Scott Thiebes

Bachelorarbeit
im Fach Allgemeine Wirtschaftsinformatik

Anforderungen an Cloud-Rechenzentren

Themasteller: Prof. Dr. A. Sunyaev

Vorgelegt in der Bachelorprüfung
im Studiengang Wirtschaftsinformatik
der Wirtschafts- und Sozialwissenschaftlichen Fakultät
der Universität zu Köln

Köln, September 2012

Inhaltsverzeichnis

Abkürzungsverzeichnis IV
Tabellenverzeichnis V
1. Einleitung 1
1.1 Problemstellung 1
1.2 Zielsetzung 2
1.3 Vorgehensweise 3
1.4 Aufbau der Arbeit 4
2. Grundlagen und Voraussetzungen des Cloud-Computing 5
2.1 Definition des Begriffs Cloud-Computing 5
2.1.1 Eigenschaften des Cloud-Computing 6
2.1.2 Dienstleistungsmodelle des Cloud-Computing 7
2.1.3 Verwendungsmodelle des Cloud-Computing 8
2.2 Aufbau moderner Rechenzentren 8
2.2.1 IT-Infrastruktur 9
2.2.2 Energieversorgungs-Infrastruktur und Klimatisierungs-Infrastruktur 10
2.2.3 Eigenschaften von Cloud-Rechenzentren 11
2.3 Fehlendes Vertrauen in Cloud-Computing und Zertifizierungen 12
3. Auswahl existierender Zertifizierungen für Rechenzentren 13
3.1 Suche nach existierenden Rechenzentrums-Zertifizierungen 13
3.1.1 Beschreibung des Vorgehens bei der Suche 13
3.1.2 Ergebnisse der Suche 14
3.2 Eingrenzung der Ergebnisse auf relevante Zertifizierungen 15
3.2.1 Kriterien zur Eingrenzung der Suchergebnisse 15
3.2.2 Ergebnisse der Eingrenzung 16
4. Anforderungen an Cloud-Rechenzentren 18
4.1 Gegenüberstellung existierender Zertifizierungen für Rechenzentren 18
4.1.1 Datacenter Star Audit 18
4.1.2 Service Organization Control 3 Report 19
4.1.3 Trusted Site Infrastructure 21
4.1.4 Uptime Institute’s Tier Certification 23
4.1.5 Gemeinsamkeiten der vorgestellten Zertifizierungen 25
4.1.6 Unterschiede der vorgestellten Zertifizierungen 26

4.2 Allgemeine Anforderungen an moderne Rechenzentren 26
4.2.1 Anforderungen an die Gebäude-Infrastruktur 27
4.2.2 Anforderungen an die Hardware- und Software-Infrastruktur 29
4.2.3 Anforderungen an das Management 30
4.3 Spezifische Anforderungen des Cloud-Computig an Rechenzentren 31
4.3.1 Anforderungen an die Gebäude-Infrastruktur 32
4.3.2 Anforderungen an die Hardware-Infrastruktur 33
4.3.3 Anforderungen an die Software-Infrastruktur 34
4.3.4 Anforderungen an das Management 36
4.4 Kriterien und Richtwerte zur Zertifizierung von Cloud-Rechenzentren 37
4.4.1 Kriterien zur Bewertung der Gebäude-Infrastruktur 37
4.4.2 Kriterien zur Bewertung der Hardware-Infrastruktur 38
4.4.3 Kriterien zur Bewertung der Software-Infrastruktur 39
4.4.4 Kriterien zur Bewertung der Managementmaßnahmen 40
5. Fazit 42
Literaturverzeichnis 44
Anhang 50
Erklärung 51
Lebenslauf 52

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
AICPA	American Institute of Certified Public Accountants
API	Programmschnittstelle
BSI	Bundesamtes für Sicherheit in der Informationstechnik
CICA	Canadian Institute of Chartered Accountants
COTS	Custom-off-the-Shelf
DCSA	Datacenter Star Audit
eco Verband	eco – Verband deutscher Internetwirtschaft e.V.
EDV	Elektronische Datenverarbeitung
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
ITIL	IT Infrastructure Library
LLC	Limited liability company
NEA	Netzersatzanlage
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PDU	Power Distribution Unit
SAS70	Service Organization Auditing Standards Nummer 70
SaaS	Software as a Service
SSAE16	Statements on Standards for Attestation Engagements Nummer 16
SOC	Service Organization Control
TIA-492	-
TSI	Trusted Site Infrastructure
TÜViT	TÜV Informationstechnik GmbH
U.S.	-
USV	Unterbrechungsfreie Stromversorgung
UTI	Uptime Institute
VM	Virtuelle Maschine

Tabellenverzeichnis

Tab. 3-1: Ergebnisse der Eingrenzung der Suchergebnisse..... 17
Tab. A-1: Zusammenfassung der Ergebnisse der Suche nach existierenden Rechenzentrum-Zertifizierungen. 50

1. Einleitung

1.1 Problemstellung

Cloud-Computing ist ein aufstrebendes neues Paradigma in der elektronischen Datenverarbeitung (EDV).[1] Einige sehen darin sogar einen der größten Fortschritte in der Geschichte der EDV.[2] Auch wenn sich noch zeigen muss, ob Cloud-Computing diesen Erwartungen tatsächlich gerecht werden kann, es könnte das Potential besitzen große Teile der IT-Branche zu verändern und zu beeinflussen, wie Computer-Hardware zukünftig gestaltet und beschafft wird.[3] Doch trotz der wachsenden Beliebtheit dieses neuen Paradigmas werden häufig auch Bedenken bezüglich der möglichen Sicherheitsrisiken geäußert, die mit dem Einsatz dieser Technologie einhergehen.[4] Dies ist unter anderem darin begründet, dass für viele Organisationen der ständige Zugriff auf die eigenen IT-Systeme, sowie die Sicherheit und Vertraulichkeit der eigenen Daten mittlerweile unerlässlich ist. So musste beispielsweise ein Anbieter von online Cloud-Speicher im August 2008 schließen, nachdem ein großer Teil der eigenen Kundendaten verloren ging.[5] Für viele Unternehmen ist daher die Frage, ob man Cloud-Computing Anbietern vertrauen sollte von großem Interesse.[6] Hierbei stellt sich zwangsläufig die Frage, wie das Vertrauen potentieller Nutzer in Cloud-Computing erzeugt werden kann. Eine Möglichkeit das Vertrauen potentieller Nutzer in die Cloud-Computing-Dienste der Anbieter zu steigern, ist die Erhöhung der Transparenz.[7] Dies gewinnt auch mit der zunehmenden Wichtigkeit von Cloud-Computing aus wirtschaftlichen Gesichtspunkten in der letzten Zeit weiter an Bedeutung.[8] Durch die Etablierung allgemeiner Standards und das Ausstellen von Zertifikaten kann Transparenz und dadurch Vertrauen

---

[1] Vgl. Sultan (2009), S. 109-110.

[2] Vgl. Marston u. a. (2011), S. 176.

[3] Vgl. Armbrust u. a. (2009), S. 1.

[4] Vgl. Zissis, Lekkas (2010), S. 1.

[5] Vgl. Brodkin (2008).

[6] Vgl. Khan, Malluhi (2010), S. 20.

[7] Vgl. Khan, Malluhi (2010), S. 24-25.

[8] Vgl. Pauley (2010), S. 37.

geschaffen werden.[9] In einigen Ländern ist es ferner obligatorisch die Einhaltung von Standards in Anwendungsbereichen, wie z.B. dem Gesundheitswesen, nachzuweisen.[10]

Innerhalb der Forschung lag der Fokus in der Vergangenheit allerdings mehr auf den Endnutzern der verfügbaren Cloud-Softwaredienste und nicht auf den Anbietern von Cloud-Computing (Cloud-Anbieter) und den Anbietern der Cloud-Softwaredienste (Cloud-Nutzer).[11] So gibt es derzeit keinen einheitlichen Zertifizierungsstandard für Cloud-Computing und einige Zertifizierungen, die die besonderen Anforderungen an Rechenzentren durch Cloud-Computing nur teilweise berücksichtigen.[12] Die Entwicklung eines einheitlichen Standards erscheint folglich notwendig. Dieser muss die Besonderheiten des Cloud-Computing berücksichtigen und die Bedenken potentieller Nutzer adressieren, um das Vertrauen in diese neue Technologie zu festigen. Diese Arbeit widmet sich daher der Frage nach Anforderungen an Cloud-Rechenzentren.

1.2 Zielsetzung

Das Ziel dieser Arbeit ist es, Kriterien und Richtwerte vorzuschlagen, die bei der Entwicklung eines Standards zur Zertifizierung von Cloud-Rechenzentren eingesetzt werden können.

Hierzu sollen allgemeine Anforderungen an heutige Rechenzentren identifiziert und erarbeitet werden. Zudem sollen bereits verfügbare Zertifizierungen untersucht und daraus allgemeine Zertifizierungskriterien abgeleitet werden. Weiterhin soll aufgezeigt werden, welche Anforderungen das Bereitstellen von Cloud-Dienstleistungen im Speziellen an die Rechenzentren der Cloud-Anbieter stellt. Anhand der ermittelten Zertifizierungskriterien und der erarbeiteten, Cloud-Computing spezifischen Anforderungen an Rechenzentren, soll aufgezeigt werden, welche Anforderungen durch vorhandene Zertifizierungen bereits abgedeckt werden und welche nicht.

---

[9] Vgl. Khan, Malluhi (2010), S. 24-25.

[10] Vgl. Armbrust u. a. (2009), S. 15.

[11] Vgl. Armbrust u. a. (2009), S. 1.

[12] Vgl. zu diesem und dem nächsten Satz Welz (2012), S. 3-4; Hansel (2012), S. 12; Reilly (2011), S. 14; Ho (2011):

1.3 Vorgehensweise

Die in dieser Arbeit vorgenommene Erarbeitung von Kriterien und Richtwerten zur Berücksichtigung bei der Standardisierung von Zertifizierungen für Cloud-Rechenzentren geschieht auf Basis einer Gegenüberstellung von bereits vorhandenen Zertifizierungen für Rechenzentren. Hierzu wird zunächst nach existierenden Rechenzentrums-Zertifizierungen gesucht und in Abhängigkeit von der Auswertung der Suchergebnisse eine Auswahl von drei bis fünf Zertifizierungen getroffen, um diese im Anschluss detailliert untersuchen zu können. Die detaillierte Betrachtung einiger weniger Zertifizierung wird hierbei einer ganzheitlichen, aber oberflächlichen Betrachtung vieler Zertifizierungen vorgezogen. Eine genauere Beschreibung des Such- und Auswahlprozesses existierender Zertifizierungen erfolgt im dritten Kapitel dieser Arbeit.

Ausgehend von einer Gegenüberstellung der ausgewählten Zertifizierungen werden allgemeine Anforderungen an heutige Rechenzentren abgeleitet. Dabei erfolgt die Gegenüberstellung der Zertifizierungen, entsprechend der Hauptbestandteile eines Rechenzentrums (RZ), in den Kategorien Gebäude-Infrastruktur-Anforderungen, Hardware-Infrastruktur-Anforderungen, Software-Infrastruktur-Anforderungen und Management-Anforderungen. Hierzu sind die Charakteristika des Gebäudes, der Rechenzentrumsumgebung, der Energieversorgung und der Klimatisierung eines Rechenzentrums zu der Kategorie Gebäude-Infrastruktur-Anforderungen zusammengefasst. Wegen der möglichen Komplexität und der Bedeutung der IT-Infrastruktur für den Betrieb eines Rechenzentrums, wird diese getrennt in den Kategorien Hardware-Infrastruktur-Anforderungen und Software-Infrastruktur-Anforderungen betrachtet. Da mit der zunehmenden Komplexität von Rechenzentren eine Reihe von möglichen Problemen und Herausforderungen im Bezug ihr Management verbunden sind, erfolgt zusätzlich auch ein Vergleich der Zertifizierungen in der Kategorie Management-Anforderungen.[13] Die so erhaltenen Anforderungen werden dahingehend analysiert, inwieweit sie die speziellen Anforderungen Cloud-Rechenzentren bereits berücksichtigen und welche Anforderungen noch nicht

[13] Vgl. Kant (2009), S. 2951.

berücksichtigt werden. Abschließend werden Kriterien und Richtwerte zur Realisierung der erarbeiteten Anforderungen diskutiert.

1.4 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in zwei Teile. Im ersten Teil werden die nötigen Grundlagen erarbeitet, wohingegen im zweiten Teil die Kriterien und Richtwerte zur für die Standardisierung der Zertifizierung von Cloud-Rechenzentren erarbeitet werden.

Die Grundlagen werden dabei in zwei weitere Teile untergliedert, welche die Kapitel zwei und drei dieser Arbeit darstellen. In Kapitel zwei wird zunächst der Begriff des Cloud-Computing definiert und näher auf dessen Besonderheiten eingegangen. Anschließend wird der Begriff Rechenzentrum definiert und der Aufbau moderner Rechenzentren beschrieben. Darauf aufbauend wird ebenfalls der Begriff Cloud-Rechenzentrum abgegrenzt und kurz erläutert weshalb es für den Betrieb von Cloud-Computing spezielle Rechenzentren geben muss. Das Kapitel schließt mit einer Erläuterung der Bedeutung eines Zertifizierungsstandards für Cloud-Rechenzentren. Kapitel drei beschreibt das Vorgehen bei der Suche nach existierenden Zertifizierungen für Rechenzentren und den anschließenden Auswahlprozess zur Eingrenzung der Ergebnisse auf relevante Zertifizierungen. Das vierte Kapitel bildet den Hauptteil der vorliegenden Arbeit. Die ausgewählten Zertifizierungen werden zunächst gegenübergestellt und auf Gemeinsamkeiten und Unterschiede untersucht. Anschließend werden allgemeine Anforderungen an Rechenzentren abgeleitet. Darauf aufbauend werden anhand häufig genannter Bedenken potentieller Cloud-Nutzer und der zuvor identifizierten allgemeinen Anforderungen an Rechenzentren die Anforderungen an Cloud-Rechenzentren abgeleitet. Das Kapitel schließt mit der Herleitung konkreter Kriterien und Richtwerte für die Standardisierung der Zertifizierung von Cloud-Rechenzentren. Das fünfte Kapitel reflektiert kritisch die Vorgehensweise in dieser Arbeit, sowie die dadurch erhaltenen Ergebnisse und liefert mögliche Ansatzpunkte für, weitere Forschung.

2. Grundlagen und Voraussetzungen des Cloud-Computing

2.1 Definition des Begriffs Cloud-Computing

Cloud-Computing ist ein aufstrebendes Paradigma in der EDV.[14] Aufgrund der potentiellen wirtschaftlichen und technischen Vorteile hat Cloud-Computing jüngst viel Aufmerksamkeit in der Öffentlichkeit und Wissenschaft erhalten.[15] Allerdings herrscht oft Unklarheit darüber, was Cloud-Computing ist und wozu es gut ist.[16] Innerhalb der Fachliteratur existieren daher viele unterschiedliche Definitionen des Begriffs Cloud-Computing,[17] die sich teilweise überschneiden. So nennen Yang und Tate neun verschiedene Definitionen von Cloud-Computing, welche Sie in einem Literaturreview ermittelt haben.[18] Aufgrund ihrer aktuellen Popularität innerhalb der Fachliteratur,[19] wird in dieser Arbeit die Definition des National Institutes of Standards and Technology (NIST), der U.S. Amerikanischen Behörde für Standardisierungsprozesse, zugrunde gelegt. Sie versteht unter Cloud-Computing ein Modell, das allgegenwärtigen, einfachen und bedarfsgerechten Zugriff auf eine gemeinsam genutzte Menge konfigurierbarer IT-Ressourcen über ein Netzwerk ermöglicht.[20] IT-Ressourcen sind zum Beispiel Netzwerke, Server, Sekundärspeicher und Anwendungen. Sie können innerhalb kürzester Zeit, mit geringem Aufwand und zumeist ohne manuelles Eingreifen des Cloud-Anbieters in Anspruch genommen und wieder freigegeben werden. Zu den Treibern des Cloud-Computing gehört sowohl die immer größere Verfügbarkeit höherer Netzwerkbandbreiten,[21] als auch die Entwicklung von Technologien, wie Virtualisierungssoftware, Mandantenfähigkeit und Web-Services.[22] Darüber hinaus nennen Mell und Grance (2009) fünf grundlegende Eigenschaften,

---

[14] Vgl. Sultan (2009), S. 109-110.

