erfolgt.

Schwachstelle.

Unter einer **Schwachstelle** ist dabei die Wahrscheinlichkeit zu verstehen,

[1] Wir verwenden den Begriff »Vermögensgegenstand« als Übersetzung des englischen Worts ›asset‹. Dieser Begriff bezieht sich also in dieser Studie nicht nur auf materielle Gegenstände, sondern auch auf ideelle Dinge wie geistiges Eigentum, Reputation, Vertrauenswürdigkeit usw.

Abbildung D.1
Risiokotaxonomie nach (The Open Group, 2009), modifiziert nach (Grobauer u. a., 2010).



mit der ein bestimmter Vermögenswert einem erfolgreichen Angriff unterliegt. Dieser Begriff ist somit durch zwei Faktoren bestimmt: Der **Wirksamkeit** des Angriffs (*threat capability*) steht die **Kontrolle** der durch den Angriff gegebene Bedrohung durch die Schutzmaßnahmen des Vermögenswerts (*control strength*) gegenüber.

Angriffshäufigkeit und Angriffspunkt.

Die**Angriffshäufigkeit** wird einerseits von der Art des Angriffspunkts und andererseits von der von der Wahrscheinlichkeit bestimmt, dass ein Angreifer einen Angriffspunkt zur Durchführung einer bestimmten Aktion ausnutzt. **Angriffspunkte** können zufällig auftreten (d. h. ein Angreifer »stolpert« über eine Schwachstelle), regelmäßig bestehen (z. B. täglich durch Wartungsarbeiten ausgelöst wird) oder aktiv durch den Angreifer ermittelt werden. Die Wahrscheinlichkeit, dass letztlich eine **Aktion** seitens des Angreifers erfolgt, wird durch den **Wert** eines erfolgreichen Angriffs für den Angreifer, den **Aufwand**, den der Angriff für den Angreifer darstellt und das **Risiko**, das der Angreifer durch den Angriff eingeht, bestimmt.

Bevor wir die rechte Seite des Diagramms aus Abb. D.1 diskutieren können, sind einige Vorbemerkungen nötig. Während die Häufigkeit eines Schadensereignisses relativ klar in Einzelfaktoren auflösbar ist, ist seine Größenordnung schwieriger zu bestimmen: Eine erfolgreiche Angriffsaktion kann mehr als einen Vermögenswert betreffen. Umgekehrt kann sich ein Schaden, der einem bestimmten Vermögenswert zugefügt wird, in unterschiedlichen Bereichen verschieden stark auswirken, so dass eine Quantifizierung nicht eindeutig möglich ist. Angriffe, die häufig auftreten, werden vorhersehbar und können in ihrer Wirkung eingedämmt werden — die Wirkung seltener oder zufällige Angriffe (»böse Überraschungen«) ist schwerer abzuschätzen. Schließlich bedingen sich Verluste gegenseitig durch oftmals komplexe Querbezüge: Ein Schadensereignis kann eine Kette von Verlusten nach sich ziehen.

Verlustkategorien.

Die Open Group Taxonomie unterscheidet sechs Verlustkategorien, die sich gegenseitig bedingen:

- **Produktivität**: Eine Organisation wird in ihrer Fähigkeit, Werte zu erzeugen, eingeschränkt.
- **Schadensbehebung**: Ausgaben, die zur Behebung eines zugefügten Schadens aufgewendet werde müssen.
- **Ersatz**: Der Verlustwert, den der Gegenstand darstellt, der durch einen Angriff beschädigt wird. Dieser Wert kann durch die Investitionskosten bemessen werden, die für eine Neuanschaffung aufgewendet werden müssen.
- **Bußgelder und Strafen**: Gerichtliche oder regulatorische Auflagen und Strafen, die aufgrund der Auswirkungen eines Angriffs gegen die geschädigte Organisation erhoben werden.
- **Wettbewerbsnachteile**, die durch den zugefügten Schaden entstehen. Hierzu zählen auch nichtmarktorientierte Nachteile wie die Verbreitung militärischer Geheimnisse, vertraulicher Regierungsinformationen, Enthüllung persönlicher Daten, usw.

- **Reputation**: Verluste, die durch die externe Wahrnehmung der geschädigten Organisation als inkompetent, leichtsinnig oder ethisch fragwürdig entstehen.

Primäre und sekudäre Faktoren der Größenordnung eines Schadensereignisses.

Kommen wir nun zurück zu den Faktoren, die die **Größenordnung** eines Schadensereignisses bestimmen und die in Abb. D.1 in primäre und sekundäre Verlustfaktoren aufgeschlüsselt werden. **Primäre Verlustfaktoren** beziehen sich einerseits die Art der betroffene Vermögensgegenstand selbst, andererseits der durch die Bedrohung ausgelöste Schaden am Vermögenswert.

Wert des Vermögensgegenstands: Kritikalität, Eigenwert und Sensitivität.

Der Wert eines **Vermögensgegenstands** kann durch seine Kritikalität, seinen Eigenwert und seine Sensitivität beurteilt werden. Unter **Kritikalität** verstehen wir hierbei die Auswirkungen auf die Prozesse der betroffenen Organisation, die ein Ausfall des Gegenstands nach sich zieht. Der **Eigenwert** eines Vermögensgegenstands besteht in den Kosten, die für einen Ersatz des Gegenstands aufgewendet werden müssen. Schließlich verstehen wir unter seiner **Sensitivität** die Größe des Schadens, die durch eine Preisgabe des Gegenstands bestimmt wird. Die Sensitivität eines Gegenstands wird unter anderem durch die Auswirkungen von **Reputationsverlust**, entstehende **Wettbewerbsnachteile** und **legale bzw. regulatorische Konsequenzen** definiert. Neben dem Wert eines Vermögensgegenstandes ist noch die **Anzahl** der betroffenen Gegenstände zu berücksichtigen.

Schaden am Vermögensgegenstand.

