Sebastian Lins
Stephan Schneider
Ali Sunyaev

Cloud-Service-Zertifizierung

Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services

2. Auflage

Springer Gabler

Cloud-Service-Zertifizierung

Sebastian Lins • Stephan Schneider
Ali Sunyaev

Cloud-Service-Zertifizierung

Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services

2., aktualisierte und erweiterte Auflage

Springer Gabler

Sebastian Lins
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Stephan Schneider
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Ali Sunyaev
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

ISBN 978-3-662-58856-7 ISBN 978-3-662-58857-4 (eBook)
https://doi.org/10.1007/978-3-662-58857-4

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

Springer Gabler

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Cloud-Computing hat im vergangenen Jahrzehnt ein großes mediales Interesse hervorgerufen. Für Anbieter von IT-Services ergeben sich neue Geschäftsmodelle, indem beispielsweise Softwareanwendungen als Services über das Internet vertrieben werden und durch nutzungsbasierte Kostenabrechnung Einstiegsbarrieren entfallen. Ebenso ergeben sich für regional orientierte, mittelständische IT-Anbieter Möglichkeiten, ihr Angebot über Cloud-Plattformen anzubieten und damit eine breitere Kundenschicht zu erreichen. Für Anwender bietet Cloud-Computing die Möglichkeit, stets aktuelle IT-Ressourcen bei hoher Flexibilität mit geringen Investitionskosten zu beziehen und sich dabei auf ihr Kerngeschäft konzentrieren zu können. Dies ist insbesondere für kleine und mittelständische Unternehmen (KMU) interessant, da diese im Vergleich zu Großunternehmen häufig mit begrenzten Ressourcen arbeiten und durch Cloud-Computing von Skaleneffekten profitieren können.

Neben diesen Vorteilen bringt Cloud-Computing aber auch neue Herausforderungen mit sich. Dazu gehören unter anderem Themen wie Rechtssicherheit beim Auslagern von Daten in andere Rechtsräume, Performanz beim Bezug von IT-Ressourcen über das Internet sowie die Integrationsfähigkeit von standardisierten Services mit einer ggf. über Jahre gewachsenen IT-Landschaft in Unternehmen. IT-Anwender geben zwar ressourcenintensive Aufgaben wie Entwicklung und Wartung von IT-Ressourcen ab, damit einhergehend geben sie jedoch auch die Kontrolle über IT-Sicherheit, Verfügbarkeit und Datenschutz ab und müssen bei deren Einhaltung auf den Cloud-Service-Anbieter vertrauen. Des Weiteren wird die breitenwirksame Nutzung von Cloud-Services durch eine am Markt vorherrschende Informationsasymmetrie gehemmt. Sie erschwert es einerseits Anwendern, Cloud-Services hinsichtlich ihrer individuellen Vorteilhaftigkeit und den

verbundenen Risiken umfassend zu bewerten, und andererseits Anbietern ihr Serviceangebot an den Bedürfnissen potenzieller Kunden auszurichten. Es ist daher eine Grundvoraussetzung für die breitenwirksame Nutzung und Entwicklung innovativer Cloud-Angebote, den Informationsaustausch zwischen Cloud-Service-Anbietern und Cloud-Service-Kunden zu fördern.

Um diese und weitere Herausforderungen zu adressieren, hat das Bundesministerium für Wirtschaft und Technologie das Technologieprogramm Trusted Cloud (www.trusted-cloud.de) als Bestandteil der Hightech-Strategie der Bundesregierung im Jahr 2010 ins Leben gerufen. Das Ziel des Technologieprogramms Trusted Cloud ist die Entwicklung und Erprobung innovativer, sicherer und rechtskonformer Cloud-Computing-Lösungen, von denen insbesondere der deutsche Mittelstand profitieren soll. Dabei liegt ein besonderer Fokus darauf, Technologien und Dienste zu entwickeln, die Transparenz am Markt schaffen, eine einheitliche Bewertung und Beurteilung von Cloud-Services ermöglichen und somit das Vergleichen von Angeboten erleichtern.

Für den Vergleich von Cloud-Angeboten haben sich über die Jahre verschiedene Vergleichsportale und Marktplätze etabliert. Jedoch finden insbesondere mittelständische Cloud-Service-Anbieter auf bestehenden elektronischen Marktplätzen nur bedingt Gehör bei potenziellen Kunden. Kriterien wie bspw. Unternehmensgröße, Reputation oder Umsatz des Cloud-Service-Anbieters haben oft maßgeblichen Einfluss auf die Anbieterauswahl. Dies erschwert es kleineren Cloud-Service-Anbietern sich am Markt zu etablieren. Bewertungen der Cloud-Servicequalität durch unabhängige Prüfinstitutionen können hier Abhilfe schaffen. Insbesondere Cloud-Kunden mit begrenzten Ressourcen können durch unabhängige Bewertungen von Cloud-Services verlässliche Informationen über die zu erwartende Servicequalität erlangen und diese in den Auswahlprozess einbeziehen.