[15] Vgl. Yang, Tate (2012), S. 36.

[16] Vgl. Armbrust u. a. (2009), S. 3.

[17] Vgl. Sultan (2010), S. 110.

[18] Vgl. Yang, Tate (2012), S. 37.

[19] Vgl. Yang, Tate (2012), S. 36.

[20] Vgl. zu diesem und den nächsten beiden Sätzen Mell, Grance (2009), S. 2.

[21] Vgl. Dwivedi, Mustafee (2010), S. 676.

[22] Vgl. Marston u. a. (2011), S. 178.

sowie drei Dienstleistungsmodelle und vier unterschiedliche Verwendungsmodelle des Cloud-Computing, die im Folgenden erläutert werden.

2.1.1 Eigenschaften des Cloud-Computing

Die fünf, durch Mell und Grance (2009) festgestellten, grundlegenden Eigenschaften des Cloud-Computing sind der On-Demand-Self-Service, ein umfassender Netzwerkzugriff, die Ressourcenteilung, eine kurzfristige Elastizität und die Messbarkeit des Dienstes.[23] On-Demand-Self-Service bedeutet dabei, dass Cloud-Nutzer IT-Ressourcen je nach Bedarf und selbstständig in Anspruch nehmen können. Eingriffe durch Mitarbeiter des Cloud-Anbieters sind dazu nicht erforderlich. Unter einem umfassenden Netzwerkzugriff versteht man weiterhin, dass der Zugriff auf die beanspruchten Ressourcen über standard Netzwerk-Technologien und von beliebigen Geräten aus erfolgen kann. Die Eigenschaft der Ressourcenteilung des Cloud-Computing bedeutet, dass die durch den Cloud-Anbieter bereitgestellten Ressourcen in Form eines sogenannten Mehr-Benutzer-Modells mehreren Cloud-Nutzern gleichzeitig zur Verfügung gestellt und den einzelnen Nutzern je nach Bedarf dynamisch zugewiesen werden. Dabei haben die einzelnen Cloud-Nutzer in der Regel keinen weiteren Einfluss auf den exakten Standort der von ihnen genutzten Ressourcen. Durch eine kurzfristige Elastizität ermöglicht es Cloud-Computing außerdem, dass die durch den Cloud-Nutzer in Anspruch genommenen Ressourcen dem Bedarf entsprechend und in manchen Fällen automatisch hoch und herunter skaliert werden. Die verfügbaren Ressourcen erscheinen aus der Sicht des Nutzers dabei fast unbegrenzt und können zu jeder Zeit dem maximalen Bedarf der Nutzer gerecht werden. Die Messbarkeit des Dienstes bedeutet ferner, dass Cloud-Computing-Systeme die Ressourcennutzung kontrollieren und automatisch optimieren. Die Nutzung der verfügbaren Ressourcen ist zudem kontrollierbar und nachvollziehbar, was für Tranzparenz auf Seiten der Anbieter und Nutzer sorgt.

---

[23] Vgl. zu diesem Kapitel Mell, Grance (2009), S. 2.

2.1.2 Dienstleistungsmodelle des Cloud-Computing

Zusätzlich zu den zuvor erläuterten fünf zentralen Eigenschaften des Cloud-Computing, definieren Mell und Grance (2009) drei unterschiedliche Diensleistungsmodelle, die jeweils verschiedene Ausprägungen des Cloud-Computing darstellen.[24] Sie bauen aufeinander auf und bieten in der genannten Reihenfolge aus Sicht der Konsumenten jeweils einen höheren Grad an Abstraktion. Die drei Diensleistungsmodelle sind Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Bei dem IaaS-Dienstleistungsmodell stellt der Cloud-Anbieter dem Cloud-Nutzer Rechenleistung, Speicher, Netzwerke und andere fundamentale IT-Ressourcen bereit, auf denen er beliebige Anwendungen betreiben kann. Dazu zählen je nach Anbieter und Angebot auch Betriebssysteme und andere Systemsoftware. Der Konsument besitzt keine direkte Kontrolle über die Cloud-Infrastruktur[25], aber über das Betriebssystem, Speicher und die eingesetzten Anwendungen. Beim PaaS-Dienstleistungsmodell stellt der Cloud-Anbieter dem Cloud-Nutzer die Möglichkeit bereit eigene oder selbst erworbene Anwendungen auf der Cloud-Infrastruktur des Anbieters zu betreiben. Dazu werden spezielle Programmiersprachen, Bibliotheken, Dienste und Werkzeuge durch den Cloud-Anbieter zur Verfügung gestellt. Der Konsument besitzt keine Möglichkeit die Cloud-Infrastruktur zu verwalten. Er besitzt jedoch die vollständige Kontrolle über die eigenen beziehungsweise die erworbenen Anwendungen. Beim SaaS-Dienstleistungsmodell stellt der Cloud-Anbieter dem Cloud-Nutzer spezielle Anwendungen bereit, die auf der eigenen Cloud-Infrastruktur betrieben und durch den Cloud-Anbieter verwaltet und aktualisiert werden. Die Anwendungen sind hierbei per Netzwerkzugriff erreichbar. Der Konsument besitzt keine Möglichkeit die Cloud-Infrastruktur zu verwalten. Möglichwerweise besitzt er eingeschränkte Konfigurationsmöglichkeiten bezüglich der verwendeten Anwendungen, die sich jedoch nur auf sich selbst und keine anderen Konsumenten der Anwendungen auswirken.

---

[24] Vgl. zu diesem Kapitel Mell, Grance (2009), S. 2-3.

[25] Cloud-Infrastruktur bezeichnet die gesamte Hardware und Software in Rechenzentren, die den Betrieb von Cloud-Computing ermöglicht.

2.1.3 Verwendungsmodelle des Cloud-Computing

Schließlich unterscheiden Mell und Grance (2009) auch vier verschiedene Verwendungsmodelle des Cloud-Computing.[26] Diese sind Private-Cloud, Community-Cloud, Public-Cloud und Hybrid-Cloud. Bei dem Private-Cloud-Verwendungsmodell steht die Cloud-Infrastruktur exklusiv zur Nutzung durch eine einzelne Organisation zur Verfügung. Die Cloud-Infrastruktur kann dabei durch die Organisation selbst, einen Drittanbieter oder eine Kombination aus diesen Beiden betrieben werden. Im Gegensatz dazu steht die Cloud-Infrastruktur beim Community-Cloud-Verwendungsmodell zur exklusiven Nutzung durch eine festgelegte Gruppe von Organisationen zur Verfügung.
Beim Public-Cloud-Verwendungsmodell steht die Cloud-Infrastruktur der allgemeinen Öffentlichkeit zur Verfügung. Sie wird durch ein Unternehmen, eine akademische oder staatliche Organisation und in organisationseigenen Räumlichkeiten, den Cloud-Rechenzentren, betrieben. Das Hybrid-Cloud-Verwendungsmodell stellt eine Mischform von zwei oder mehr der oben genannten Verwendungsmodelle dar.

2.2 Aufbau moderner Rechenzentren

Moderne Rechenzentren bilden die Grundlage für eine Reihe von Internetdiensten und insbesondere auch für Cloud-Computing.[27] Traditionell wird unter einem Rechenzentrum eine Menge von mehreren Servern und Netzwerkgeräten verstanden, die aufgrund ähnlicher Umwelt- und Sicherheitsanforderungen, sowie zur einfacheren Wartung in einem gemeinsamen Gebäude betrieben werden.[28] Rechenzentren bestehen im Allgemeinen aus vier Grundbestandteilen. Das sind die Gebäude, in denen sich die gesamte Hardware, weitere Geräte und die Sicherheitsanlagen zum Schutz der Geräte befinden, die IT-Infrastruktur, die Energieversorgungs-Infrastruktur und die Klimatisierungs-Infrastruktur.[29] Im Folgenden werden die für diese Arbeit relevanten Bestandteile erläutert.

---

[26] Vgl. zu diesem Kapitel Mell, Grance (2009), S. 3.

[27] Vgl. Kant (2009), S. 2939.

[28] Vgl. Barroso, Hölzle (2009), S. 2.

[29] Vgl. Marwah u. a. (2010), S. 64; Barroso, Hölzle (2009), S. 2.

2.2.1 IT-Infrastruktur

In dieser Arbeit wird IT-Infrastruktur eines Rechenzentrums als die gesamte Hardware und Software, die zum Betrieb eines Rechenzentrums notwendig ist definiert. Sie lässt sich daher weiter unterteilen in die Hardware-Infrastruktur und die Software-Infrastruktur.

Die Hauptbestandteile der Hardware-Infrastruktur sind die Server-Hardware, sowie sämtliche Netzwerkgeräte und Sekundärspeicher-Komponenten.[30] Die eingesetzte Hardware kann sich dabei von Rechenzentrum zu Rechenzentrum stark unterscheiden,[31] ist innerhalb der einzelnen Rechenzentren aber in der Regel homogen.[32] Server bestehen aus einem oder mehreren Prozessoren, einem Hauptspeicher, einer Netzwerkschnittstelle und einem schnellen lokalen Sekundärspeicher.[33] Sie werden in sogenannten Racks angeordnet. Im einfachsten Fall sind Racks Metallgehäuse,[34] die bis zu 42 Server aufnehmen können.[35] Zusätzlich können sie auch mit einem eigenen Stromverteiler, Kühlsystemen und weiteren Geräten zur Verwaltung und Steuerung der Server ausgestattet sein. Einige tausend Racks werden wiederum zu sogenannten Clustern zusammengefasst.[36]

Die Software-Infrastruktur eines Rechenzentrums lässt sich in drei aufeinander aufbauende Ebenen einteilen.[37] Die unterste Ebene bildet die Platform-Level-Software. Software auf dieser Ebene dient dem Betrieb einzelner Server und zur Abstraktion der Server-Hardware gegenüber den darüber liegenden Software-Ebenen. Dazu zählen beispielsweise die Betriebssysteme der Server. Auf der nächst höheren Ebene folgt die Cluster-Level-Infrastruktur. Die Software auf dieser Ebene verwaltet Ressourcen und

---

[30] Vgl. Barroso, Hölzle (2009), S. 31.

[31] Vgl. Barroso, Hölzle (2009), S. 5.

[32] Vgl. Barroso, Hölzle (2009), S.92.

[33] Vgl. zu diesem und dem nächsten Satz Abts, Feldermann (2012), S. 44.

[34] Vgl. Kant (2009), S. 2940.

[35] Vgl. Patel, Shah (2005), S. 4.

[36] Vgl. Abts, Felderman (2012), S. 44.

[37] Vgl. zum nächsten Absatz Barroso, Hölzle (2009), S. 13.

liefert Dienste auf der Cluster-Ebene. Die oberste Ebene bildet die Application-Level-Software. Software auf dieser Ebene stellt die Dienste des Rechenzentrums bereit, welche durch die Cloud-Nutzer in Anspruch genommen werden können.

2.2.2 Energieversorgungs-Infrastruktur und Klimatisierungs-Infrastruktur

Die Energieversorgungs-Infrastruktur liefert den Strom für das Gebäude und die Geräte in einem Rechenzentrum. Sie ist dafür zuständig eine kontinuierliche und gleichmäßige Stromzufuhr für die Hardware-Infrastruktur zu gewährleisten.[38] Die Energieversorgungs-Infrastruktur besteht aus mehreren Schichten, durch die der Strom zu den einzelnen Racks geleitet wird.[39] Dabei durchfließt er Transformatoren und Lastumschalter, die unterbrechungsfreie Stromversorgung (USV) und die sogenannte ‚Power Distribution Unit' (PDU). Die USV stellt eine ununterbrochene Stromzufuhr in das System sicher.[40] Sie kann im Falle einer Störung der Hauptenergiequelle das Rechenzentrum kurzfristig auch weiterhin mit Strom versorgen. Die PDU verteilt den Strom von der USV zu den einzelnen Racks.

Rechenzentren haben einen großen Energiebedarf und waren 2006 für etwa 1,5% des gesamten Energiebedarfs der USA verantwortlich.[41] Da die Energiekosten einen großen Anteil an den Gesamtkosten des Betriebs eines Rechenzentrums einnehmen, ist die Gestaltung der Energieversorgungs-Infrastruktur ein wichtiger Faktor beim Entwurf moderner Rechenzentren.[42] Weiterhin sind auch die lokalen Energiekosten ein wichtiger Faktor bei der Wahl des Standortes für ein Rechenzentrum.[43]

Die Klimatisierungs-Infrastruktur eines Rechenzentrums ist für die Kühlung der Hardware-Infrastruktur verantwortlich. Je nach Aufbau der Rechenzentren kann sie

---

[38] Vgl. Marwah u. a. (2010), S. 64.

[39] Vgl. zu diesem und dem nächsten Satz Marwah u. a. (2010), S. 65.

[40] Vgl. zu diesem und den nächsten beiden Sätzen Kant (2009), S. 2941.

[41] Vgl. zu diesem und dem nächsten Satz Woods (2010), S. 36.

[42] Vgl. Barroso, Hölzle (2009), S. 10.

[43] Vgl. Armbrust u. a. (2009), S. 6.

komplex und kostenintensiv sein.[44] Mehr als 20% des gesamten Energiebedarfs von Rechenzentren werden beispielsweise zur Kühlung aufgewendet.[45] Dabei kann die Hardware durch zwei Arten gekühlt werden, per Luft- oder per Wasser-Kühlung. Ein Vorteil der Wasser-Kühlung ist, dass sie effektiver als die Kühlung durch Luft ist.[46] Allerdings besteht bei der Kühlung mit Wasser grundsätzlich eine größere Ausfallgefahr der Hardware, sollte durch eine Beschädigung austretendes Wasser die Hardware schädigen.

2.2.3 Eigenschaften von Cloud-Rechenzentren

Der zuvor beschriebene Aufbau moderner Rechenzentren trifft sowohl auf herkömmliche Rechenzentren, als auch auf Cloud-Rechenzentren zu. Darüber hinaus besitzen Cloud-Rechenzentren jedoch auch einige besondere Eigenschaften. Cloud-Rechenzentren sind sehr große und aus handelsüblicher Server-Hardware bestehende Rechenzentren,[47] die bis zu einige Millionen Server umfassen können.[48] Diese große Anzahl von Servern ist hierbei notwendig, um die Elastizität des Dienstes und den Anschein unendlicher Ressourcen zu gewährleisten.[49] In Cloud-Rechenzentren wird zudem die gesamte IT-Infrastruktur des Rechenzentrums als ein einziges System betrachtet, um eine effiziente und leistungsfähige Dienstleistung bereitstellen zu können.[50] Aufgrund ihrer Größe und der Betrachtung als eine einzige Einheit bezeichnen Barroso und Hölzle (2009) solche Rechenzentren auch als Warehouse Scale Computer, also Computer vom Ausmaß eines Lagerhauses. Wegen der, aus Sicht des Verfassers, fehlenden Präzision des Begriffs und dem Fokus des vorliegenden Forschungsvorhabens wird im Folgenden jedoch weiterhin der Begriff Cloud-Rechenzentrum verwendet.