Der **Schaden am Vermögensgegenstand** wird durch die folgenden Faktoren bestimmt: Die Kompetenz des Angreifers, die Art der Angriffsaktion und des Angriffsursprungs, d.h. von innerhalb oder außerhalb der angegriffenen Organisation. Die **Kompetenz des Angreifers** bestimmt die Größenordnung des Schadens, den ein Angreifer befähigt ist, dem Vermögensgegenstand zuzufügen (im Unterschied zur Angriffswirksamkeit, die sich auf die Befähigung des Angreifers bezieht, einen Angriff auszuführen). **Arten von Angriffsaktionen** sind: **Unerlaubter Zugriff**, **Missbrauch**, **Preisgabe** bzw. **Enthüllung von Daten**, **Veränderung von Daten**, **Konfigurationen**, etc., und die **Unterbindung erlaubter Zugriffe**.

Organisatorische Verluste.

Sekundäre Verlustfaktoren sind einerseits organisatorisch, andererseits extern. **Organisatorische Verluste** werden durch den Zeitpunkt des Angriffs, die Sorgfaltspflicht der angegriffenen Organisation, der Reaktion auf den zugefügten Schaden und der Schadensfeststellung bestimmt. Der **Zeitpunkt** des Angriffs ist wichtig, wenn ein Angriff zu einem bestimmten Zeitpunkt einen größeren Schaden als zu anderen Zeitpunkten verursachen kann. Die **Sorgfaltspflicht** der Organisation für den Gegenstand des Angriffs bestimmt seine legalen Konsequenzen wie auch etwaige Reputationsverluste. Letztlich sind die Kosten für die **Reaktion** (Begrenzung, Beseitigung bzw. Rückkehr zum normalen Operationsmodus) auf den zugefügten Schaden sowie seiner **Feststellung und Analyse** zu berücksichtigen.

Externe Auswirkungen.

Externe Auswirkungen bestehen in den Kosten für die **Erkennung** des Angriffs, **gesetzliche bzw. regulatorische Aspekte**, **Wettbewerbsnachteile**, nachteilige **Darstellung** der betroffenen Organisation in den Medien und die Auswirkung des Verhältnisses der Organisation zu ihren Teilhabern.

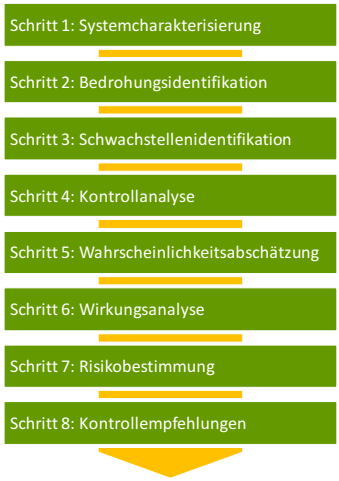


Abbildung D.2
Risikobewertung nach (NIST, 2002), modifiziert nach (Grobauer u. a., 2010).

D.2 Risikobewertung

Prozess des NIST zur Risikobewertung.

Zur tatsächlichen Bewertung des Risikopotentials schlägt das NIST (NIST, 2002) einen generischen achtstufigen Prozess vor (vgl. Abb. D.2), der in großen Teilen auf die in Abschnitt D.1 diskutierten Taxonomie abgebildet werden kann. Alternativ hierzu können auch andere Standards, z. B. die des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angewendet werden (BSI, 2008a,b,c,d), der bereits in (Streitberger u. Ruppel, 2009) ausführlich diskutiert wurde.

D.2.1 Systemcharakterisierung

Welche Komponenten und Ressourcen machen ein System aus?

In diesem Schritt werden die Komponenten und Ressourcen untersucht, die ein System (einen Vermögensgegenstand im Sinne der in Abschnitt D.1 vorgestellten Begriffsbildung) ausmachen, und seine Abgrenzung gegenüber anderen System, die sich außerhalb des Fokus' der Analyse befinden. Dazu zählen:

- Hardware
- Software
- Systemschnittstellen
- Daten und Information
- Personen, die das System benutzen bzw. mit seiner Wartung beschäftigt sind
- Systemaufgaben
- System- und Datenkritikalität
- System- und Datensensitivität

Weiterhin sind zu berücksichtigen:

- Funktionale Anforderungen des Systems

- Sicherheitsanforderungen (organisatorisch, gesetzlich, usw.)
- Sicherheitsarchitektur des Systems.

D.2.2 Bedrohungsidentifikation

Was sind die Quellen potentieller Bedrohungen?

Im zweiten Schritt wird die Quelle potentieller Bedrohungen identifiziert. In diesem Schritt werden die Faktoren analysiert, die den linken Teilbaum aus Abb. D.1 ausmachen, mit Ausnahme der Schwachstellenidentifikation (Abschnitt D.2.3) und der Kontrollanalyse (Abschnitt D.2.4). Neben diesen Faktoren wird auch noch die Motivation eines Angreifers untersucht, um die Natur der Bedrohung besser zu verstehen und ihre Wirkung abschätzen zu können.

D.2.3 Schwachstellenidentifikation

Wie können die Schwachstellen eines Systems identifiziert werden?

In diesem Schritt werden Schwachstellen des untersuchten Systems identifiziert. Die Empfehlung (NIST, 2002) nennt unter Anderem die folgenden primären Quellen:

- Audit-Berichte, Systemanomalien-Berichte, Sicherheits-Reviews oder Systemtest-Berichte, die für das untersuchte System bereits vorliegen.
- Schwachstellenlisten wie etwa die NIST I-CAT Datenbank [2]
- Sicherheitsratgeber (FedCIRC, Department of Energy's Computer Incident Advisory Capability bulletins).
- Sicherheitshinweise der Hersteller bzw. Anbieter
- Internet-Recherchen, Blogs und Foren.[3]

Recherchen können durch pro-aktive Methoden ergänzt werden (vgl. Abschnitt D.2.4)

D.2.4 Kontrollanalyse

Welche Maßnahmen stehen zur Abwehr bzw. Abmilderung von Angriffen zur Verfügung?