Das Projekt „Value4Cloud“ setzt hier an und hat marktunterstützende Mehrwertdienste für Cloud-Services entwickelt, die auf bestehenden Marktplätzen und Informationsportalen eingebunden werden können. Value4Cloud ist eines von 14 geförderten Projekten im Rahmen des Trusted-Cloud-Technologieprogramms. Value4Cloud zielt unter anderem darauf ab, mittelständische Anwender bei der Bewertung von Qualitätsaspekten von Cloud-Services umfassend zu unterstützen, um Vertrauen in Services und Anbieter zu fördern. Aus dem Projekt Value4Cloud gehen Informationen und Werkzeuge hervor, die das Vertrauen potenzieller Anwender stärken und technische, organisatorische sowie rechtliche Hemmnisse abbauen.

Im Kontext des Forschungsprojekts Value4Cloud haben die Autoren dieses Buchs ein Rahmenwerk zur Zertifizierung von Cloud-Services entwickelt. Die wesentlichen Bestandteile dieses Rahmenwerks bilden Gestaltungsempfehlungen für

Cloud-Service-Zertifizierungen und einen Kriterienkatalog zur Zertifizierung von Cloud-Services, welche in diesem Buch vorgestellt werden. Es zeigt sich, dass Zertifizierungen zur Adressierung bestehender Probleme im Cloud-Service-Markt beitragen können, indem sie Vertrauen schaffen, die Transparenz von Cloud-Services erhöhen, und es Cloud-Service-Anbietern ermöglichen, eingesetzte Systeme und Prozesse zu verbessern.

Der in diesem Buch vorgestellte Kriterienkatalog zur Zertifizierung von Cloud-Services, aber auch bestehende Zertifizierungen am Markt, bspw. das *„Star Audit"* von EuroCloud, suggerieren ein hohes Maß an Sicherheit, Verfügbarkeit und Compliance, bei einer Gültigkeit von ein bis drei Jahren. Aufgrund der inhärenten Dynamik und der ständigen (technischen) Weiterentwicklung von Cloud-Services, werden jedoch hohe Anforderungen an Zertifizierungen gestellt. Daher ist eine langjährige Gültigkeit im Cloud-Computing-Umfeld kritisch zu betrachten. Die Einhaltung bestimmter Anforderungen und Kriterien kann über diesen Zeitraum gefährdet sein, bspw. durch das Auftreten von schwerwiegenden Sicherheitsvorfällen oder Änderungen an der Konfiguration des Cloud-Services.

Um die Glaubwürdigkeit ausgestellter Zertifikate zu erhöhen, und um kontinuierlich sicherzustellen, dass Cloud-Services sicher und zuverlässig angeboten werden, hat das Bundesministerium für Bildung und Forschung fünf Projekte in dem Forschungsbereich „Sicheres Cloud Computing" im Rahmen der Hightech-Strategie der Bundesregierung gefördert und initiiert. Das Projekt „Next Generation Certification" (NGCert; www.ngcert.de) beschäftigt sich mit der Forschung und Entwicklung dynamischer Zertifizierungen für Cloud-Services, die es ermöglichen kritische Anforderungen an Cloud-Services kontinuierlich und (teil-)automatisiert zu überprüfen. Im Kontext des Forschungsprojekts NGCert haben die Autoren dieses Buchs Grundlagen, Metriken, Messmethoden und Gestaltungsrichtlinien zur kontinuierlichen und (teil-)automatisierten Zertifizierung von Cloud-Services erarbeitet und Akzeptanzstudien mit relevanten Akteuren am Markt durchgeführt. Die Ergebnisse dieser Forschung werden in diesem Buch zusammengefasst vorgestellt.

Das Buch richtet sich insbesondere an (potenzielle) Kunden von Cloud-Services, Anbieter von Cloud-Services sowie Anbieter von Cloud-Service-Zertifizierungen. Es dient (potenziellen) Cloud-Service-Kunden als Kriterienkatalog und Entscheidungshilfe, um Cloud-Angebote zu bewerten, vergleichen und auszuwählen. Zudem zeigt es den Bedarf und den Mehrwert für Cloud-Service-Kunden von kontinuierlichen Zertifizierungen auf. Es dient Cloud-Service-Anbietern als Kriterienkatalog zum Self-Assessment und zur Verbesserung eigener Services. Durch die Einführung einer kontinuierlichen Zertifizierung werden Vorteile für Cloud-Service-Anbieter aufgezeigt, Maßnahmen zur Teilnahme an einer

kontinuierlichen Zertifizierung vorgestellt und Lösungsansätze zur Bewältigung möglicher Herausforderungen bei einer Teilnahme diskutiert. Außerdem dient das Buch Anbietern von Cloud-Service-Zertifizierungen als Kriterienkatalog und Rahmenwerk zur Beurteilung und zur Verbesserung des eigenen Kriterienkatalogs und Zertifizierungsrahmenwerks. Durch die umfassende Einführung und Diskussion von kontinuierlichen Zertifizierungsverfahren wird diesen Anbietern zudem aufgezeigt, wie sie zukünftig ihre Prozesse zur Überprüfung automatisieren können, um eine neue Generation von transparenten und fortlaufend gültigen Zertifizierungen anbieten zu können.