---

[44] Vgl. Kant (2009), S. 2941.

[45] Vgl. zu diesem und dem nächsten Satz Woods (2010), S. 36.

[46] Vgl. zu diesem und dem nächsten Satz Woods (2010), S. 38.

[47] Vgl. Armbrust u. a. (2009), S. 1-2.

[48] Vgl. Yang, Tate (2012), S. 39.

[49] Vgl. Armbrust u. a. (2009), S. 5.

[50] Vgl. zu diesem und dem nächsten Satz Barroso, Hölzle (2009), S. vi.

2.3 Fehlendes Vertrauen in Cloud-Computing und Zertifizierungen

Cloud-Computing ist eine Form des IT-Outsourcings.[51] Wie bei jeder Form des Outsourcings gehen auch mit Cloud-Computing Risiken einher.[52] Trotz der möglichen wirtschaftlichen und technischen Vorteile die der Einsatz von Cloud-Computing mit sich bringen kann, werden daher immer wieder auch Bedenken gegenüber dieser neuen Technologie geäußert.[53] Zu den häufigsten genannten Bedenken zählen die Fragen nach der Sicherheit, Verfügbarkeit und Übertragbarkeit der angebotenen Cloud-Computing-Dienste. Dabei besteht die geäußerte Skepsis zumeist nicht gegenüber den Absichten der Cloud-Anbieter sondern gegenüber der Technologie Cloud-Computing und deren Fähigkeiten.[54] Es existieren verschiedene Möglichkeiten das Vertrauen potentieller Nutzer in Cloud-Computing zu stärken.[55] Khan und Malluhi nennen als eine Möglichkeit, für Transparenz auf Seiten der Cloud-Anbieter zu sorgen.[56] Transparenz und somit Vertrauen potentieller Cloud-Nutzer in Cloud-Computing-Dienste kann dabei durch Zertifizierungen erzeugt werden. Sie signalisieren gegenüber den potentiellen Nutzern die Einhaltung der Zertifizierungskriterien und bieten darüber hinaus auch einen einheitlichen Maßstab zur Bewertung verschiedener Cloud-Anbieter.

---

[51] Vgl. Clemons, Chen (2011), S. 8.

[52] Vgl. Clemons, Chen (2011), S. 3.

[53] Vgl. zu diesem und dem nächsten Satz Sultan (2010), S. 115.

[54] Vgl. Khan, Malluhi (2010), S. 20.

[55] Vgl. zu diesem und dem nächsten Satz Khan, Malluhi (2010), S. 20-21.

[56] Vgl. Khan, Malluhi (2010), S. 25.

3. Auswahl existierender Zertifizierungen für Rechenzentren

3.1 Suche nach existierenden Rechenzentrums-Zertifizierungen

Zur Herleitung allgemeiner Anforderungen an heutige Rechenzentren sollen in dieser Arbeit drei bis fünf Zertifizierungen für Rechenzentren gegenüber gestellt und auf Gemeinsamkeiten und Unterschiede hin untersucht werden. Die Suche nach bereits existierenden Rechenzentrum-Zertifizierungen erfolgte hierzu in drei Schritten, die im Folgenden erläutert werden.

3.1.1 Beschreibung des Vorgehens bei der Suche

In einem ersten Schritt wurde nach Artikeln in wissenschaftlichen Zeitschriften gesucht, die entweder konkret eine Zertifizierung für Rechenzentren oder ganz allgemein die Zertifizierung von Rechenzentren betrachteten. Dabei wurden auch solche Artikel berücksichtigt, die sich nicht auf Zertifizierung von Rechenzentren konzentrierten. Eine Bewertung der Ergebnisse anhand der gefundenen Artikel sollte nicht stattfinden. Die Suche erfolgte zunächst in den Online-Katalogen von EBSCOhost, Proquest (ABI/INFORM), Association for Computing Machinery (ACM) Digital Library und Institute of Electrical and Electronics Engineers (IEEE) Computer Society Digital Library unter Verwendung der Suchbegriffe ‚data center', ‚data center certification', ‚datacenter certification', ‚data center audit' und ‚data center auditing'. Die Ergebnisse wurden hierbei auf einen Zeitraum nach 1990 und geprüfte Beiträge eingegrenzt. Eine Eingrenzung auf Beiträge nach 1990 erscheint dabei wegen der schnellen Entwicklung innerhalb der IT-Branche und der damit verbundenen Entwicklung von Rechenzentren als sinnvoll. Weiterhin wurde unter Verwendung der Begriffe ‚Rechenzentrum', ‚Rechenzentrum Zertifizierung' und ‚Rechenzentrums Audit' in der Online-Datenbank von Wiso-net gesucht. Die Ergebnisse wurden auf Beiträge in Fachzeitrschriften begrenzt. Das Ziel dieses Schrittes war es, eine erste Übersicht über mögliche Zertifizierungen zu erhalten.

In dem darauffolgenden Schritt wurde die Suche schließlich von Suchseiten, welche sich auf wissenschaftliche Beiträge spezialisiert haben, auf allgemeine Suchseiten erweitert. Die Suche wurde mit den Begriffen ‚data center certification', ‚data center audit', ‚Rechenzentrum Zertifizierung' und ‚Rechenzentrums Audit' jeweils auf den

englischen und deutschen Seiten von Google, Bing und Yahoo durchgeführt. Die Auswahl allgemeiner Suchseiten wurde dabei auf diese drei begrenzt, da sie die meist verwendeten allgemeinen Suchseiten im deutsch- und englischsprachigen Raum sind.[57] Aufgrund der hohen Anzahl von Suchergebnissen wurden pro Suchmaschine und Suchbegriff jeweils nur die ersten fünfzig Ergebnisse zur der weiteren Betrachtung berücksichtigt. Das Ziel dieses Schrittes war es, weitere Zertifizierungen für Rechenzentren zu finden.

Im dritten und letzten Schritt wurden die Webseiten der Rechenzentrum-Betreiber daraufhin untersucht, ob und welche Zertifizierungen sie für ihre Rechenzentren aufführen. Ziel war das Auffinden weiterer Zertifizierungen und die Bestätigung der bisherigen Suchergebnisse.

3.1.2 Ergebnisse der Suche

Die Suche lieferte insgesamt 13 Zertifizierungen bzw. Standards, die im Zusammenhang mit Rechenzentren stehen. Sie sind in Tabelle A-1 des Anhangs zusammengefasst. Die Recherche innerhalb der Fachliteratur über die Online-Kataloge von Ebsco, Proquest (ABI/INFORM), ACM Digital Library und IEEE Computer Society Digital Library brachte als erste Ergebnisse die beiden Standards Service Organization Auditing Standards Nummer 70 (SAS70) und Service Organization Control 3 (SOC3) Report. Die beiden Zertifizierungen Trusted Site Infrastructure (TSI) und Telecommunications Infrastructure Standards for Data Centers (TIA-492) sind das Ergebnis der Suche in der Online-Datenbank Wiso-net.

Die Suche in den allgemeinen Suchmaschinen lieferte neun weitere Ergebnisse, darunter auch das Datacenter Star Audit (DCSA) und die Tier Certification des Uptime Institutes (UTI). Eine Betrachtung der Suchergebnisse der Suchmaschinen Bing und Yahoo zeigte hierbei, dass die Ergebnisse zu großen Teilen übereinstimmen. Eine weitere Recherche in dieser Hinsicht zeigte, dass dies darin begründet ist dass beide Seiten seit dem Jahr 2009 den gleichen Suchalgorithmus verwenden.[58] Es zeigte sich

[57] Vgl. Alexa Internet, Inc. (2012).

[58] Vgl. BBC NEWS (2009).

außerdem, dass bei der Suche nach dem Begriff ‚data center certification' auf den englischsprachigen Suchseiten der obigen Anbieter zumeist Zertifizierungen in Form von Mitarbeiterqualifikationen für Rechenzentrum-Personal aufgeführt wurden.

Durch die weiteren Untersuchungen der Webseiten von Rechenzentrum-Betreibern konnten keine weiteren Zertifizierungen ermittelt werden. Allerdings bestätigten sie einige Ergebnisse der ersten beiden Schritte, wie z.B. die Tier Certification des UTI.

3.2 Eingrenzung der Ergebnisse auf relevante Zertifizierungen

Da bei der Suche zunächst eine erste oberflächliche Begutachtung der gefundenen Zertifizierungen und Standards erfolgte, ist es notwendig diese genauer zu untersuchen. Dabei gilt es festzustellen, ob sie für das vorliegende Forschungsvorhaben relevant sind oder nicht. Aufgrund des begrenzten Umfangs der Arbeit erfolgt eine Eingrenzung der zu untersuchenden Zertifizierungen auf maximal fünf Zertifizierungen. Die Evaluierung und Eingrenzung wurde hierbei anhand von sechs Kriterien vorgenommen, die nach Ansicht des Verfassers dazu beitragen, die Eignung der Suchergebnisse zu beurteilen. Sie werden im Folgenden erläutert.

3.2.1 Kriterien zur Eingrenzung der Suchergebnisse

Zunächst wird geprüft, ob es sich bei den gefundenen Zertifizierungen um Zertifizierungen oder Standards für Rechenzentren handelt. Erfüllt eine Zertifizierung dieses Kriterium nicht, wird sie nicht weiter berücksichtigt, da sie in diesem Fall für den Gegenstand der vorliegenden Arbeit nicht weiter relevant ist. Anschließend wird untersucht, ob die Zertifizierung auf Standards nach ISO/DIN zurückgreift. Die Anwendung etablierter Standards nach ISO/DIN wird im Rahmen dieser Arbeit grundsätzlich als ein positives Zeichen und Qualitätsmerkmal einer Zertifizierung gewertet. Um jedoch ein gewisses Maß an Diversität zu erreichen, wird bei der Auswahl der Zertifizierungen darauf geachtet, dass nicht alle Zertifizierungen auf den gleichen Standards beruhen. Das Fehlen etablierter Standards ist daher kein generelles Ausschlusskriterium für eine der gefundenen Zertifizierungen. Weiterhin wird überprüft, ob bereits zertifizierte Rechenzentren aufgelistet werden. Die Auflistung bereits zertifizierter Rechenzentren wird hierbei als positives Indiz für die Verbreitung

einer Zertifizierung gewertet. Da in der vorliegenden Arbeit allgemeine Kriterien zur Zertifizierung von Rechenzentren hergeleitet werden sollen, werden Zertifizierungen mit einer weiten Verbreitung solchen mit einer geringen Verbreitung vorgezogen. Darauf aufbauend werden die zertifizierten Rechenzentren dahingehend untersucht, ob sich unter ihnen bedeutende oder staatliche Organisationen befinden. Die Zertifizierung bedeutender (dazu zählen beispielsweise große Wirtschaftsunternehmen) oder staatlicher Organisationen wird als weiterer Qualitätsindikator einer Zertifizierung gewertet, da diese zumeist besonders hohe Anforderungen an die eingesetzte IT-Infrastruktur stellen. Zertifizierungen mit entsprechend aufgeführten Rechenzentren werden anderen bei der Auswahl vorgezogen. Das fünfte Kriterium prüft des Weiteren, ob die ausgestellten Zertifikate dauerhaft gültig sind oder regelmäßig erneuert werden müssen. Aufgrund der schnellen Entwicklung innerhalb der IT-Branche scheinen dauerhafte Zertifizierungen nicht sinnvoll. Zertifizierungen mit einer Gültigkeitsdauer von zwei Jahren oder weniger werden daher bei der Auswahl bevorzugt. Abschließend wird festgestellt, ob die Zertifizierungskriterien frei verfügbar sind oder nicht und ob es ggf. eine Kontaktmöglichkeit gibt. Zertifizierungen, deren Kriterienkataloge nicht vorliegen, können nicht weiter berücksichtigt werden, da diese Informationen essentiell für eine Gegenüberstellung und das Ableiten allgemeiner Anforderungen an Rechenzentren sind. Gibt es eine Kontaktmöglichkeit, wurde diese wahrgenommen, um möglicherweise auf diesem Wege die Kriterienkataloge zu erhalten. War die Kontaktaufnahme ebenfalls ohne Erfolg, wurden die betroffenen Zertifizierungen verworfen.

3.2.2 Ergebnisse der Eingrenzung

Eine genauere Untersuchung der gefundenen Suchergebnisse zeigte dass insgesamt vier der 13 Ergebnisse nicht von Bedeutung für die Zertifizierung von Rechenzentren sind. Es handelte sich z.B. um Zertifizierungen zur Bewertung der Energieeffizienz von Gebäuden oder um Standards der Kreditkartenindustrie. Sie wurden daher bei der weiteren Betrachtung nicht mehr berücksichtigt. Ebenfalls wurde eine Zertifizierung aus der Betrachtung genommen, da sie für Rechenzentren mit einer IT-Flächen von maximal 200m^2 geeignet ist. Vor dem Hintergrund der Größe von Cloud-Rechenzentren erscheint diese Einschränkung nicht sinnvoll. Drei weitere Zertifizierungen boten insgesamt nur unzureichende Informationen über ihren Aufbau und die eigene

Zielsetzung und wurden daher ebenfalls aus der Betrachtung genommen. Es blieben vier Zertifizierungen und ein Standard nach Berücksichtigung der ersten fünf Eingrenzungskriterien. Drei von fünf Kriterienkataloge waren dabei nicht frei verfügbar, woraufhin die betroffenen Organisationen kontaktiert wurden. Dabei konnten zwei von drei Kriterienkatalogen durch die entsprechenden Organisationen bereitgestellt werden. Für eine Zertifizierung stand auch nach der Kontaktaufnahme kein Kriterienkatalog zur Verfügung. Sie wurde daher aus der weiteren Betrachtung genommen. Die Ergebnisse der Eingrenzung nach den zuvor erläuterten Kriterien sind in Tabelle 3-1 zusammengefasst.

Name	Weitere Betrachtung	Anmerkungen
Data Centre Audit (Sudlows)	Nein	Nur wenige Informationen verfügbar.
Data Center Audit (Emerson Network Power)	Nein	Nur für RZ mit einer IT-Fläche $\leq 200m^2$ geeignet.
Data Center Compliance Certification	Nein	Nur wenige Informationen verfügbar.
Data Center Tier Certification	Nein	Nur wenige Informationen verfügbar.
Datacenter Star Audit	Ja	
Data Security Standard	Nein	Keine RZ-Zertifizierung.
ISO/IEC 27001:2005	Nein	Keine RZ-Zertifizierung.
Leadership in Energy and Environmental Design	Nein	Keine RZ-Zertifizierung.
Service Organisation Control 3	Ja	-
Statement on Auditing Standards No. 70: Service Organizations	Nein	Keine RZ-Zertifizierung.
Telecommunications Infrastructure Standards for Data Centers (TIA-492)	Nein	Kriterienkatalog nicht verfügbar.
Tier Certification (UTI)	Ja	-
Trusted Site Infrastructure	Ja	-

Tab. 3-1: Ergebnisse der Eingrenzung der Suchergebnisse.

4. Anforderungen an Cloud-Rechenzentren

4.1 Gegenüberstellung existierender Zertifizierungen für Rechenzentren

4.1.1 Datacenter Star Audit

Das DCSA ist eine vom eco – Verband deutscher Internetwirtschaft e.V. (eco Verband) entwickelte Zertifizierung für Rechenzentren.[59] Der eco Verband wurde 1995 gegründet und ist eine Interessenvertretung der Internetwirtschaft in Deutschland.[60] Eine seiner wichtigsten Aufgaben sieht er darin, die Interessen der Mitglieder gegenüber der Politik und internationalen Gremien zu vertreten. Neben dem Datacenter Star Audit bietet er weitere Dienstleistungen wie beispielsweise das EuroCloud Star SaaS Audit an.