In diesem Schritt wird untersucht, inwieweit implementierte oder für eine Implementierung vorgesehene Kontrollmaßnahmen geeignet sind, die Wahrscheinlichkeit eines erfolgreichen Angriffs zu verringern. Die Implementierung der Kontrollmaßnahmen (technisch, etwa Verschlüsselung oder Eindringlings-Detektions-Software, oder nicht-technisch, z.B. Sicherheitsrichtlinien oder physische Zugangskontrollen) ist dabei in Beziehung zur Angriffsquelle zu setzten. Kontrollen sind entweder präventiv oder überwachend:

- Präventive Maßnahmen soll das Unterlaufen von Sicherheitsrichtlinien verhindern. Hierzu zählen Zugangskontrollen, Verschlüsselung, Firewalls, usw.

[2] http://icat.nist.gov

[3] Z.B. SecurityFocus.com

Klasse	Definition
Niedrig	Der Angreifer ist unzureichend motiviert oder nicht in der Lage, einen Angriff durchzuführen. Kontrollmaßnahmen sind implementiert und geeignet, einem Angriff vorzubeugen oder ihn zu verhindern oder zumindest zu behindern.
Mittel	Der Angreifer ist motiviert und fähig einen Angriff durchzuführen. Effektive und effiziente Kontrollmaßnahmen jedoch sind implementiert.
Hoch	Der Angreifer ist motiviert und fähig einen Angriff durchzuführen. Kontrollmaßnahmen sind nicht verfügbar oder nicht effektiv.

Tabelle D.1
Wahrscheinlichkeitsquantifizierung nach (NIST, 2002).

- Überwachende Maßnahmen sollen aktuelle Angriffe entdecken. Beispiele sind intrusion detection Software oder Zertifikatsprüfungen.

D.2.5 Wahrscheinlichkeitsabschätzung

Wie wahrscheinlich ist eine Bedrohung?

Aufgrund der in den **Abschnitten D.2.1 – D.2.4** beschriebenen Analysen kann nun die Wahrscheinlichkeit einer Bedrohung abgeschätzt werden. Dabei wird berücksichtig:

- Die Quelle einer Bedrohung, ihre Motivation sowie ihre Befähigung, einen erfolgreichen Angriff vorzunehmen
- Die Natur der angegriffenen Schwachstelle
- Die Existenz und Effektivität von Kontrollmaßnahmen.

In (NIST, 2002) wird die in Tab. D.1 Quantifizierung vorgeschlagen:

D.2.6 Wirkungsanalyse

Wie wirkt sich ein Angriff auf den Vermögensgegenstand aus?

Nachdem in den vorhergehenden Schritten die Art eines potentiellen Angriffs analysiert wurde, wird in diesem Schritt seine Wirkung auf Vermögensgegenstände der betroffenen Organisation untersucht. Die in (NIST, 2002) vorgeschlagene Methodologie ist dabei weniger detailliert dargestellt als die feingranulare Begriffsbildung aus (The Open Group, 2009), die in Abschnitt D.1 diskutiert wurde. Beide Ansätze stimmen jedoch in den wesentlichen Elementen überein.

Wesentlich für die Wirkungsanalyse sind die folgenden Faktoren, die bereits in Schritt 1 (Abschnitt D.2.1) ermittelt wurden:

- Systemaufgaben
- System- und Datenkritikalität
- System- und Datensensitivität

Tabelle D.2 Wirkungsquantifizierung nach (NIST, 2002).

Klasse	Definition
Niedrig	Die erfolgreiche Ausnutzung einer Schwachstelle resultiert im greifbaren Verlust von Vermögensgegenständen oder hat eine spürbare Auswirkung auf einige Prozesse der betroffenen Organisation.
Mittel	Die erfolgreiche Ausnutzung einer Schwachstelle resultiert im kostspieligen Verlust von Vermögensgegenständen oder hat Auswirkungen auf die Prozesse und Aufgabenerfüllung der betroffenen Organisation oder resultiert in einer erhöhten Verletzungsgefahr.
Hoch	Die erfolgreiche Ausnutzung einer Schwachstelle resultiert im überaus kostspieligen Verlust von Vermögensgegenständen oder macht die Aufgabenerfüllung der betroffenen Organisation unmöglich oder resultiert in der Gefahr schwerer oder lebensbedrohlicher Verletzungen.

Die Wirkung eines sicherheitsrelevanten Zwischenfalls kann sich auf die Systemintegrität, die Systemverfügbarkeit und die Systemvertraulichkeit auswirken:

Auf welche Faktoren kann ein Angriff wirken?

- **Integritätsverlust**. Integrität bezieht sich hierbei auf die Anforderung, das Daten und Prozesse eines Systems vor unzulässiger und fehlerhafter Modifikation geschützt werden müssen. Die Verwendung korrumpierter Daten und Prozesse resultiert nicht nur in Systeminstabilitäten sowie fehlerhaften und fehlbegründeten Entscheidungen durch den Systembenutzer, sondern erzeugt auch weitere Systemschwachstellen, die in nachfolgenden Angriffen ausgenutzt werden können.
- **Verfügbarkeitseinschränkung**. Einschränkungen der Systemverfügbarkeit führen dazu, dass Systembenutzer in der Erfüllung und Wahrnehmung ihrer Aufgaben und Verantwortlichkeiten behindert sind bzw. diesen nicht mehr nachkommen können.
- **Vertraulichkeitsverlust**. System- und Datenvertraulichkeit bezieht sich auf den Schutz sensibler Daten und Systemprozesse vor nichtautorisierter Enthüllung. Zu betrachten ist hier der Schutz personenbezogener Daten, Schutz geistigen Eigentums, nationale Sicherheitsbelange, Firmengeheimnisse usw.

Zur Wirkungsanalyse wird wiederum eine dreistufige Quantifizierung vorgeschlagen (Tab. D.2).

D.2.7 Risikoabschätzung

Quantifizierung des Risikos

Zur abschließenden Risikoabschätzung aufgrund der vorgenommenen Analysen kann nun die in Tab. D.3 dargestellte Berechnungsvorschrift verwendet werden, die den Wirkungs- und Bedrohungen Zahlenwerte zugeordnet:

Der Klassifizierung der Risiken liegt die folgende Quantifizierung zugrunde:

	Wirkung		
Bedrohung	Niedrig (10)	Mittel (50)	Hoch (100)
Niedrig (0,1)	Niedrig $10 \times 0,1 = 1$	Niedrig $50 \times 0,1 = 5$	Niedrig $100 \times 0,1 = 10$
Mittel (0,5)	Niedrig $10 \times 0,5 = 5$	Mittel $50 \times 0,5 = 25$	Mittel $100 \times 0,5 = 50$
Hoch (1,0)	Niedrig $10 \times 1,0 = 10$	Mittel $50 \times 1,0 = 50$	Hoch $100 \times 1,0 = 100$

Tabelle D.3
Risikobestimmung nach (NIST, 2002).

- Niedrig: 1 - 10,
- Mittel: 11 - 50,
- Hoch: 51 - 100.

Für diese Risiken werden nun die in Tab. D.4 aufgezählten allgemeinen Empfehlungen bezüglich der erforderlichen Maßnahmen gegeben.

D.2.8 Kontrollempfehlungen

Im letzten Schritt werden Empfehlungen zur Implementierung von Maßnahmen gegeben, die Risiken beseitigen oder abmildern können. Zielsetzung ist hier hierbei, Risiken auf ein akzeptables Maß zu verringern; eine vollständige Beseitigung ist aus Kostengründen nicht immer möglich oder wünschenswert. Die folgenden Faktoren sollen dabei in Rechnung gezogen werden:

- Effektivität der Empfehlung (z. B. Systemkompatibilität)
- Gesetzliche Bestimmungen und regulatorische Richtlinien
- Richtlinien der betroffenen Organisation
- Einfluss auf die Prozesse und Aufgabenerfüllung der Organisation
- Sicherheit und Zuverlässigkeit

D.2.9 Beispiel: Risikobewertung nach ENISA

ENISA-Kompendium Cloud-spezifischer Risiken.

Das ENISA Dokument (ENISA, 2009) identifiziert 53 Cloud-spezifische Risiken aus drei Kategorien (Verletzung von Richtlinien und organisatorische Risiken, technische Risiken, gesetzliche Risiken), die sich auf 31 Cloud-spezifische und 21 weitere Schwachstellen und 23 Vermögensgegenstände bezieht. Jedem Risiko wird eine Wahrscheinlichkeit zugeordnet, die in Beziehung zu einem vergleichbaren Risiko bei herkömmlicher Technologien gesetzt wird; ebenso wird die Wirkung quantifiziert und in Beziehung zu herkömmlichen Technologien gesetzt. Zusammenfassend wird eine Quantifizierung des Risikos angegeben. Tab. D.5 erläutert den Ansatz anhand eines Beispiels.

Tabelle D.4
Generelle Empfehlungen nach (NIST, 2002).

Klasse	Empfehlung
Niedrig	Für ein als »niedrig« eingestuftes Risiko hat der Betreiber des potentiell betroffenen Systems zu entscheiden, ob und welche Maßnahmen erforderlich sind.
Mittel	Für ein als »mittel« eingestuftes Risiko werden korrektive Maßnahmen empfohlen. Ein Plan, wie und in welchem Zeitrahmen diese Maßnahmen implementiert werden können, ist zu entwickeln.
Hoch	Für ein als »hoch« eingestuftes Risiko sind korrektive Maßnahmen dringend erforderlich. Das betroffene System kann unter Umständen seinen Betrieb fortsetzen, korrektive Maßnahmen müssen jedoch so schnell wie möglich geplant und implementiert werden.

D.3 Kontrollmaßnahmen

Bewertungsprozeduren für Kontrollmaßnahmen zur Behebung oder Verminderung von Schwachstellen werden in (NIST, 2009) ausführlich diskutiert. Maßnahmen werden dabei in Familien und Unterfamilien unterteilt, wobei für jede Unterfamilie eine Reihe von Prozeduren definiert wird. Einige Teilfamilien sind als »obsolet« gekennzeichnet, da sie bereits durch andere Teilfamilien abgedeckt werden. Die folgenden Familien werden genannt:

Liste der in (NIST, 2009) vorgeschlagenen Familien von Kontrollmaßnahmen.

- Zugangskontrolle (AC)
- Sicherheitsbewusstsein und Training (AT)
- Audit und Rechenschaftslegung (AU)
- Sicherheitsbewertung und Autorisierung (CA)
- Konfigurationsmanagement (CM)
- Notfallplanung (CP)
- Identifikation und Authentifizierung (IA)
- Reaktionen auf Zwischenfälle (IR)
- Wartung (MA)
- Medienschutz (MP)
- Physische Schutz und Umweltschutz (PE)
- Planung (PL)
- Persönliche Sicherheit (PS)
- Risikobewertung (RA)
- Systemanschaffung und Dienstinanspruchnahme (SA)
- Schutz von Systemen und Kommunikation (SC)

- Integrität von Systemen und Information (SI)
- Programm-Management (PM)

Eine vollständige Aufzählung aller Familien und Teilfamilien und der damit verbundenen Zielsetzungen und Prozeduren würde den Umfang dieser Studie sprengen. Die folgende Tabelle gibt einen exemplarischen Überblick über die Familie »Zugangskontrolle«.