In dieser Arbeit wird die Version 2.0 des DCSA Kriterienkataloges untersucht.[61] Das DCSA definiert fünf unterschiedliche Erfüllungsgrade, die aufeinander aufbauen und zunehmend strengere Anforderungen an Rechenzentren stellen.[62] Der Fokus dieser Zertifizierung liegt auf der Sicherstellung der Rechenzentrums-Sicherheit, Verfügbarkeit und Redundanz der Gebäude-Infrastruktur. Ausgestellte Zertifikate sind 24 Monate lang gültig. Die Bewertung der Rechenzentren erfolgt beim DCSA in den vier Kategorien, Technik (35%), Gebäude (25%), Personal (20%) und Prozesse (20%).[63] Die Anforderungen in der Kategorie Technik beziehen sich auf die technische Infrastruktur eines Rechenzentrums. Dies beinhaltet nicht die eingesetzte Software und nur teilweise die eingesetzte Hardware, in Form der Netzwerk-Infrastruktur. Die Kategorie gliedert sich in die drei Teilkategorien ‚Technik I: Elektrische Sicherheit', ‚Technik II: Klima' und ‚Technik III: Datennetze und Netzinfrastruktur / Managed Services'. In der Teilkategorie Elektrische Sicherheit werden Rechenzentren auf die Art der Energieversorgung geprüft. Dabei wird untersucht, wie und durch wieviele Energielieferanten des Rechenzentrum mit Energie versorgt wird, wie der Strom innerhalb des Rechenzentrums auf die notwendigen Geräte verteilt wird, ob es

---

[59] Vgl. Jabs u. a. (2010).

[60] Vgl. zu diesem und dem nächsten Satz (2012a).

[61] Vgl. zu diesem Kapitel eco Verband (o. J.).

[62] Vgl. zu diesem und den nächsten drei Sätzen eco Verband (2012b).

[63] Die Angaben und Klammen stellen die jeweilige Gewichtung der einzelnen Kategorien dar.

redundante Versorgungssysteme wie beispielweise Notstromaggregate und Batterien gibt und ob die Technik gegenüber Spannungsschwankungen und Überspannung geschützt ist. In der Teilkategorie Klima werden Rechenzentren auf die Art, Leistungsfähigkeit und Redundanz der eingesetzten Klimatisierung sowie auf Umgebungswerte wie z. B. Umgebungstemperaturen und Luftfeuchtigkeit hin geprüft. In der Teilkategorie Datennetze und Netzinfrastruktur / Manager Services wird die Art und Redundanz des Anschlusses an einen Internet Service Provider (ISP), die interne Netzwerkinfrastruktur, die verfügbare Bandbreite sowie die Art und der Umfang der angebotenen Managed Services[64] berücksichtigt. Die Anforderungen in der Kategorie Gebäude und mechanische Sicherheit sind in der DCSA Zertifizierung am umfangreichsten ausgeprägt. Neben der physischen Sicherheit der Rechenzentren, werden auch Brandschutzmaßnahmen, mögliche Gefährdungen in der näheren Umgebung und die Skalierbarkeit der Gebäude-Infrastruktur überprüft. Die Anforderungen in der Kategorie Arbeitsprozesse überprüfen Rechenzentren auf Konformität zur IT Infrastructure Library (ITIL). Die ITIL ist eine Umsetzung des IT-Service-Managements.[65] Sie stellt ein Framework bereit, welches Nutzern dabei hilft IT-Dienstleistungen zu identifizieren, zu planen, auszuliefern und zu unterstützen. Außerdem wird geprüft, ob Prozesse zur Datensicherung und andere Zertifizierungen vorhanden sind. Auch wird überprüft, ob neue Mitarbeiter einer Sicherheitsüberprüfung unterzogen werden und ob es feste Prozesse zur Vergabe von Zugangsrechten zu den verschiedenen Sicherheitsbereichen in einem Rechenzentrum gibt. Die Anforderungen in der Kategorie Personal und Mitarbeiter-Qualifikation betrachten die Anzahl, Verfügbarkeit und Qualifikation des eingesetzten Personals. Dabei wird sowohl auf Mitarbeiter externer Firmen, die innerhalbe des Rechenzentrums tätig sind, als auch auf eigene Mitarbeiter des Rechenzentrum-Betreibers eingegangen.

4.1.2 Service Organization Control 3 Report

Die nächste untersuchte Zertifizierung ist die SOC3. Ein SOC3 Report wird auf Grundlage der Trust Services Principles, Criteria, and Illustrations erstellt.[66] Die Trust

---

[64] Managed Services sind IT-Dienstleistungen, deren Bereitstellung und Verfügbarkeit von einem externen Anbieter, dem Managed Services Provider, übernommen wird.

[65] Vgl. zu diesem und den nächsten beiden Sätzen Arraj (2010), S. 3-4.

[66] Vgl. AICPA (2012a),

Services Principles, Crietria, and Illustrations wurden durch das American Institute of Certified Public Accountants (AICPA), mit Hilfe des Canadian Institute of Chartered Accountants (CICA), und als Nachfolger der Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy entwickelt.[67] Das AICPA ist ein 1887 gegründeter Verband U.S. Amerikanischer Wirtschaftsprüfer.[68] Zu seinen Aufgaben gehört die Entwicklung von Audit-Standards zur Auditierung von privaten, öffentlichen und gemeinnützigen Organisationen im Bereich des Rechnungswesens. SOC3 Reports sind zur Veröffentlichung vorgesehen und ermöglichen den Organisationen die Konformität der eigenen Dienstleistungen zu bestimmten Standards nach außen zu kommunizieren.[69]

In dieser Arbeit werden die Trust Services Principles, Criteria and Illustrations des AICPA mit Stand vom 15. September 2009 untersucht.[70] Sie dienen als Grundlage der Erstellung eines SOC3 Reports. Der Kriterienkatalog ist für die Anwendung auf IT basierte Systeme wie z. B. E-Commerce-Systeme ausgelegt.[71] Die im Kriterienkatalog formulierten Anforderungen konzentrieren sich auf die Prozesse von IT-Dienstleistern. Es werden sowohl Anforderungen an das Management, als auch Anforderungen an die eingesetzte Software und Hardware, sowie einige Anforderungen an die Gebäude-Infrastruktur definiert. Sie sind in die fünf Kategorien Sicherheit, Verfügbarkeit, Prozessintegrität, Vertraulichkeit und Datenschutz eingeteilt. Sicherheit bezeichnet den Schutz des Systems vor physischen und logischen Zugriffen durch eine unautorisierte Partei. Kontrollierte Zugriffe helfen beim Schutz vor Missbrauch, Fehlbedienungen von Software, Diebstahl von Ressourcen sowie vor unbeabsichtigten Änderungen, der Löschung oder Veröffentlichung von Informationen. Verfügbarkeit kennzeichnet die Möglichkeit des Zugriffs auf das System zum Zwecke der Verarbeitung, Überwachung und Wartung. Sie beinhaltet insbesondere nicht die Systemfunktionalität und Nutzbarkeit des Systems. Innerhalb des Kriterienkatalogs werden keine Mindestanforderungen an die Verfügbarkeit gestellt. Dies obliegt einer spezifischen

---

[67] Vgl. AICPA, CICA (2009), S. 1-2.

[68] Vgl. zu diesem und dem nächsten Satz AICPA (2012b).

[69] Vgl. AICPA (2012a).

[70] Vgl. zu diesem Kapitel AICPA, CICA (2009).

[71] Vgl. AICPA, CICA (2009), S. 3.

Vereinbarung durch die beteiligten Parteien. Die Anforderungen sollen sicherstellen, dass die getroffenen Vereinbarungen eingehalten werden können. Prozessintegrität beschreibt die Vollständigkeit, Fehlerfreiheit, Validität, Aktualität und Autorisierung der Systemverarbeitung. Sie wird als Voraussetzung dafür betrachtet, dass Systemnutzer die korrekten, angeforderten Informationen, Güter oder Dienstleistungen erhalten. Vertraulichkeit meint die Fähigkeit des Systems, als vertraulich gekennzeichnete Informationen vor unbefugten Zugriffen zu schützen. Datenschutz meint die Rechte und Pflichten von Individuen und Organisationen, die im Zusammenhang mit dem Sammeln, Verwenden, Speichern, Offenlegen und Löschen von persönlichen Daten bestehen. Persönliche Daten sind dabei alle Daten, die direkt oder indirekt zur Identifizierung einer Person genutzt werden können. Jede Kategorie besteht darüber hinaus aus den vier Dimensionen Grundsätze, Kommunikation, Prozeduren und Überwachung. Die Anforderungen verlangen, dass in jeder Kategorie Grundsätze definiert werden. Diese legen den Umfang der Dienstleistungen in jeder Kategorie fest. Ferner sollen die Grundsätze an die nötigen Parteien kommuniziert und entsprechende Prozeduren zu ihrer Einhaltung implementiert werden. Schließlich sollen die implentierten Prozeduren überwacht und ggf. bei nicht Einhaltung der definierten Grundsätze angepasst werden.

4.1.3 Trusted Site Infrastructure

Die Trusted Site Infrastructure (TSI) ist eine von der TÜV Informationstechnik GmbH (TÜViT) entwickelte Zertifizierung für Rechenzentren.[72] Der TÜViT ist ein Unternehmen der TÜV NORD Gruppe und nach seinen Grundsätzen dazu verpflichtet, die eigenen Dienstleistungen unabhängig und neutral anzubieten und durchzuführen.[73]

In dieser Arbeit wird Version 3.0 des Trusted Site Infrastructure (TSI) Kriterienkataloges untersucht.[74] Auf Basis der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) identifiziert der Kriterienkatalog vier Gefährdungspotentiale. Diese sind höhere Gewalt,

---

[72] Vgl. TÜViT GmbH (2011), S. 6-7.

[73] Vgl. TÜViT GmbH (2011), S. 32.

[74] Vgl. zu diesem Kapitel TÜViT GmbH (2011).

organisatorische Mängel, technisches Versagen und vorsätzliche Handlungen. Der Fokus dieser Zertifizierung liegt auf der Gebäude-Infrastruktur und der Empfehlung von Maßnahmen zum präventiven Schutz der IT- und Kommunikationssysteme. Ziel ist es, eine möglichst hohe System- und Datensicherheit und Funktionssicherheit zu erreichen. Ein ausgestelltes Zertifikat ist 24 Monate lang gültig und kann nach einer erneuten Zertifizierung jeweils um weitere 24 Monate verlängert werden. Die TSI teilt Rechenzentren in vier aufeinander aufbauende Erfüllungsgrade ein. Die einzelnen Erfüllungsgrade werden als Level 1 bis Level 4 bezeichnet und stellen zunehmend strengere Anforderungen an die zertifizierten Rechenzentren. Level 1 Rechenzentren besitzen einen mittleren Schutzbedarf, Level 2 Rechenzentren einen erweiterten Schutzbedarf, Level 3 Rechenzentren einen hohen Schutzbedarf und Level 4 Rechenzentren einen sehr hohen Schutzbedarf. Um eine Zuteilung eines Rechenzentrums zu einem dieser Levels vorzunehmen, werden diese in acht unterschiedlichen Aspekten untersucht. Diese sind Umfeld, Baukonstruktion, Brandschutz, Melde- & Löschtechnik, Sicherheitssysteme & -organisation, Energieversorgung, Raumlufttechnische Anlagen, Organisation und Dokumentation.
Die ersten sechs Kategorien konzentrieren sich auf die physische Absicherung des Rechenzentrums. Dies umfasst die Meidung und den präventiven Schutz vor möglichen Sicherheits- und Ausfallrisiken. Dazu gehören z.B. die Meidung von Gefahren in der Umgebung des Rechenzentrums, die redundante Auslegung der Energieversorgung, sowie den Schutz und Bekämpfung von Feuern. Die beiden Kategorien Organisation und Dokumentation adressieren dagegen Risiken des Managements. Dies beinhaltet bspw. die Kommunikation der Zuständigkeiten innerhalb des Rechenzentrums, das Durchführen regelmäßiger Wartungen und das Vorhandensein von Plänen und Vorschriften für Notfallsituationen. Das zertifizierte Level ergibt sich aus dem geringsten erreichten Level unter den einzelnen Aspekten.

Die TSI sieht darüber hinaus auch eine sogenannte Dual Site Zertifizierung vor. Diese bedeutet, dass zwei Rechenzentren gemeinsam Zertifiziert werden. Das zertifizierte Level ergibt sich dabei allerdings nicht alleine aus den erreichten Leveln der beiden betrachteten Rechenzentren. Um für eine Dual Site Zertifizierung infrage zu kommen, erfordert die TSI, dass die IT-Flächen der beiden betrachteten Rechenzentren ähnlich groß sind und beide bereits einzeln TSI zertifiziert sind. Zudem müssen beide Rechenzentren in unterschiedlichen Gebäuden liegen und über eine redundante

Datennetzverbindung miteinander verbunden sein. Außerdem dürfen sich mögliche Umgebungsgefährdungen nicht gleichzeitig auf beide Rechenzentren auswirken.

4.1.4 Uptime Institute's Tier Certification

Die Tier Certification ist eine vom Uptime Institute LLC entwickelte Zertifizierung für Rechenzentren.[75] Das UTI ist eine seit 1993 tätige und unabhängige Sparte der The 451 Group Unternehmensgruppe, mit Hauptsitz in den USA.[76] Es ist eine Forschungs-, Lehr- und Consulting-Organisation im Rechenzentrums-Bereich.

In dieser Arbeit wird die Tier Standard Topologie mit Stand vom 1. August 2012 untersucht.[77] Sie formuliert keine konkreten Kriterien sondern allgemeine Anforderungen an Rechenzentren. Ausgehend davon definiert sie vier aufeinander aufbauende Erfüllungsgrade, die mit Tier I bis Tier IV bezeichnet werden und zunehmend strengere Anforderungen stellen. Ziel der Tier Certification des UTI ist eine ganzheitliche Betrachtung der Gebäude-Infrastruktur. Diese ist nötig, um einen ordnungsgemäßen Betrieb von Rechenzentren gewährleisten zu können. Dabei wird weniger Wert auf die Betrachtung individueller Systeme und Subsysteme gelegt. Stattdessen werden alle Teilsysteme als gleich wichtig betrachtet. Nicht berücksichtigt werden die eingesetzten IT-Systeme, bestehend aus Hardware und Software. Das schwächste Teilsystem eines Rechenzentrums bestimmt hierbei seine Zuteilung zu einer der vier Tiers. Ein ausgestelltes Zertifikat ist 24 Monate lang gültig.

Der Tier I Erfüllungsgrad stellt grundsätzliche Anforderungen an die Gebäude-Infrastruktur eines Rechenzentrums. Er bringt den Wunsch der Nutzer nach dedizierten Räumlichkeiten für die IT-Systeme zum Ausdruck, bietet eine bessere Ausstattung als die übliche Unterbringung in einem Büro und sorgt für eine höhere Verfügbarkeit, bspw. durch die Fähigkeit kurze Stromausfälle zu überbrücken. Rechenzentren dieses Erfüllungsgrades besitzen keine redundanten Energieversorgungskomponenten und sind an einen einzelnen Energielieferanten angeschlossen. Des Weiteren besitzen sie ein

---

[75] Vgl. UTI (2012), S. ii.

[76] Vgl. zu diesem und dem nächsten Satz UTI (2012a).

[77] Vgl. zu diesem Kapitel UTI (2012b).

dediziertes Kühlsystem und einen Notstromgenerator, um kurze Ausfälle des Energielieferanten kompensieren zu können. Rechenzentren auf dieser Ebene sind anfällig für Ausfälle aufgrund des täglichen Betriebs, unerwarteter Störungen und Bedienungsfehler. Weiterhin muss die gesamte Anlage in regelmäßigen Abständen, z. B. einmal jährlich, zur Wartung heruntergefahren werden. Tier II Rechenzentren besitzen einige wichtige redundante Komponenten und verfügen über eine höhere Verfügbarkeit als Tier I zertifizierte Rechenzentren. Zu den redundanten Komponenten gehören Stromgeneratoren, USV, Batterien, Kühlanlagen und die Wärmeschutz-Ausrüstung. Sie sind weiterhin anfällig für Ausfälle aufgrund unerwarteter Störungen und Bedienungsfehler. Der tägliche Betrieb stellt ein geringeres Risiko für Ausfälle dar. Ausfälle von einzelnen Komponenten der Energieversorgung können jedoch den Betrieb beeinträchtigen, während ein Ausfall des Energieversorgungssystems oder des Energielieferanten mit Sicherheit zu einer Störung führt. Die gesamte Anlage muss in regelmäßigen Abständen zur vollständigen Wartung heruntergefahren werden. Redundante Komponente können jedoch während des laufenden Betriebs gewartet werden. Tier III Rechenzentren realisieren das Konzept der gleichzeitigen Wartbarkeit. Alle Komponenten der Energieversorgung sind redundant ausgelegt und es gibt zwei unabhängige Versorgungsnetze, die alle Systeme mit Energie versorgen können. Dazu gehört auch der Anschluss an einen alternativen Energielieferanten. Rechenzentren dieser Ebene sind weiterhin Anfällig für Beeinträchtigungen des Betriebes aufgrund unvorhergesehener Störungen. Das Risiko für Beeinträchtigungen durch den täglichen Betrieb oder Bedienungsfehler ist geringer. Rechenzentren, die den Tier III Anforderungen entsprechen können während des laufenden Betriebs gewartet werden. Es ist nicht notwendig die Anlage zum Zwecke der Wartung herunter zu fahren. Während der Wartung besteht jedoch ein erhöhtes Ausfallrisiko der Anlage. Tier IV Rechenzentren realisieren das Konzept der fehlertoleranten Gebäude-Infrastruktur. Das bedeutet, dass eine beliebige Störung zu einem beliebigen Zeitpunkt zu keiner Beeinträchtigung des Betriebs der Anlage führen kann. Alle wichtigen Systeme, wie bspw. die Energieversorgung und Kühlung sind mehrfach redundant vorhanden. Es existieren mehrere physikalisch voneinander unabhängige Energieversorgungssysteme und alle IT-Systeme werden gleichzeitig von mindestens zwei Energiequellen versorgt. Rech Zentren auf dieser Ebene sind nicht anfällig für Ausfälle aufgrund des täglichen Betriebs, ungeplanter Störungen oder Bedienungsfehler. Die Anlage kann regelmäßig

gewartet werden ohne dass sie heruntergefahren werden muss. Während der Wartung besteht ein geringfügig höheres Risiko für Beeinträchtigungen des Betriebs.

4.1.5 Gemeinsamkeiten der vorgestellten Zertifizierungen

Die Gegenüberstellung der obigen Zertifizierungen zeigt, dass sie einige Gemeinsamkeiten besitzen. Insbesondere drei der vier vorgestellten Zertifizierungen, das DCSA, die TSI und die Tier Certification des UTI besitzen hierbei Gemeinsamkeiten im Bezug auf ihre Anforderungen an Rechenzentren. Sie sind speziell auf Rechenzentren ausgerichtet und definieren unterschiedliche Erfüllungsgrade.[78] Dabei haben sich vier bis fünf aufeinander aufbauende Erfüllungsgrade mit jeweils steigenden Anforderungen durchgesetzt. In ihren höchsten Erfüllungsgraden erfordern die drei genannten Zertifizierungen alle, dass mehrfach redundante Energieversorgungs- und Klimatisierungssysteme vorhanden sind.[79] Sie konzentrieren sich auf die Gebäude-Infrastruktur und berücksichtigen neben redundanten Energieversorgungs- und Klimatisierungssystemen auch dedizierte Räumlichkeiten, die physikalische Absicherung des Rechenzentrums, sowie mögliche Gefahrenpotentiale in der Umgebung der Rechenzentren. Darüberhinaus vergeben ihre Zertifikate auch nur für eine begrenzte Dauer und erfordern danach eine Re-Zertifizierung des Rechenzentrums. Alle vier Zertifizierungen berücksichtigen, allerdings in unterschiedlichem Maße, Anforderungen an das Management der Rechenzentren. So gehen das DCSA, die TSI und die Tier Certification des UTI ebenfalls auf die Konformität der Rechenzentren zur ITIL ein. Innerhalb des DCSA sind dabei jedoch die Kriterien im Bezug auf die ITIL am stärksten ausgeprägt. Den größten Fokus auf das Management legt die SOC3.

Am wenigsten ausgeprägt sind bei allen vier Zertifizierungen die Anforderungen an die Hardware und Software. Wenn Anforderungen an die Hardware gestellt werden, dann beschränken sie sich unter den betrachteten Zertifizierungen auf das interne Netzwerk. Anforderungen im Bezug auf die Software sind fast nicht vorhanden. Als einzige

---

[78] Vgl. eco Verband (2012c), S.2, 4; TÜViT GmbH (2011), S. 6-7, 15; UTI (2012b), S. 1.

[79] Vgl. eco Verband (2012c), S. 9; TÜViT GmbH, S. 15-16; UTI (2012b), S. 4.

Zertifizierung geht die SOC3 auf die eingesetzte Software ein und erfordert einen Schutz gegen Schadsoftware und die Verschlüsselung von Zugangsdaten.[80]

4.1.6 Unterschiede der vorgestellten Zertifizierungen

Neben den beschriebenen Gemeinsamkeiten besitzen die vorgestellten Zertifizierungen auch einige Unterschiede. So sind die beiden deutschsprachigen Zertifizierungen, das DCSA und die TSI, bspw. konkreter im Bezug auf die Beschreibung der gestellten Anforderungen. Sie Formulieren konkrete Fragen oder Kriterien. Die beiden englischsprachigen Zertifizierungen, die Tier Certification des UTI und die SOC3 Reports sind weniger konkret und lassen mehr Raum für Interpretation. Die Tier Standard Topology des UTI nennt als Grund hierfür z. B. dass der eingeräumte Interpretationsspielraum die Möglichkeit zu Innovationen bieten soll.[81] Ferner ist die SOC3 Zertifizierung als einzige keine auf Rechenzentren spezialisierte Zertifizierung. Stattdessen ist sie auf alle Arten von Systemen anwendbar, die durch den Einsatz von IT ermöglicht werden.[82] Sie adressiert daher weniger an physische Anforderungen wie z. B. die Lage und Absicherung des Gebäudes, sondern konzentriert sich auf Maßnahmen des Managements. Obwohl drei der vier untersuchten Zertifizierungen überwiegend die physische Sicherheit der Rechenzentren berücksichtigen, scheint es kein einheitliches Schema zur Einteilung zu geben. Die Einteilung der Kriterien in verschiedene Kategorien unterscheidet sich bei allen Zertifizierungen erheblich. Darüber hinaus bieten der TÜViT und das UTI ergänzende Zertifizierungen zu ihren Rechenzentrum-Zertifizierungen an.

4.2 Allgemeine Anforderungen an moderne Rechenzentren

Auf Grundlage der vorgestellten Zertifizierungen sollen in diesem Abschnitt zunächst allgemeine Anforderungen an moderne Rechenzentren hergeleitet werden. In Anlehnung an die in Kapitel 2.2 genannten Bestandteile moderner Rechenzentren, werden die Anforderungen in die vier Kategorien Gebäude-Infrastruktur, Hardware-Infrastruktur, Software-Infrastruktur und Management eingeteilt.

---

[80] Vgl. AICPA, CICA (2009), S. 13.

[81] Vgl. UTI (2012b), S. 5.

[82] Vgl. AICPA, CICA (2009), S. 3.

4.2.1 Anforderungen an die Gebäude-Infrastruktur

Die Anforderungen an die Gebäude-Infrastruktur sind unter den zuvor betrachteten Rechenzentrums-Zertifizierungen am stärksten ausgeprägt. Im Folgenden werden zu dieser Kategorie ebenfalls die Anforderungen an die Umgebung des Rechenzentrums, die Energieversorgung und die Klimatisierung gezählt, da sie einen unmittelbaren Einfluss auf die Baukonstruktion des Rechenzentrums haben. So bestimmen z. B. die Umgebungsanforderungen die endgültige Lage des Rechenzentrums. Insgesamt lassen sich die Anforderungen an die Gebäude-Infrastruktur daher in die vier Teilkategorien Umgebung, Baukonstruktion, Energieversorgung und Klimatisierung aufteilen.

In der Teilkategorie Umgebung eines Rechenzentrums umfassen die Anforderungen alles, was sich nicht auf dem Gelände oder innerhalb des Gebäudes, aber innerhalb der Umgebung des Rechenzentrums befindet. Hauptsächlich behandeln die genannten Kriterien die Vermeidung von Gefahrenpotentialen, da diese den Betrieb eines Rechenzentrums stören könnten. Hierzu zählt bspw. die Meidung von Hochwasser, Erdbeben, Lawinen und Tornado gefährdeten Gebieten. Ebenso sollten auch Gefahrgut produzierende Betriebe sowie Straßen und Bahnstrecken, auf denen Gefahrgut transportiert wird, gemieden werden. Als weitere mögliche Gefahrenquellen werden Staudämme, Flughäfen, Kraftwerke und andere elektromagnetische Quellen genannt. Auch werden hohe Gebäude und regelmäßig stattfindenden Großveranstaltungen in der Nähe des Rechenzentrums als mögliche Gefahren eingestuft. Die Anforderungen an die Baukonstruktion eines Rechenzentrums beinhalten alles, was sich unmittelbar auf dem Gelände des Rechenzentrums oder innerhalb des Gebäudes befindet. Sie adressieren Sicherheitsrisiken wie beispielsweise die Absicherung gegen unautorisierte Zutritte zum Gebäude und den Schutz vor Bränden. Aber auch die bauliche Eignung des Gebäudes, um die benötigten IT-Systeme sicher und in ausreichender Menge betreiben zu können wird in dieser Kategorie berücksichtigt. Zu den Anforderungen an die Baukonstruktion gehören zunächst dedizierte Räumlichkeiten für das Rechenzentrum. Je nach angestrebtem Erfüllungsgrad und Umfang der IT-Systeme bedeutet dies entweder, dass das Rechenzentrum in einem eigenen, abgegrenzten Bereich eines Gebäudes mit weiteren Mietern, oder aber auf einem eigenen Gelände und in einem extra dafür vorgesehenen Gebäude betrieben wird. Weiterhin sollte das Gebäude über eine massive

Bauweise verfügen, die es gegen Außenweinwirkungen wie bspw. Beschuss oder gegen mögliche Terroranschläge schützt. Zusätzlich dazu wird auch eine allgemeine Zugangskontrolle zum Gelände, zum Gebäude und den einzelnen Sicherheitsbereichen im Rechenzentrum gefordert.

Die Art und Redundanz des Energieversorgungssystems in einem Rechenzentrum stellt einen zentralen Aspekt in den meisten der betrachteten Zertifizierungen dar. Ziel der Anforderungen an die Energieversorgung ist es eine möglichst hohe Verfügbarkeit des Systems zu garantieren und die IT-Systeme z. B. vor Überspannung zu schützen.[83] Je nach Größe und angestrebtem Erfüllungsgrad variieren die Anforderungen an die Energieversorgung jedoch. Im geringsten Fall sollte sie ausreichend dimensioniert sein, um den Energiebedarf der gesamten Anlage decken zu können und mindestens eine USV zum Ausgleich von Spannungsschwankungen und zur Überbrückung kurzer Stromausfälle besitzen. Einige Zertifizierungen wie z.B. die Tier Certification des UTI fordern zudem bereits beim niedrigsten Erfüllungsgrad, dass es eine sogenannte Netzersatzanlage (NEA) inklusive Kraftstoff zum Betrieb gibt.[84] Der Ausfall des lokalen Energielieferanten wird in diesem Fall nicht als eine Ausnahme betrachtet, sondern als die Regel vorausgesetzt. Weitere Kriterien in dieser Kategorie sind die Verfügbarkeit von Batterien zur mittelfristigen Überbrückung eines Ausfalls des Energielieferanten, eine unabhängige Versorgung der IT-Systeme mit Strom, die Absicherung der Energieversorgung gegenüber Manipulation und ein Blitzschutz. Um die Verfügbarkeit der IT-Systeme gewährleisten zu können, erfordern die meisten untersuchten Zertifizierungen je nach Erfüllungsgrad eine einfach oder mehrfach redundante Energieversorgung für die gesamte Anlage. Dies beinhaltet je nach Anforderungslevel dass mindestens zwei unabhängige und von einander getrennte Stromverteilungsnetze existieren und, dass das Rechenzentrum mindestens an einen zweiten, unabhängigen Energielieferanten angebunden ist.

Auch bei den Anforderungen an die Klimatisierung liegt der Fokus auf der Verfügbarkeit der Rechenzentren. Wie bereits in Kapitel 2.2.2 thematisiert wurde,

---

[83] Vgl. TÜViT GmbH (2011), S. 10.

[84] Vgl. UTI (2012), S. 1.

haben moderne Rechenzentren einen großen Energiebedarf. Damit einhergehend erzeugt die eingesetzte IT auch Abwärme.[85] Um optimale Betriebstemperaturen für die IT-Systeme gewährleisten zu können, ist daher eine ausreichende Klimatisierung der IT-Räumlichkeiten notwendig. Die Anforderungen an die Klimatisierungen von Rechenzentren beinhalten daher, dass die Rückkühlanlagen zur Kühlung der Raumluft ausreichend dimensioniert sind und auch im Falle von, für die Umgebung typischen, Höchsttemperaturen noch eine ausreichende Kühlleistung besitzen. Wird Wasser zur Rückkühlung eingesetzt, so ist eine sichere und ausreichende Versorgung mit Kühlwasser zu berücksichtigen. Neben der Kühlfunktion wird ebenfalls gefordert, dass die Klimatisierung über Luftfilter verfügt, um bspw. Staub aus der Luft zu filtern und dass für eine geeignete Luftfeuchtigkeit innerhalb der IT-Räumlichkeiten gesorgt wird. Ein in der Praxis weit verbreitetes Aufstellungssystem der Racks ist das sogenannte Kalter-Gang-Warmer-Gang-Prinzip[86]. Es hat sich zur Kühlung der Raumluft bewährt und verhindert in gewissem Maße, dass sich gekühlte Raumluft mit aufgeheizter Raumluft vermischt, wodurch die Kühlleistung der Klimaanlage reduziert wird. Zusätzlich dazu, sollte neben den IT-Systemen auch die Rückkühlanlagen redundant vorhanden sein und redundant mit Strom versorgt werden. Je nach Erfüllungsgrad ist eine einfach oder mehrfach redundante Klimatisierung erforderlich. Auch wird die Einhaltung der Grenzwerte für Temperatur und Luftfeuchte überprüft.

4.2.2 Anforderungen an die Hardware- und Software-Infrastruktur

Insgesamt definieren die betrachteten Zertifizierungen nur wenige Anforderungen an die Hardware-Infrastruktur der Rechenzentren. Ein großer Teil der Kriterien bezieht sich dabei auf die Anbindung des Rechenzentrums an einen bzw. mehrere ISPs, den Aufbau des internen Netzwerks. Zu den Anforderungen gehört, dass Rechenzentren an mindestens einen ISP angeschlossen sind und die vertraglich zugesicherte Netzbandbreite für den Spitzenlastbetrieb ausreichend dimensioniert ist. In höheren Erfüllungsgraden wird außerdem die Anbindung an mindestens einen weiteren, unabhängigen ISP gefordert. Auch sollte die Übergabe des WAN an die Rechenzentren

---

[85] Vgl. Patel, Shah (2005), S. 6.