Zugangskontrolle als Beispiel für eine Familie von Kontrollmaßnahmen nach (NIST, 2009). Die Familie ist in 22 Teilfamilien gegliedert.

- **Bezeichnung**: Zugangskontrolle
- **Akronym**: AC
- **Kategorie**: Technisch
- **Teilfamilien**

  AC-1 Zugangskontrollrichtlinien und -prozeduren: Implementiert und dokumentiert die untersuchte Organisation die notwendigen Richtlinien und Prozeduren?

  AC-2 Account-Verwaltung: Wie werden Benutzer- und System Accounts verwaltet?

  AC-3 Zugangskontrollzwang: Wie werden Zugangsautorisierungen erzwungen?

  AC-4 Informationsfluss: Wie wird die Verbreitung von Information innerhalb des Systems und er Zugang zu diesen Informationen geregelt?

  AC-5 Trennung von Pflichten: Werden Pflichten innerhalb der Organisation definiert, in getrennter Weise Personen oder Rollen zugeordnet. Existieren entsprechende Dokumentationen. Werden gezielt Information zur Wahrnehmung dieser Pflichten zur Verfügung gestellt?

  AC-6 Minimale Privilegien: Definiert die Organisation für Zugang zu Daten und Prozessen die hierfür notwendigen minimalen Privilegien und trifft Maßnahmen, dass ausschließlich diese Privilegien erteilt werden?

  AC-7 Fehlgeschlagene Anmeldungsversuche: Trifft die Organisation Maßnahmen im Falle fortlaufend fehlerhafter Login-Versuche (Beschränkung der Anzahl, Account-Sperrung usw.)?

  AC-8 Benachrichtigung über erlaubte Systembenutzung: Trägt die Organisation Sorge, dass Benutzer zu jedem Zeitpunkt über ihre Privilegien und die erlaubte Systembenutzung informiert sind (Disclaimer, Banner usw.)?

  AC-9 Benachrichtigung über vorhergehende Anmeldungen: Werden Benutzer über Anzahl und Zeitpunkt der vorhergehenden erfolgreichen oder erfolglosen Login-Versuche informiert? Werden Änderungen in der Login-Prozedur oder im der Account-Verwaltung angekündigt?

AC-10 Kontrolle gleichzeitiger Sitzungen: Ist die Anzahl der Sitzungen, für die ein Benutzer angemeldet sein kann, beschränkt?

AC-11 Sitzungssperre: Wird eine Benutzersitzung nach einer bestimmten Zeitspanne der Inaktivität gesperrt?

AC-12 (obsolet)

AC-13 (obsolet)

AC-14 Ohne Authentifizierung erlaubte Aktionen: Gibt es Aktionen, die Benutzer ohne Authentifizierung ausführen dürfen? Ist die Begründung hierfür und der Anwendungskontext solcher Aktionen ausreichend dokumentiert?

AC-15 (obsolet)

AC-16 Sicherheitsattribute: Können Informationen, die gespeichert, verarbeitet oder übermittelt werden, Sicherheitsattribute zugeweisen werden? Können solche Attribute dynamisch je nach Verwendungskontext dieser Informationen definiert werden?

AC-17 Remote-Zugang: Erlaubt die Organisation einen Remote-Zugang zu dem System? Existieren hierfür Einschränkungen und Richtlinien und wie werden diese erzwungen und umgesetzt? Welche Authentifizierung-Mechanismen sind vorhanden? Wie werden Remote-Zugänge beobachtet? Werden Verschlüsselungsmechanismen verwendet?

AC-18 Zugang mit Hilfe von Luftschnittstellen: Erlaubt die Organisation einen Zugang über Luftschnittstellen? Welche Maßnahmen, Einschränkungen, Richtlinien usw. werden verwendet?

AC-19 Zugangskontrolle für mobile Geräte: Welche Maßnahmen zur Zugangskontrolle für mobile Endgeräte werden verwendet? Welche Anforderungen sind für solche Geräte definiert? Für welche Informationen und Prozesse ist Zugang mit Hilfe mobiler Geräte zulässig? Wie werden solche Zugänge protokolliert? Wie wird mit portablen Speichermedien umgegangen?

AC-20 Verwendung externer Informationssysteme: Existieren Regelungen und Mechanismen zur Steuerung des Zugangs zu externen Informationssystemen in Verbindung mit des Benutzung der organisationseigenen Systems?

AC-21 Kollaboration und gemeinsame Benutzung von Informationen: Existieren Regelungen und Mechanismen, die die Kollaboration von Benutzern und die gemeinsame Nutzung von Informationen betreffen?

AC-22 Öffentlich zugängliche Informationen: Erteilt die Organisation bestimmten Personen die Erlaubnis, Informationen öffentlich zu machen. Wie werden diese Personen trainiert? Werden solche Informationen regelmäßig überprüft und gegebenenfalls gesperrt?

R.10 Böswilliger Insider — Missbrauch von hochprivilegierten Rollen

Wahrscheinlichkeit	Mittel	**Vergleich**: Geringer als bei herkömmlichen Technologien
Wirkung	Sehr hoch	**Vergleich**: Höher, gleiche Wirkung auf einen spezifischen Benutzer

Schwachstellen

- V34. Unklare Rollen und Verantwortlichkeiten
- V35. Mangelhafte Durchsetzung von Rollenverbindlichkeiten
- V36. »Need to know« Prinzip wird nicht angewendet
- V1. AAA Schwachstellen
- V39. Schwachstellen im System oder Betriebssystem
- V37. Unzureichende physische Sicherheitsmaßnahmen
- V10. Unverschlüsselte Datenverarbeitung
- V48. Anwendungsschwachstellen oder unzureichendes Patch-Management

Vermögensgegenstand

- A1. Firmenreputation
- A2. Kundenvertrauen
- A3. Expertise und Loyalität der Angestellten
- A4. Geistiges Eigentum
- A5. Persönliche sensitive Daten
- A6. Persönliche Daten
- A7. Persönliche kritische Daten
- A8. Operationelle Daten
- A9. Dienstbreitstellung (Realzeit-Einschränkungen)
- A10. Dienstbereitstellung (allgemein)

Risiko	**HOCH**

Tabelle D.5
Risikobewertung nach (ENISA, 2009).