[86] Bei dem Kalter-Gang-Warmer-Gang-Prinzip handelt es sich um ein Aufstellungsschema für Racks. Sie werden .nebeneinander aufgestellt, sodass sie Gänge bilden. Dabei dienen jeweils Abwechselnd ein Gang zur Aufnahme der warmen Luft aus den Racks und ein Gang zur Aufnahme der gekühlten Luft.

in extra dafür vorgesehenen und gegen Manipulation abgesicherten Räumlichkeiten stattfinden. Im Bezug auf das interne Netzwerk wird, in Abhängigkeit vom Anforderungslevel, eine redundante Verkabelung oder das Vorhandensein eines zweiten, unabhängigen Netzwerkes gefordert. Weitere Anforderungen an die Hardware-Infrastruktur betreffen die Anwendung von Datensicherungssystemen. Es wird davon ausgegangen, dass jedes Rechenzentrum über ein entsprechendes System verfügt, dass Daten in regelmäßigen Abständen auf externen Datenträgern, wie bspw. CDs, Festplatten oder Bändern sichert. Sie müssen getrennt von der restlichen IT in brandsicheren und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten aufbewahrt werden.

Die Anforderungen an die Software-Infrastruktur der Rechenzentren sind innerhalb der analysierten Zertifizierungen am geringsten ausgeprägt. Sie beschränken sich auf den Einsatz von Schutzsoftware, sowie die Zuorden- und Rückverfolgbarkeit getätigter Systemeingaben. Zu den Aufgaben der eingesetzten Schutzsoftware gehört es das System auf logischer Ebene, d. h. durch die Vergabe und Überprüfung von Zugangsrechten, vor unbefugten Zugriffen zu schützen. Dies umfasst auch die verschlüsselte Aufbewahrung der vergebenen Authentifizierungsdaten. Zudem wird der Einsatz entsprechender Virenschutz-Software und Firewalls gefordert.

4.2.3 Anforderungen an das Management

Neben den Anforderungen an die Gebäude-Infrastruktur sind die Anforderungen an das Management am stärksten ausgeprägt. Sie lassen sich grob in die drei Teilkategorien ‚Anforderungen an das Personal', ‚Anforderungen an die Dokumentation und Überwachung' und ‚Anforderungen an die Prozesse' gliedern. Das Ziel dieser Kategorie von Anforderungen ist es, die Systemsicherheit, Verfügbarkeit, Vertraulichkeit und Prozessintegrität durch Managementmaßnahmen herzustellen bzw. zu steigern. Teilweise beinhaltet dies auch die Kommunikation der angewandten Maßnahmen nach außen, an potentielle Kunden.[87] Daher berücksichtigen zwei der vier analysierten Zertifizierungen explizit, ob die Rechenzentren bereits andere Zertifizierungen besitzen.

[87] Vgl. AICPA, CICA (2009), S. 5.

Die Anforderungen an das Personal eines Rechenzentrums lassen sich in zwei Gruppen teilen. Zum einen betreffen sie die Verfügbarkeit des eingesetzten Personals in den verschiedenen Bereichen und zum anderen die Eignung der Mitarbeiter. Zur Eignung der Mitarbeiter zählt hierbei nicht nur die berufliche Qualifikation, sondern auch eine ausführliche Sicherheitsüberprüfung neuer Mitarbeiter und eine regelmäßig stattfindende Sicherheitsunterweisung. Hierdurch soll eine hohe Systemsicherheit und Vertraulichkeit realisiert werden. Auch hat die Verfügbarkeit des Personals in gewissem Maße Einfluss auf die Verfügbarkeit der gesamten Anlage, bspw. in Form von Technikern und Administratoren, die im Falle von Störungen, den Normalzustand der Anlage wiederherstellen können.

Diese Teilkategorie konzentriert sich darauf, den Betrieb des Rechenzentrums in allen wichtigen Aspekten zu überwachen und zu dokumentieren, um im Falle von Abweichungen und Störungen zeitnah und angemessen reagieren zu können. Die Anforderungen tragen zur Erhöhung der Sicherheit und Verfügbarkeit des Rechenzentrums bei. Die ständige Überwachung der Betriebszustände der IT-Systeme, Energieversorgung und Klimatisierung gehört hierzu, ebenso wie ein Brandschutz-, Notfall- und Sicherheitskonzept und eine vorangegangene Risikoanalyse. Auch sollten regelmäßige Wartungen aller wichtigen Anlagenteile vorgenommen und protokolliert werden.

Die Anforderungen an die Prozesse in einem Rechenzentrum sind vielfältig. Alle analysierten Zertifizierungen berücksichtigen sie in einem gewissen Maße, wobei sich die SOC3 fast ausschließlich den Prozessen von IT-Dienstleistern widmet. Allerdings bleiben diese Anforderungen abstrakt und wenig konkret. Weitere geforderte Prozesse dienen bspw. dazu den zukünftigen Energie-, Kühl-, und Platzbedarf prognostizieren zu können, oder im Falle von Sicherheitslücken in der Lage zu sein, die betroffenen Parteien rechtzeitig darüber zu informieren. Drei Zertifizierungen berücksichtigen zudem auch die Konformiät zur ITIL.

4.3 Spezifische Anforderungen des Cloud-Computig an Rechenzentren

In diesem Abschnitt werden, ausgehend von den in Kapitel 2.1 beschriebenen Charakteristika des Cloud-Computing und dem in Kapitel 2.2 beschriebenen Aufbau

von Rechenzentren, einige Anforderungen des Cloud-Computing an Rechenzentren beschrieben. Dies gilt insbesondere für die On-Demand-Self-Service-Eigenschaft und die kurzfristige Elastizität des Cloud-Computing. Obgleich sich die bereitgestellten Funktionalitäten der drei Cloud-Computing-Dienstleistungsmodelle unterscheiden, sind die in Kapitel 2.1.1 aufgezeigten Eigenschaften des Cloud-Computing allen dreien inhärent. Ebenfalls besitzen, wie in Kapitel 2.2.3 beschrieben, herkömmliche Rechenzentren und Cloud-Rechenzentren die gleichen vier Grundbestandteile. Aus diesem Grund erscheint eine Einteilung der Anforderungen in die Dimensionen Gebäude-Infrastruktur, Hardware-Infrastruktur, Software-Infrastruktur und Management gegenüber einer Einteilung nach den drei Dienstleistungsmodellen des Cloud-Computing besser geeignet und wird im Folgenden daher angewendet.

4.3.1 Anforderungen an die Gebäude-Infrastruktur

Die in Abschnitt 4.2.1 erläuterten allgemeinen Anforderungen and die Umgebung eines Rechenzentrums haben zum Ziel eine möglichst hohe physische Sicherheit und Verfügbarkeit der Rechenzentren zu gewährleisten. Da von Seiten der Zertifizierungen und auch von Seiten der Rechenzentrum-Betreiber bereits große Anstrengungen in dieser Hinsicht unternommen werden,[88] lassen sich keine neuen Anforderungen and die Rechenzentrumsumgebung durch den Betrieb von Cloud-Computing identifizieren.

Wie in Abschnitt 4.2.1 ebenfalls beschrieben, adressieren die Anforderungen an die Baukonstruktion eines Rechenzentrums die physische Absicherung der Rechenzentren und die bauliche Eignung zum sicheren Betrieb der notwendigen Anzahl an IT-Systemen. Eine Eigenschaft des Cloud-Computing ist die Verfügbarkeit einer großen Menge von IT-Ressourcen. Eine ausreichend große IT-Fläche ist im Falle von Cloud-Computing daher notwendig. Dies ist auch im Hinblick auf den von Cloud-Computing-Diensten geforderten Anschein unendlicher Ressourcen relevant. Sollte es aufgrund einer unerwartet hohen Nachfrage notwendig werden neue Hardware zu beschaffen und diese innerhalb des Rechenzentrums zu betreiben, so müssen alle betroffenen Systeme und auch die verfügbaren IT-Flächen über die Kapazitäten verfügen, um diese zusätzliche Hardware aufnehmen zu können.

---

[88] Vgl. Barroso, Hölzle (2009), S. 39.

Die untersuchten Anforderungen an die Energieversorgung und Klimatisierung herkömmlicher Rechenzentren variieren je nach angestrebtem Erfüllungsgrad. Sie sind darauf ausgelegt eine hohe Verfügbarkeit und eine möglichst lange Lebensdauer der IT-Systeme zu garantieren. Der oft genannte Anspruch potentieller Cloud-Nutzer nach nahezu hundertprozentiger Verfügbarkeit des Dienstes ist hierbei vergleichbar mit den Verfügbarkeitsansprüchen höherer Erfüllungsgrade der betrachteten Zertifizierungen. Des Weiteren ist davon auszugehen, dass der Energieverbrauch pro Quadratmeter IT-Fläche in den nächsten Jahren weiter ansteigen wird,[89] was den Einsatz leistungsfähigerer Energieversorgungssysteme bedingt. Damit einhergehend nimmt auch die durch die Hardware abgegebene Wärme pro Quadratmeter in Zukunft zu, was folglich auch leistungsfähigere Klimatisierungssysteme erfordert.

4.3.2 Anforderungen an die Hardware-Infrastruktur

Die an klassische Rechenzentren gestellten Hardware-Anforderungen sind wenig umfangreich und beschränken sich in der Regel auf die Gestaltung der Netzwerke. Ein möglicher Grund hierfür ist, dass Rechenzentren in der Vergangenheit eher als eine Möglichkeit zur Unterbringung verschiedener Server mit ähnlichen Verfügbarkeits- und Sicherheitsansprüchen betrachtet wurden, anstatt als ein einheitliches System.[90] Aufgrund der Eigenschaften des Cloud-Computing ist jedoch eine ganzheitliche Betrachtung der IT-Infrastruktur als ein einziges System angebracht. Dies hat zur Folge, dass die Hardware-Infrastruktur der Rechenzentren bezogen auf Cloud-Computing umfassenderen Anforderungen gerecht werden muss. Im Hinblick auf die Cloud-Computing Eigenschaft On-Demand-Self-Service muss die Hardware-Infrastruktur z. B. so gestaltet sein dass die von einem Benutzer benötigten IT-Ressourcen auch kurzfristig, d.h. innerhalb von Minuten, durch den Benutzer abgerufen werden können. Bezogen auf die Eigenschaft der kurzfristigen Elastizität muss die Hardware-Infrastruktur ausreichend dimensioniert sein, um jederzeit auch den maximalen Bedarf der Nutzer befriedigen zu können. Weiterhin folgt aus den beiden Eigenschaften des On-Demand-Selb-Service und der kurzfristigen Elastizität, dass die tatsächlich

---

[89] Vgl. Patel, Shah (2005), S. 1.

[90] Vgl. zu diesem und dem nächsten Satz Barroso, Hölzle (2009), S. 2-3.

beanspruchte Menge von IT-Ressourcen mit Unsicherheiten verbunden ist. Die Vorhersage der durchschnittlich und auch maximal beanspruchten Menge IT-Ressourcen ist daher nur schwer möglich. Dies erfordert neben der ausreichenden Dimensionierung der Hardware-Infrastruktur auch die Skalierbarkeit dieser. Darüber hinaus muss die verwendete Hardware auf die eingesetzte Virtualisierungssoftware abgestimmt sein.[91] Ist dies nicht der Fall, besteht die Gefahr großer Leistungsschwankungen und die durch die Cloud-Nutzer angeforderte Leistung kann möglicherweise nicht garantiert werden. Eine zusätzliche Anforderung betrifft den Netzwerkzugriff. Er gehört zu den grundlegenden Eigenschaften des Cloud-Computing. Daher muss der Netzwerkzugriff auf die verfügbaren IT-Ressourcen nicht nur jeder Zeit garantiert, sondern auch jeder Zeit mit einer hohen Bandbreite möglich sein.

4.3.3 Anforderungen an die Software-Infrastruktur

Die Anforderungen an die Software-Infrastruktur traditioneller Rechenzentren sind, ähnlich wie die Hardware-Anforderungen zuvor, bisher wenig ausgeprägt. Ausgehend von den drei in Kapitel 2.2.1 beschriebenen Software-Ebenen in Rechenzentren, lassen sich jedoch weitere Anforderungen durch Cloud-Computing auf den Ebenen der Plattform-Level-Software und Application-Level-Software identifizieren. Die Platform-Level-Software wird hierbei durch die verwendete Virtualisierungssoftware und die Application-Level-Software durch die Programmschnittstellen (API) repräsentiert. Darauf aufbauend wird im Folgenden eine Einteilung der Software-Infrastruktur-Anforderungen in die Dimensionen Virtualisierung und Programmschnittstellen vorgenommen.

Die Virtualisierung der Server-Hardware auf Software-Ebene gehört zu den Schlüsseltechnologien des Cloud-Computing.[92] Sie ermöglicht die Aufteilung der Server-Hardware auf mehrere virtuelle Maschinen (VM), die jeweils einen Teil der Leistung eines Servers für sich beanspruchen. Diese als Ressourcenteilung bezeichnete Eigenschaft führt dazu, dass ein und dieselbe Hardware gleichzeitig durch mehrere unterschiedliche Benutzer verwendet wird. Die gleichzeitige Verwendung von

---

[91] Vgl. zu diesem und dem nächsten Satz Armbrust (2009), S. 17-18.

[92] Vgl. Zissis, Lekkas (2012), S. 584.

Hardware durch unterschiedliche Benutzer wird dabei auch als Mandantenfähigkeit oder Multitenancy bezeichnet. Die mit der Mandantenfähigkeit von Cloud-Computing-Umgebungen verbundenen Neuerungen implizieren allerdings die Notwendigkeit neuer Maßnahmen zum Schutz der Nutzer.[93] VMs müssen untereinander so geschützt sein, dass kein Nutzer aus einer VM auf die Daten in einer anderen VM zugreifen kann. Zudem muss die eigentliche Virtualisierungssoftware, auch Hypervisor genannt, gegen Angriffe mit Schadsoftware abgesichert sein. Eine unzureichende Sicherung des Hypervisors kann sich potentiell auf alle von ihm verwalteten VMs auswirken und stellt daher eine große Gefahr für die Sicherheit der Nutzerdaten dar.

Jeder Cloud-Computing-Dienst stellt seinen Nutzern bestimmte APIs bereit, um ihnen den Zugriff auf die verfügbaren IT-Ressourcen zu ermöglichen.[94] Die sichere Gestaltung dieser APIs ist deshalb relevant, da die Verwendung in einer nicht beabsichtigten Art und Weise ein Sicherheitsrisiko für andere Benutzer darstellt.[95] APIs mit Sicherheitslücken oder nicht ausreichend gegen Manipulation geschützte APIs könnten etwa dazu führen, dass einige Nutzer mehr Ressourcen beanspruchen, als ihnen zustehen. Dies bedeutet unweigerlich eine Minderung der Leistung für andere Nutzer und Umsatzverluste für betroffene Cloud-Anbieter[96]. Darüber hinaus ist eine oft genannte Sorge möglicher Cloud-Nutzer ein Daten-Lock-In. Die bereitgestellten APIs sollten deswegen so gestaltet werden, dass die Möglichkeit besteht Daten mit möglichst wenig Aufwand auf einen anderen Cloud-Computing-Dienst zu übertragen. Ebenfalls erfordern die Eigenschaft der Messbarkeit des Cloud-Computing-Dienstes und die Notwendigkeit zur bedarfsgerechten Abrechnung, dass die angebotenen APIs die Ressourcennutzung protokollieren und diese Daten für Nutzer und Anbieter gleichermaßen verfügbar machen.