ANHANG E

IT-Grundschutz

Dieses Kapitel ergänzt die im vorhergehenden Kaptiel III.1 präsentierten Überlegungen zur Sicherheit von Cloud-Systemen um das Thema Grundschutz, das sich im wesentlichen auf die Identifikation von Gefährdungen konkreter schützenswerter Vermögensgegenstände und Maßnahmen zu deren Schutz bezieht; insbesondere untersuchen wir die Grundschutzkataloge des BSI auf ihre Anwendbarkeit im Bereich Cloud-Computing. Eine vollständige Diskussion dieser Kataloge kann aufgrund ihres Umfangs an dieser Stelle nicht geleistet werden, wir beschränken uns deshalb auf diejenigen Teile der Kataloge, die sich mit dem Thema Dienstauslagerung beschäftigen.

E.1 Standards zum BSI Grundschutz

Das BSI definiert eine Reihe von Standards zum IT-Grundschutz:

- »Managementsysteme für Informationssicherheit (ISMS)« (BSI, 2008a) definiert grundlegende Anforderungen an solche Managementsysteme.
- »IT-Grundschutz-Vorgehensweise« (BSI, 2008b) beschreibt den Aufbau von Managementsystemen für Informationssystemen in der Praxis.
- »Risikoanalyse auf der Basis von IT-Grundschutz« (BSI, 2008c) zielt darauf ab, Anwendern eine Vorgehensweise zum Risikomanagement an die Hand zu geben.
- »Notfallmanagement« (BSI, 2008d) erklärt, wie ein systematisches Notfallmanagement aufgebaut werden kann.

E.2 Grundschutzkataloge des BSI: Zielsetzung und Aufbau

Zielsetzung: Etablierung eines angemessenen Schutzniveaus.

Die Zielsetzung der vom BSI herausgegebenen Grundschutzkataloge ist wie folgt umrissen:

> *In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme empfohlen. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.*[1]

Die Grundschutzkataloge sind in eine Reihe von Bausteinen unterteilt, die sich auf bestimmte Komponenten, Vorgehensweisen und IT-Systeme eines IT-Verbunds beziehen, wobei unter einen IT-Verbund *»die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen [ist], die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.«*[2].

Kategorisierung der Bausteine.

Jeder Baustein identifiziert eine Gefährdungslage sowie entsprechende Maßnahmenempfehlungen. Die Bausteine sind in fünf Kategorien unterteilt:

- **B 1**: Übergreifende Aspekte der Informationssicherheit des IT-Verbunds d. h., solche Aspekte, die den gesamten betrachteten Komplex von IT-Systeme, Infrastruktur, usw. betreffen, also z. B. IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.
- **B 2**: Sicherheit der Infrastruktur[3], d. h. baulich-physischen Gegebenheiten, d. h. Gebäude, Serverraum, Schutzschrank häuslicher Arbeitsplatz, etc.
- **B 3**: Sicherheit der IT-Systeme bezieht sich auf einzelne Systeme, z. B. TK-Anlagen, Laptops, oder Server.

[1] Vgl. (BSI, 2010a, Allgemeines→Einstiegskapitel).

[2] Vgl. (BSI, 2010a, Allgemeines→Einstiegskapitel)

[3] Nicht zu verwechseln mit der Verwendung des Begriffs »Infrastruktur« als Cloud-Diensttyp, der dort Kommunikation, Rechenkapazität und Speicher umfasst.

- **B 4**: Sicherheit im Netz bezieht sich auf die Vernetzungsaspekte, d. h. insbesondere Netzverbindungen und die Kommunikation. Beispiele sind »Heterogene Netze«, Modems sowie »Remote Access«.
- **B 5**: Sicherheit in Anwendungen beschäftigt sich mit den eigentlichen IT-Anwendungen, z. B. E-Mail, Webserver, Faxserver und Datenbanken.

Orthogonal dazu sind eine Reihe von Gefährdungen und Maßnahmen definiert, die in einem oder mehreren Bausteinen Verwendung finden.

Gefahrenkategorien.

Die Gefährdungskataloge sind fünf Kategorien gegliedert:

- **G 1**: Höhere Gewalt
- **G 2**: Organisatorische Mängel
- **G 3**: Menschliche Fehlhandlungen
- **G 4**: Technisches Versagen
- **G 5**: Vorsätzliche Handlungen

Maßnahmenkategorien

Maßnahmen sind wie folgt kategorisiert:

- **M 1**: Infrastruktur[4]
- **M 2**: Organisation
- **M 3**: Personal
- **M 4**: Hard- und Software
- **M 5**: Kommunikation
- **M 6**: Notfallvorsorge

Baustein Datenschutz.

Zusätzlich zu diesen Kategorien wurde mit der Herausgabe eines Bausteins für Datenschutz (B 1.5) jeweils eine weitere Gefahren- (G 6) und Maßnahmenkategorie (M 7) definiert (vgl. Kapitel III.3).

Maßnahmenempfehlungen sind (neben solchen allgemeiner Natur) innerhalb eines Bausteins anhand eines »Lebenszyklus'« des betrachteten Gegenstands strukturiert (vgl. Tab. E.1).

Weiterhin ist für jede Maßnahme eine Qualifikationsstufe definiert, die die Priorisierung der Maßnahme bzgl. einer Zertifizierung nach ISO 27001 (ISO, 2008) angibt. Tab. E.2 erklärt diese Stufen.

[4]Hier wieder im Sinne von baulicher Infrastruktur, vgl. Fußnote 3

Tabelle E.1
Gliederung der Maßnahmen für einen Grundschutz-Baustein nach (BSI, 2010a, Allgemeines→Einstiegskapitel).

Phase	Typische Tätigkeiten
Planung und Konzeption	Definition des Einsatzzwecks Festlegung von Einsatzszenarien Abwägung des Risikopotentials Dokumentation der Einsatzentscheidung Erstellung des Sicherheitskonzepts Festlegung von Richtlinien für den Einsatz
Beschaffung	Festlegung der Anforderungen an zu beschaffende Produkte Auswahl der geeigneten Produkte
Umsetzung	Konzeption und Durchführung des Testbetriebs Installation und Konfiguration entsprechend Sicherheitsrichtlinie Schulung und Sensibilisierung aller Betroffenen
Betrieb	Sicherheitsmaßnahmen für den laufenden Betrieb (z. B. Protokollierung) Kontinuierliche Pflege und Weiterentwicklung Änderungsmanagement Organisation und Durchführung von Wartungsarbeiten Audit
Aussonderung	Entzug von Berechtigungen Entfernen von Datenbeständen und Referenzen auf diese Daten Sichere Entsorgung von Datenträgern
Notfallvorsorge	Konzeption und Organisation der Datensicherung Nutzung von Redundanz zur Erhöhung der Verfügbarkeit Umgang mit Sicherheitsvorfällen Erstellen eines Notfallplans

Stufe	Erklärung
A (Einstieg)	Diese Maßnahmen müssen für alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz (Auditor-Testat »IT-Grundschutz Einstiegsstufe«, Auditor-Testat »IT-Grundschutz Aufbaustufe« und ISO 27001-Zertifikat auf Basis von IT-Grundschutz) umgesetzt sein. Diese Maßnahmen sind essentiell für die Sicherheit innerhalb des betrachteten Bausteins. Sie sind vorrangig umzusetzen.
B (Aufbau)	Diese Maßnahmen müssen für das Auditor-Testat »IT-Grundschutz Aufbaustufe« und für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind besonders wichtig für den Aufbau einer kontrollierbaren Informationssicherheit. Eine zügige Realisierung ist anzustreben.
C (Zertifikat)	Diese Maßnahmen müssen für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind wichtig für die Abrundung der Informationssicherheit. Bei Engpässen können sie zeitlich nachrangig umgesetzt werden.
Z (zusätzlich)	Diese Maßnahmen müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz verbindlich umgesetzt werden. Sie stellen Ergänzungen dar, die vor Allem bei höheren Sicherheitsanforderungen hilfreich sein können.
W (Wissen)	Diese Maßnahmen dienen der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind. Sie müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz geprüft werden.

Tabelle E.2
Qualifikationsstufen der Maßnahmen der BSI Grundschutzkataloge (nach (BSI, 2010a, Einstiegskapitel)).

Literaturverzeichnis

[BITKOM 2009] BITKOM: Cloud Computing - Evolution in der Technik, Revolution im Business / Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Berlin, 2009. – BITCOM Leitfaden

[Breitenstrom u. a. 2008] BREITENSTROM, C. ; BRUNZEL, M. ; KLESSMANN, J.: *Elektronische Safes für Daten und Dokumente*. http://www.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf, Dezember 2008. – Whitepaper: Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS)

[BSI 2004] BSI: *IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten*. https://www.bsi.bund.de/cae/servlet/contentblob/478208/publicationFile/30989/Outsourcing_pdf.pdf, März 2004. – Ergänzung zum Zertifizierungsschema Nr. 1

[BSI 2008a] BSI: Managementsysteme für Informationssicherheit / Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2008. – BSI Standard 100-1

[BSI 2008b] BSI: IT-Grundschutz-Vorgehensweise / Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2008. – BSI Standard 100-2

[BSI 2008c] BSI: Risikoanalyse auf der Basis von IT-Grundschutz / Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2008. – BSI Standard 100-3

[BSI 2008d] BSI: Notfallmanagement / Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2008. – BSI Standard 100-4

[BSI 2010a] BSI: *IT-Grundschutz*. https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/itgrundschutz_node.html, 2010. – Information des Bundesamtes für Sicherheit in der Informationstechnik

[BSI 2010b] BSI: *BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter*. https://www.bsi.bund.de/ContentBSI/Presse

/Pressemitteilungen/Cloud_Computing_28092010.html, September 2010. – ENTWURF

[Cartlidge u. a. 2007] CARTLIDGE, A. ; HANNA, A. ; RUDD, C. ; MACFARLANE, I. ; WINDEBANK, J. ; RANCE, S. ; CARTLIDGE, A. (Hrsg.) ; LILLYCROP, M. (Hrsg.): An Introductionary Overview of ITIL® V3 / Information Technology Service Management Forum (itSMF). 2007. – Leitfaden

[Colman 2006] COLMAN, R.: Service Level Agreements: a Shared Services Cornerstone. In: *CMA Management* (2006), Nr. 5, S. 37–39

[Deeg 2010] DEEG, M.: *Virtualisierung, essenzielles Werkzeug in der IT-Fabrik*. http://www.fuehrungskraefteforum.de/inhalte/2010/cloud/Deeg.pdf, August 2010. – Präsentation Führungskräfteforum »Cloud-Computing — Anwendungsszenarien in der öffentlichen Verwaltung«

[ENISA 2009] ENISA: Cloud Computing: Benefits, risks and recommendations for information security / European Network and Information Security Agency. 2009. – Leitfaden. – http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[Fiedler u. a. 2010] FIEDLER, J. ; PETERS, J. ; SCHUPPAN, T.: Die Neuordnung öffentlicher Verwaltung durch eine Industrialisierung von Verwaltungsprozessen — Bündelungs-, Industrialisierung- und Shared Service-Ansätze bei der öffentlichen Leistungserbringung / ISPRAT. Berlin, 2010. – Projektbericht