---

[93] Vgl. zu diesem und den nächsten drei Sätzen Dubie (2008), S. 23-24.

[94] Vgl. zu diesem und dem nächsten Satz Zissis, Lekkas (2010), S. 586.

[96] Daten-Lock-In meint einen Zustand, bei dem der Wechsel des Cloud-Nutzers zu einem anderen Cloud-Anbieter nur schwer möglich ist, da keine standardisierten Verfahren existieren die Daten des Cloud-Nutzers auf einen anderen Anbieter zu übertragen. Ein Wechsel ist in diesem Fall nicht mehr wirtschaftlich.

4.3.4 Anforderungen an das Management

Obgleich die in Kapitel 4.2.4 erläuterten Anforderungen bereits einige Aspekte des Managements von Cloud-Rechenzentren abdecken lassen sich ausgehend von den grundlegenden Eigenschaften des Cloud-Computing weitere Anforderungen ableiten. Das betrifft insbesondere die Prozesse der Cloud-Rechenzentren und weniger die das Personal oder die Dokumentation. So erfordert die On-Demand-Self-Service-Eigenschaft die weitestgehende Automatisierung der Bereitstellung von IT-Ressourcen. Auch erfordert sie die Möglichkeit den zukünftigen Bedarf an Ressourcen vorhersagen zu können, um eine sichere Planung zu ermöglichen. Zu den Charakteristika des Cloud-Computing gehört, dass die von Cloud-Nutzern beanspruchten Ressourcen stets dem aktuellen Bedarf entsprechen und sie nur für die Leistung Aufkommen müssen, die sie auch tatsächlich benötigen. Demnach sind Maßnahmen zu treffen, die eine Abrechnung gemäß den tatsächlich beanspruchten IT-Ressourcen ermöglichen.

Ferner sind aufgrund der Sicherheitsbedenken potentieller Cloud-Nutzer auch auf der Ebene des Managements entsprechende Maßnahmen zu realisieren, die die Nutzer der Cloud-Computing-Dienste vor möglichen Sicherheitsrisiken schützen. Das betrifft sowohl den Schutz vor Sicherheitsrisiken von außen als auch den Schutz der Cloud-Nutzer untereinander. Zwei diesbezüglich genannte Probleme sind die sogenannten Malicious-Insider und das Reputation-Fate-Sharing.[97] Malicious-Insider sind Cloud-Nutzer, die mögliche Sicherheitslücken des Systems ausnutzen, um anderen Nutzern Schaden zu zufügen oder an deren Daten zu gelangen. Reputation-Fate-Sharing bezeichnet einen Umstand, bei dem das schlechte Verhalten eines Nutzers, die Reputation aller anderen Nutzer des selben Cloud-Dienstes negativ beeinflusst.[98] Ein weiteres Problem betrifft darüber hinaus die Beschlagnahme von Hardware durch Sicherheitsbehörden. Wegen der angewandten Ressourcenteilung besteht hier grundsätzlich die Gefahr, dass durch das Unrechtmäßige Verhalten eines Nutzers auch andere Nutzer betroffen sind. Daher sind ebenfalls Maßnahmen notwendig, die Cloud-Nutzer vor dieser Gefahr schützen.

---

[97] Vgl. zu Maclicious-Insider Marston u. a. (2011), S. 187;
Vgl. zu Reputation-Fate-Sharing Armbrust u. a. (2009), S. 18.

[98] Ein praktisches Beispiel hierfür ist das sogenannte IP-Blacklisting. Dabei wird der Zugriff auf einen Dienstes anhand der IP seines Servers gesperrt. Wegen der gemeinsam genutzten Hardware können dabei jedoch auch andere Dienste unabsichtlich gesperrt.

4.4 Kriterien und Richtwerte zur Zertifizierung von Cloud-Rechenzentren

Auf Basis der zuvor erarbeiteten Anforderungen an Rechenzentren durch Cloud-Computing werden in diesem Kapitel Kriterien und Richtwerte beschrieben, die bei der Entwicklung von Standards zur Zertifizierung von Cloud-Rechenzentren berücksichtigt werden sollten. Im Unterschied zu den in Kapitel 4.3 erläuterten Anforderungen stellen die hier genannten Kriterien und Richtwerte konkrete und nach Ansicht des Verfassers best mögliche Ausprägungen dar diese zu realisieren. Dabei wird davon ausgegangen, dass alle zuvor genannten Anforderungen an traditionelle Rechenzentren auch auf Cloud-Rechenzentren zutreffen. Aus diesem Grund wird in diesem Abschnitt nicht näher auf sie eingegangen. Stattdessen werden lediglich solche Kriterien beschrieben, die sich direkt oder indirekt aus den zuvor beschriebenen spezifischen Cloud-Computing-Anforderungen ergeben.

4.4.1 Kriterien zur Bewertung der Gebäude-Infrastruktur

Die in den Kapiteln 4.2.1 und 4.3.1 beschriebenen Anforderungen an die Gebäude-Infrastruktur von traditionellen Rechenzentren und Cloud-Rechenzentren haben zum Ziel die Ansprüche potentieller Cloud-Nutzer an die Sicherheit und Verfügbarkeit von Cloud-Computing-Diensten zu befriedigen. Die Unterbringen des Rechenzentrums in einem Gebäude mit mehreren Parteien erscheint deshalb im Falle von Cloud-Rechenzentren nicht empfehlenswert, da dies nicht nur ein Sicherheitsrisiko durch die anderen Parteien bedeuten würde, sondern auch der verfügbare Platz für die, zum Betrieb von Cloud-Computing benötigten Menge von IT-Ressourcen in der Regel nicht ausreicht. Ein dediziertes Glände mit ausreichend dimensionierten Räumlichkeiten ist im Hinblick auf die beiden Aspekte Sicherheit und Skalierbarkeit von Cloud-Rechenzentren folglich notwendig. Darüber hinaus müssen die Systeme zur Energieversorgung und Klimatisierung der Rechenzentren mehrfach redundant vorhanden sein, sodass die Erreichbarkeit des Dienstes zu jedem Zeitpunkt garantiert ist und die Anlagen und IT-Systeme regelmäßig gewartet werden können. Eine einfache Redundanz würde in diesem Fall keine ausreichende Verfügbarkeit garantieren, denn

bei Anwendung einfacher Redundanzen bestünde während Wartungsarbeiten ein erhöhtes Ausfallrisiko.[99]

4.4.2 Kriterien zur Bewertung der Hardware-Infrastruktur

Die Analyse der Anforderungen an die Hardware-Infrastuktur von Cloud-Rechenzentren hat gezeigt, dass diese vor allem drei zentrale Eigenschaften besitzen muss. Sie muss ausreichend dimensioniert, skalierbar und durch den Cloud-Nutzer selbstständig und kurzfristig zu beanspruchen sein. Die beiden erstgenannten Eigenschaften lassen sich hierbei durch den Einsatz von Custom-off-the-Shelf-Hardware[100] (COTS-Hardware) realisieren. Sie steht in einer großen Stückzahl und zu verhältnismäßig geringen Kosten zur Verfügung.[101] Ergänzend dazu ist COTS-Hardware aufgrund der großen Produktionsmengen auch kurzfristig zu beschaffen und kann somit die Forderung nach der Skalierbarkeit der Hardware-Infrastruktur bedienen. Die Verwendung von COTS-Hardware ist ausgehend von den zuvor genannten Aspekten daher, aus Sicht des Verfassers ein wichtiges Kriterium für die Bewertung von Cloud-Rechenzentren. Vor dem Hintergrund der in Kapitel 4.3.2 beschriebenen Notwendigkeit zur Abstimmung der Hardware mit der eingesetzten Virtualisierungssoftware stellt sich zudem die Frage, inwieweit spezialisierte Hardware von den verfügbaren Virtualisierungslösungen unterstützt wird. Daran anschließend sollte auch die Verwendung von Sekundärspeichern auf Basis der Flash-Technologie als ein Kriterium bei der Bewertung der Hardware berücksichtigt werden. Es hat sich gezeigt dass besonders die Daten-Durchsatzrate von Sekundärspeichern in virtualisierten Umgebungen großen Schwankungen unterlegen ist.[102] Der Einsatz von Flashspeicher-Technologie kann diese durch eine insgesamt höhere Daten-Durchsatzrate und das Fehlen mechanischer Bauteile möglicherweise kompensieren. Ferner erfordern die in Kapitel 4.3.2 erläuterten Unsicherheiten im Bezug auf die beanspruchte Menge von IT-Ressourcen, dass eine Überversorgung mit Hardware vorhanden ist, um stets den maximalen Anforderungen entsprechen zu können. Im

---

[99] Vgl. zu UTI (2012b), S. 1-2, 4.

[100] COTS-Hardware bezeichnet handelübliche Hardware, die in standardisierter Weise produziert wird und in großen Mengen verfügbar ist.

[101] Vgl. Barroso, Hölzle (2009), S. 92.

[102] Vgl. zu diesem und dem nächsten Satz Armbrust u. a. (2009), S. 17.

Vergleich zu herkömmlichen Rechenzentren zeigt sich also, dass das Risiko der Überversorgung mit Hardware von Cloud-Nutzern zu Cloud-Anbietern übergeht.[103] Die angemessene Überversorgung mit Hardware ist demnach ebenfalls ein wichtiges Kriterium. Zuletzt müssen die Netzwerke von Cloud-Rechenzentren so gestaltet sein, dass sie jeder Zeit einen schnellen Zugriff auf die verfügbaren Ressourcen ermöglichen, da der umfassende Netzwerkzugriff ebenfalls eine grundlegende Eigenschaft des Cloud-Computing ist. Dies kann etwa durch eine mehrfach redundante Anbindung der Rechenzentren an unabhängige ISPs erfüllt werden.

4.4.3 Kriterien zur Bewertung der Software-Infrastruktur

Die Anforderungen an die Software-Infrastruktur von Cloud-Rechenzentren haben gezeigt, dass insbesondere die eingesetzte Virtualisierungssoftware und die bereitgestellte API für deren Bewertung relevant sind. Die Virtualisierungssoftware muss dabei dem aktuellen Stand der Technik entsprechen, um die verwalteten VMs und damit letztlich die Daten der Nutzer vor unbefugten Zugriffen und Missbrauch schützen zu können. Dies beinhaltet auch das regelmäßige Einspielen von Sicherheitsaktualisierungen für den Hypervisor und die von ihm verwalteten VMs. Außerdem ist möglicherweise der Einsatz entsprechender Software zum Schutz der VMs und des Hypervisors, zusätzlich zur obligatorischen Software zum Schutz vor herkömmlicher Schadsoftware und Firewalls erforderlich. Die bereitsgestellte API muss gegen Manipulation abgesichert sein und entsprechende Mechanismen und Best-Practices implementieren. Auch muss sie eine Komponente zur Überwachung der beanspruchten Ressourcen enthalten, die diese in Echtzeit aufzeichnet und es dem System ermöglicht automatisch auf die gelieferten Daten zu reagieren. Dies ist notwendig, um die Messbarkeit und kurzfristige Elastizität von Cloud-Computing-Diensten zu realisieren. Eine weitere Befürchtung potentieller Cloud-Nutzer ist die Gefahr eines Daten-Lock-Ins und die Insolvenz des Cloud-Anbieters.[104] Um diesen Befürchtungen entgegenwirken zu können, sollten die verwendete Virtualisierungssoftware und die bereitgestellten APIs auf Standards basieren, soweit diese existieren. Standardisierte Formate zur Speicherung der Daten und der Einsatz von

---

[103] Vgl. Armbrust u. a. (2009), S. 10.

[104] Vgl. zu diesem und den nächsten beiden Sätzn Armbrust u. a. (2009), S. 15.

auf Standards beruhender Software zum Übertragen der Daten erleichtern es Nutzern bei Bedarf den Anbieter zu wechseln. Damit verringern sich die Gefahren durch mögliche Daten-Lock-Ins.[105]

4.4.4 Kriterien zur Bewertung der Managementmaßnahmen

Die in Kapitel 4.3.4 aufgezeigten Management-Anforderungen in Cloud-Umgebungen verdeutlichen, dass in diesem Bereich gegenüber herkömmlichen Rechenzentrum-Zertifizierungen weitere Kriterien berücksichtigt werden müssen. Bezogen auf die On-Demand-Self-Service-Eigenschaft bedeutet dies, dass in jedem Cloud-Rechenzentrum Prozesse implementiert werden müssen, die eine automatisierte Bereitstellung der benötigten IT-Ressourcen in Form von VMs ermöglichen. Darüber hinaus müssen bestehende Prozesse zur Vorhersage der zukünftigen Entwicklung der Leistungsbeanspruchung auf die Bedürfnisse der Cloud-Nutzer angepasst werden. Auch wenn, wie in Kapitel 4.3.2 thematisiert wurde, eine genaue Prognose durch die Eigenschaften des Cloud-Computing erschwert wird, kann aus Gründen der Planungssicherheit nicht vollkommen darauf verzichtet werden. Um zum Beispiel eine angemessene, aber nicht zu große Überversorgung mit Ressourcen zu garantieren. Dabei müssen vor allem Leistungsschwankungen in virtualisierten Umgebungen berücksichtigt werden. Ebenfalls müssen die für den Betrieb des Hypervisors und der VMs benötigten Ressourcen mit in die Prognose einfließen, da sie aus der Sicht des Verfassers nicht zu den durch die Cloud-Nutzer beanspruchten Ressourcen gezählt werden dürfen. Eine solche Hinzurechnung zu den von Cloud-Nutzern beanspruchten IT-Ressourcen würde der bedarfsgerechten Abrechnung widersprechen, denn die zum Betrieb der Virtualisierungssoftware verwendeten Ressourcen können nicht direkt durch den Cloud-Nutzer genutzt werden. Daher muss bei der Bewertung von Cloud-Rechenzentren auch berücksichtigt werden, dass Abrechnungsprozesse installiert sind, die eine exakte und bedarfsgerechte Abrechnung ermöglichen. Schließlich müssen bei der Bewertung von Cloud-Rechenzentren auch solche Kriterien berücksichtigt werden, die die Sicherheit der Cloud-Nutzer durch Managementmaßnahmen sicherstellen. Dazu gehört in erster Linie dass es Prozesse gibt, die Cloud-Nutzer zeitnah über mögliche Sicherheitsrisiken informieren. Dadurch wird den Nutzern die Möglichkeit eingeräumt

---

[105] Vgl. Armbrust u. a. (2009), S. 15.

rechtzeitig auf Gefahren, wie zum Beispiel Datendiebstahl reagieren zu können. Unter Berücksichtigung der Tatsache, dass es viele hundert bis tausend VMs in Cloud-Rechenzentren gibt, sollten auch Prozesse existieren, die Verwaltung einer so großen Anzahl von VMs ermöglichen. Die Verwaltung beinhaltet dabei z. B. das systematische Patching[106] der VMs. Ohne solche Prozesse kann die Gefahr bestehen, dass der Überblick über die Verwaltung der VMs verloren geht. Auch würde es ein unstrukturiertes Vorgehen erschweren Fehler im System zu erkennen und z.B. fehlerhafte Patches rückgängig zu machen. Vor dem Hintergrund der Gefahren durch Malicious-Insider, Reputation-Fate-Sharing und die mögliche Beschlagnahmung der Hardware durch Sicherheitsbehörden ist darüber hinaus die Existenz weiterer Prozesse zum Schutz der Nutzer bei der Bewertung zu berücksichtigen. Neben Prozessen zur Information der Nutzer bieten sich hier auch solche Prozesse an, die im Falle von Malicious-Insidern, einer schlechten Reputation oder der tatsächlich bevorstehenden Beschlagnahmung der Hardware, die VMs der Nutzer automatisch auf andere Hardware oder in ein anderes Rechenzentrum übertragen, um auch weiterhin den Zugriff auf die Daten der anderen Cloud-Nutzer gewährleisten zu können. Dazu empfiehlt sich auch die redundante Daten-Anbindung an ein weiteres Rechenzentrum. Durch diese können die Risiken durch Ausfälle des Systems gemindert und den Verfügbarkeitsansprüchen der Cloud-Nutzer besser entsprochen werden.