[Fischer u. Sterzenbach 2006] FISCHER, T. M. ; STERZENBACH, S.: Controlling von Shared Service Centers — Ergebnisse einer empirischen Studie in deutschen Unternehmen. In: *Zeitschrift für Planung* 17. Jg. (2006), Nr. 1, S. 123–128

[Graudenz u. Schramm] GRAUDENZ, D. ; SCHRAMM, G.: IT-Kooperationen / ISPRAT. – Whitepaper

[Grobauer u. a. 2010] GROBAUER, B. ; WALLOSCHEK, T. ; STÖCKER, E.: Towards a cloud-specific Risk Analysis Framework / Siemens AG. 2010. – Whitepaper

[Groll u. Brodnik 2009] GROLL, B. ; BRODNIK, B.: *Das müssen Behörden beim Outsourcing beachten*. http://www.egovernment-computing.de/systems/articles/184992/, Mai 2009

[Harnisch 2010] HARNISCH, R.: *Virtualisierung im Rechenzentrum*. http://www.fuehrungskraefteforum.de/inhalte/2010/cloud/Harnisch.pdf, August 2010. – Präsentation Führungskräfteforum »Cloud-Computing — Anwendungsszenarien in der öffentlichen Verwaltung«

[Isberner 2010] ISBERNER, K.: Grün, wolkig und (zukunfts-)sicher — Das Rechenzentrum der Zukunft. In: *Datareport* 2 (2010), S. 10–13. – Broschüre des IT-Dienstleisters Dataport

[ISO 2007] ISO: Information technology — Security techniques — Information security risk management — / International Organization for Standardization (ISO). 2007 (ISO/IEC 27005:2007). – Internationaler Standard

[ISO 2008] ISO: Information technology — Security techniques — Information security management systems — Requirements / International Organization for Standardization (ISO). 2008 (ISO/IEC 27001:2008). – Internationaler Standard

[Kammer u. Schulz 2010] KAMMER, M. ; SCHULZ, S. E.: *Öffentliche IT im Wandel — Rechtsfragen von IT-Kooperationen*. 2010. – Arbeitspapier und Diskussionsbeitrag für den ISPRAT-Workshop am 27. September 2010

[Keusekotten 2010] KEUSEKOTTEN, J.: *Kompetenz- und Musterrechenzentrum Green IT im Bundesverwaltungsamt*. http://www.fuehrungskraefte-forum.de/inhalte/2010/datacenter/Keusekotten.pdf, September 2010

[Mell u. Grance 2009] MELL, P. ; GRANCE, T.: The NIST Definition of Cloud Computing / National Institute for Standards and Technology. 2009. – Entwurf (Version 15). – http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[NIST 2002] NIST ; STONEBRUNER, G. (Hrsg.) ; GOGUEN, A. (Hrsg.) ; FERINGA, A. (Hrsg.): Risk Management Guide for Information Technology Systems / National Institute for Standards and Technology. 2002 (800-30). – NIST Special Publication. – http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[NIST 2009] NIST: Recommended Security Controls for Federal Information Systems and Organizations / National Institute of for Standards and Technology. 2009 (800-53 rev 3). – NIST Special Publication. – http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[Open Cloud Manifesto 2009] *Open Cloud Manifesto*. http://www.opencloudmanifesto.org, 2009

[Picot 2003] PICOT, A.: *Die grenzenlose Unternehmung*. Wiesbaden : Gabler, Betriebswirt.-Vlg, 2003

[Reuben 2007] REUBEN, J. S.: A survey on virtual machine security / Helsinki University of Technology. 2007. – Technischer Bericht

[Schieferdecker u. a. 2010] SCHIEFERDECKER, I. ; BARNICKEL, N. ; FLÜGGE, M. ; HAGER, S.: *Vorstudie zur City Data Cloud Berlin*. August 2010

[Schreiber 2004] SCHREIBER, T.: Session Riding — A Widespread Vulnerability in Today's Web Applications / SecureNet GmbH. München, Dezember 2004. – Whitepaper

[Schulz 2010] SCHULZ, S. E.: Organisation des öffentlichen Einkaufs: Grundlagen, rechtliche Rahmenbedingungen und praktische Fallbeispiele. In: *Multimedia und Recht* (2010), S. 75 ff. – Erscheint Anfang 2011

[Schuppan 2006] SCHUPPAN, T.: *Strukturwandel der Verwaltung mit E-Government*. Berlin, 2006

[Schuppan 2007] SCHUPPAN, T.: Accountability Modes for Informatised Public Service Networks. In: *Paper for IRSPM '07*. Potsdam, 2–4 April 2007

[Streitberger u. Ruppel 2009] STREITBERGER, W. ; RUPPEL, A.: Cloud Computing Sicherheit — Schutzziele. Taxonomie. Marktübersicht / Fraunhofer-Institut für Sichere Informationssysteme. Garchingen, September 2009. – Studie

[The Open Group 2009] THE OPEN GROUP: Risk Taxonomy / The Open Group. Reading, Berkshire, United Kingdom, Januar 2009 (C081). – Technical Standard. – http://www.opengroup.org/onlinepubs/9699919899/toc.pdf

[Vaquero u. a. 2009] VAQUERO, L. M. ; RODERO-MERINO, L. ; CACERES, J. ; LINDNER, M.: A break in the clouds: towards a cloud definition. In: *SIGCOMM Comput. Commun. Rev.* 39 (2009), Nr. 1, S. 50–55

[Walther 2006] WALTHER, R.: *Service Level Agreements. Ein methodischer Baustein im Dienstleistungscontrolling*. Saarbrücken : VDM Verlag Dr. Müller, 2006

[Weichert 2010] WEICHERT, T.: *Cloud Computing und Datenschutz*. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de /vortraege/20100618-weichert-cloud-computing.pdf, vgl. auch https://www.datenschutzzentrum.de/cloud-computing/, 2010

Abbildungsverzeichnis

Tabellenverzeichnis