[106] Patching bezeichnet die Behebung von Fehlern und Sicherheitslücken in Softwareprodukten.

5. Fazit

Die vorliegende Arbeit hat vor dem Hintergrund der Cloud-Computing inhärenten Eigenschaften und den damit verbundenen Risiken und Bedenken potentieller Cloud-Nutzer die besonderen Anforderungen an Cloud-Rechenzentren aufgezeigt. Die Gegenüberstellung existierender Zertifizierungen für traditionelle Rechenzentren machte dabei deutlich, dass in einigen Bereichen bereits hohe Anforderungen an diese gestellt werden. Dies gilt insbesondere für die beiden Bereiche Gebäude-Infrastruktur und Management. Ferner zeigte die Analyse der Hardware- und Software-Anforderungen, dass diese unter den untersuchten Zertifizierungen wenig ausgeprägt sind. Die spezifischen Eigenschaften des Cloud-Computing und damit einhergehende Bedenken der Cloud-Nutzer erfordern jedoch, weitere Anforderungen an die Hardware und Software der Cloud-Rechenzentren. Auch hat Kapitel 4.3.4 deutlich gemacht, dass sich trotz der bereits breiten Anforderungen an das Management weitere Anforderungen durch den Betrieb von Cloud-Computing ergeben. Die auf dieser Grundlage in Kapitel 4.4 erarbeiteten Kriterien zur Zertifizierung von Cloud-Rechenzentren helfen dabei, nach Ansicht des Verfasser, das Vertrauen möglicher Cloud-Nutzer in diese Technologie zu steigern und sollten daher bei der Entwicklung eines Zertifizierungsstandards für Cloud-Computing berücksichtigt werden.

Abschließend erhebt die vorliegende Arbeit aufgrund der geringen Anzahl von insgesamt nur vier untersuchten Zertifizierungen keinen Anspruch auch Vollständigkeit im Bezug auf die Existenz weiterer möglicher Anforderungen an Rechenzentren. So konnte bspw. eine von ingesamt fünf Zertifizierungen in der engeren Auswahl, die TIA-492, aufgrund des fehlenden Kriterienkatalogs nicht genauer untersucht werden, obwohl die Suche zeigte, dass sie häufig als eine relevante Zertifizierung für Rechenzentren genannt wird. Ebenfalls befindet sich der Kriterienkatalog des DCSA zum Zeitpunkt dieser Arbeit in Überarbeitung. Eine Untersuchung der TIA-492 und der aktualisierten Version des DCSA Kriterienkataloges unter Berücksichtigung der Ergebnisse der vorliegenden Arbeit könnte daher weitere Anforderungen liefern, oder zumindest die bereits erarbeiteten Kriterien fundieren. Darüber hinaus erfolgte die Herleitung der in Kapitel 4.4 aufgezeigten Kriterien in erster Linie aus der Sicht potentieller Cloud-Nutzer und im Hinblick auf die sich daraus ergebenden Implikationen für Cloud-Anbieter. Sie adressieren die Bedenken und Ansprüche der Cloud-Nutzer und gehen

daher in der Regel von Maximalanforderungen[107] aus. Deshalb ist unter den identifizierten Anforderungen und Kriterien ein Fokus auf die On-Demand-Self-Service-Eigenschaft und die kurzfristige Elastizität des Cloud-Computing zu erkennen. Eine Betrachtung aus der Sicht der Cloud-Anbieter könnte aus diesem Grund weitere Anforderungen liefern, die bisher noch nicht berücksichtigt wurden und sollte deshalb weiter erforscht werden. Dies betrifft insbesondere mögliche Folgen im Bezug auf die Kosten durch den Betrieb und die Energieeffizienz[108] sehr großer Rechenzentren. Ebenfalls unberücksichtigt blieben die möglichen rechtlichen Folgen die sich durch die unterschiedlichen Gesetzgebungen in den verschiedenen Ländern ergeben. Vor dem Hintergrund der Unsicherheiten aufgrund vieler unterschiedlicher Datenschutzgesetze und deren Komplexität gilt es zu klären, welche Rechte und Pflichten sowohl Cloud-Anbieter, als auch Cloud-Nutzer in den jeweiligen Ländern haben und wie diese an potentielle Cloud-Nutzer kommuniziert werden können. Eine ausführliche Untersuchung der weltweit wichtigsten Datenschutzgesetze unter Berücksichtigung der besonderen Eigenschaften des Cloud-Computing und den sich daraus ergebenden Implikationen für den Betrieb von Cloud-Rechenzentren sollte darum angestrebt werden. Die Recherche nach existierenden Rechenzentrum-Zertifizierungen hat zudem gezeigt, dass es eine Vielzahl verschiedener Zertifizierungen für Rechenzentrum-Personal gibt. Es stellt sich daher auch die Frage, welche allgemeinen Anforderungen an das Personal eines Cloud-Rechenzentrums gestellt werden.

---

[107] Maximalanforderungen bezeichnet die aus sicht der Cloud-Nutzer best mögliche Ausstattung, ohne dabei mögliche Folgen wie Kosten und Energieeffizienz zu berücksichtigen.

[108] Ein häufig mit der Energieeffizienz von Rechenzentren in Verbindung gebrachter Begriff ist der, der Green-IT.

Literaturverzeichnis

AICPA (2012a)

American Institute of Certified Public Accountants, Inc. (Hrsg.): SOC 3. Trust Services Report for Service Organisations. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC3Report.aspx, Abruf am 16.09.2012.

AICPA (2012b)

American Institute of Certified Public Accountants, Inc. (Hrsg.): About the AICPA. http://www.aicpa.org/About/Pages/About.aspx, Abruf am 17.09.2012.

AICPA, CICA (2009)

American Institute of Certified Public Accountants, Inc. (Hrsg.), Canadian Institute of Chartered Accountants (Hrsg): TRUST SERVICES PRINCIPLES, CRITERIA, AND ILLUSTRATIONS. http://www.webtrust.org/item27806.doc, Abruf am 20.08.2012.

Alexa Internet, Inc. (2012)

Alexa Internet, Inc (Hrsg.): Alexa Top 500 Global Sites. http://www.alexa.com/topsites/global, Abruf am 14.09.2012.

Abts, Felderman (2012)

Dennis Abts, Bob Felderman: A guided tour of data-center networking. In: Communications of the ACM, Jg. 55, 2012, S. 44-51.

Arraj (2010)

Valerie Arraj: ITIL: The Basics. http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf, Abruf ab 0.7.09.2012.

Armbrust u. a. (2009)

Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia: Above the Clouds. A Berkeley View of Cloud Computing. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, Abruf am 04.08.2012.

Barroso, Hölzle (2009)

Luiz André Barroso, Urs Hölzle: The Datacenter as a Computer. An Introduction to the Design of Warehouse-Scale Machines. In: Synthesis Lectures on Computer Architecture, Jg. 4, 2009, S. 1-108.

BBC NEWS (2009)

BBC NEWS (Hrsg.): Microsoft and Yahoo seal web deal. http://news.bbc.co.uk/2/hi/business/8174763.stm, Abruf am 14.09.2012.

Brodkin (2008)

Jon Brodkin: Loss of customer data spurs closure of online storage service ‚The Linkup'. http://www.networkworld.com/news/2008/081108-linkup-failure.html, Abruf am 10.08.2012.

Clemons, Chen (2011)

Eric K. Clemons, Yuanyuan Chen: Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing. In: IEEE (Hrsg.): Proceedings of the 44th Hawaii International Conference on System Sciences HICSS (2011), Jan. 4 - 7, 2011, Kauai, Hawaii, HI, USA, S. 1-10.

Dubie (2008)

Denise Dubie: Security concerns cloud virtualization deployments. In: NetworkWorld Asia, Jg. 4, 2008, S. 23-24.

Dwivedi, Mustafee (2010)

Yogesh K. Dwivedi, Navonil Mustafee: It's unwritten in the Cloud: the technology enablers for realising the promise of Cloud Computing. In: Journal of Enterprise Information Management, Jg. 23, 2010, S. 673-679.

eco Verband (2012a)

eco – Verband deutscher Internetwirtschaft e. V. (Hrsg.): Wir gestalten das Internet | eco – Verband der deutschen Internetwirtschaft e.V. http://www.eco.de/about.html, Abruf am 16.09.2012.

eco Verband (2012b)

eco – Verband deutscher Internetwirtschaft e. V. (Hrsg.): Datacenter Star Audit (DCSA) | The quality standard for your Data Center. http://www.dcaudit.de, Abruf am 16.09.2012.

eco Verband (2012c)

eco – Verband deutscher Internetwirtschaft e. V. (Hrsg.): Erfüllungsgrade Datacenter Star Audit. http://www.dcaudit.de/wp-content/blogs.dir/11/files/2009/12/de_performance_levels.pdf, Abruf am 31.08.2012.

eco Verband (o. J.)

eco – Verband deutscher Internetwirtschaft e. V. (Hrsg.): Anlage 1/1 zum eco Datacenter Star Audit Vertrag. Request for Information.

Hansel (2012)

Sven Hansel: Unternehmen müssen sich "Cloud-ready" machen. http://www.wiso-net.de/genios1.pdf?START=0A1&ANR=2109713&DBN=ZGEN&ZNR=1&ZHW=-7&WID=27032-2290582-82223_1, Abruf am 11.08.2012.

Ho (2011)

Victoria Ho: Lack of security standard deters cloud adoption. Firms slow to come on board without certifications that address continuity. In: The Business Times, 24.10.2011. Abgerufen über http://search.proquest.com/docview/900187496?accountid=10218, Abruf am 11.08.2012.

Jabs u. a. (2010)

Andreas Jabs, Oliver Thörner, Hans Wicklein, Roland Broch: Das zertifizierte RZ. Herausforderungen in Zeiten von Outsourcing, SaaS und Cloud Computing. http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=ZWIW&DOKV_NO=BEFO20100805968-E-FIZT-BEFO-DOMA-ZDEE&DOKV_HS=0&PP=1, Abruf am 16.09.2012.

Kant (2009)

Krishna Kant: Data center evolution. A tutorial on state of the art, issues, and challenges. In: Computer Networks, Jg. 53, 2009, S. 2939-2965.

Khan, Malluhi (2010)

Khaled M. Khan, Qutaibah Malluhi: Establishing Trust in Cloud Computing. In: IT Professional, Jg. 12, 2010, S. 20-27.

Marston u. a. (2011)

Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi: Cloud Computing — The business perspective. In: Decision Support Systems. Jg. 51, 2011, S. 176-189.

Marwah u. a. (2010)

Manish Marwah, Paulo Maciel, Amip Shah, Ratnesh Sharma, Tom Christian, Virgilio Almeida; Carlos Araújo, Erica Souza, Gustavo Callou, Bruno Silva, Sérgio Galdino, Jose Pires: Quantifying the sustainability impact of data center availability. In: SIGMETRICS Perform. Eval. Rev, Jg. 37, 2010, S. 64-68.

Mell, Grance (2009)

Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Abruf am 04.08.2012.

Pauley (2010)

Wayne A. Pauley: Cloud Provider Transparency – An Empirical Evaluation. In: IEEE Security & Privacy, Jg. 8, 2010, S. 32-39.

Patel, Shah (2005)

Chandrakant D. Patel, Amip J. Shah: Cost Model for Planning, Development and Operation of a Data Center. http://www.hpl.hp.com/techreports/2005/HPL-2005-107R1.pdf, Abruf am 14.09.2012.

Reilly (2011)

Seamus Reilly: Cloud confidence needs new assurance standard. In: Computer Weekly, 14.03.2011, S. 14.

Sultan (2009)

Nabil Sultan: Cloud Computing for education. A new dawn? In: International Journal of Information Management. Jg. 30, 2010, S. 109–116.

TÜViT GmbH (2011)

TÜV Informationstechnik GmbH (Hrsg). Kriterienkatalog: Sichere Infrastrukturen für Informationssysteme. Trusted Site Infrastructure.

UTI (2012a)

Uptime Institute LLC (Hrsg.): About Uptime Institute. http://uptimeinstitute.com/about-us, Abruf a. 16.09.2012.

UTI (2012b)

Uptime Institute LLC (Hrsg.): Data Center Site Infrastructure Tier Standard: Topology. http://uptimeinstitute.com/component/docman/doc_download/5-tiers-standard-topology, Abruf am 07.08.2012.

Woods (2010)

Andy Woods: Cooling the data center. In: Communications of the ACM, Jg. 53, 2010, S. 36-42.

Welz (2012)

Dr. Bernd Welz: eco MMR Kongress zum „Datenschutz 2012“ Datenschutzrechtliche Herausforderungen aus nationaler, europäischer und US-amerikanischer Sicht. http://www.eco.de/wp-content/blogs.dir/20120320-kongressbericht.pdf, Abgerufen am 06.08.2012

Yang, Tate (2012)

Haibo Yang, Mary Tate: A Descriptive Literature Review and Classification of Cloud Computing Research. In: Communications of the Association for Information Systems, Jg. 31, 2012, S. 36-60.

Zissis, Lekkas (2012)

Dimitrios Zissis, Dimitrios Lekkas: Addressing Cloud Computing security issues. In: Future Generation Computer Systems. Jg. 28, 2012, S. 583-592.

Anhang

Name	Abkürzung	Organisation	Webseite
Data Centre Audit	-	Sudlows	http://www.sudlows.com/divisions/data-centre-design-build/data-centre-consultancy-audit/
Data Center Audit	DCA	Emerson Network Power	http://www.emersonnetworkpower.com/en-ASIA/Services/ServiceOfferings/Pages/DataCenterAudit.aspx
Data Center Compliance Certification	DCC	EPI Singapore	http://www.epi-ap.com/data-center-audit-a-certification.html
Data Center Tier Certification	DCTC	International Data Center Authority	http://idc-a.org/data-center-audit-program-dcap.html
Datacenter Star Audit	DCSA	Verband der deutschen Internetwirtschaft e.V.	http://www.dcaudit.de
Data Security Standard	PCI DSS	Payment Card Industry	https://www.pcisecuritystandards.org/security_standards/
ISO/IEC 27001:2005	ISO 27001	International Organisation for Standardization	http://www.iso.org/iso/catalogue_detail?csnumber=42103
Leadership in Energy and Environmental Design	LEED	U.S. Green Building Council	http://www.usgbc.org/DisplayPage.aspx?CategoryID=19
Service Organisation Control 2/3	SSAE16 SOC2/3	American Institute for CPAs	http://www.aicpa.org
Statement on Auditing Standards No. 70: Service Organizations	SAS 70	American Institute for CPAs	http://www.aicpa.org
Telecommunications Infrastructure Standards for Data Centers	TIA-492	Telecommunica-tions Industry Association	http://www.tiaonline.org
Tier Certification	UTI	Uptime Institute	http://uptimeinstitute.com
Trusted Site Infrastructure	TSI	TÜViT	https://www.tuvit.de/de/trusted-site-infrastructure-911.htm

Tab. A-1: Ergebnisse der Suche nach existierenden Rechenzentrum-Zertifizierungen.