Wir möchten den Value4Cloud- und NGCert-Projektkonsortien für die hervorragende Zusammenarbeit in den Projekten danken: Fortiss und dem Lehrstuhl für Wirtschaftsinformatik, Technische Universität München (Prof. Dr. Helmut Krcmar), Universität Kassel (Prof. Dr. Jan-Marco Leimeister, Prof. Dr. Alexander Roßnagel), SpaceNet (Sebastian von Bomhard), Gate – Technologiezentrum und Gründerzentrum gate Garching (Dr. Franz Glatz), Universität Passau (Prof. Dr. Hermann de Meer), Fujitsu Technology Solutions (Britta Laatzen), EuroCloud Deutschland_eco e.V. und eco – Verband der Internetwirtschaft (Andreas Weiss, Christine Neubauer). Für die Mitarbeit und Unterstützung bei der Ausarbeitung des Kriterienkatalogs möchten wir uns beim TÜV Rheinland sowie weiteren Feld- und Transferpartnern bedanken. Ebenso möchten wir uns bei Jens Lansing, Heiner Teigeler, Scott Thiebes und Fangjian Gao für ihre Mitarbeit bedanken.

Die diesem Buch zugrunde liegenden Vorhaben Value4Cloud und NGCert wurden mit Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen 01MD11043A, und Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0079 gefördert. Die Vorhaben und die Ergebnisse des Buches fließen auch in aktuelle Forschungsprojekte des Karlsruher Instituts für Technologie ein. So wird im Projekt AUDITOR (www.auditor-cert.de) eine Datenschutzzertifizierung für Cloud-Services entwickelt und berücksichtigt erstmals die kontinuierliche Überprüfung von Zertifizierungskriterien.

Sebastian Lins
Dr. Stephan Schneider
Prof. Dr. Ali Sunyaev

Inhaltsverzeichnis

Einleitung

1

Zusammenfassung

Dieses Kapitel motiviert die Relevanz von (kontinuierlichen) Cloud-Service-Zertifizierungen und beschreibt den Beitrag des Buches.

Cloud-Computing ist ein zentraler Wachstumsmotor und Innovationstreiber, welcher bereits die gesamte IT-Branche nachhaltig verändert hat (Benlian et al. 2018). Cloud-Computing beschreibt die bedarfsgerechte und flexible Bereitstellung und Nutzung von IT-Ressourcen als Service über das Internet (aus der „Wolke"). IT-Ressourcen können sich dabei auf Software (Software as a Service), Plattformen für die Entwicklung und den Betrieb von Anwendungen (Platform as a Service) sowie Infrastruktur in Form von Speicher und Rechenleistung (Infrastructure as a Service) beziehen (Mell und Grance 2011). Das Cloud-Computing-Ökosystem ist jedoch durch Unsicherheiten und einem Mangel an Transparenz geprägt (Sunyaev und Schneider 2013; Fernandes et al. 2014) und die Adoption von Cloud-Services ist durch Hemmschwellen wie bspw. Sicherheitsrisiken, Kontrollverlust über die eigenen Daten, und intransparente Preismodellen erschwert (Schneider und Sunyaev 2016). Kunden haben es weiterhin schwer, Cloud-Services hinsichtlich ihrer individuellen Vorteile und den verbundenen Risiken umfassend zu bewerten.

In diesem Zusammenhang können Zertifizierungen von Cloud-Services Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Kundenseite erhöhen sowie es Cloud-Service-Anbietern ermöglichen, ihre Systeme und Prozesse zu überprüfen

S. Lins et al., *Cloud-Service-Zertifizierung*,
https://doi.org/10.1007/978-3-662-58857-4_1

und zu verbessern (Sunyaev und Schneider 2013; Lins et al. 2016). In diesem Buch werden Forschungsergebnisse von zwei dreijährigen Forschungsprojekten vorgestellt. Zum einen das Forschungsprojekt „Value4Cloud“ das vom Bundesministerium für Wirtschaft und Technologie im Rahmen des Technologieprogramms „Trusted Cloud“ gefördert wurde. Im Kontext des Forschungsprojekts „Value4Cloud“ haben die Autoren ein Rahmenwerk zur Zertifizierung von Cloud-Services entwickelt, das praxisnahe Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen beschreibt. Zum anderen das Forschungsprojekt „Next Generation Certification“ (NGCert) das vom Bundesministerium für Bildung und Forschung in dem Forschungsbereich „Sicheres Cloud Computing“ im Rahmen der Hightech-Strategie der Bundesregierung gefördert wurde. Im Rahmen von NGCert haben die Autoren dieses Buchs Grundlagen, Metriken, Messmethoden und Gestaltungsrichtlinien zur kontinuierlichen und (teil-)automatisierten Zertifizierung von Cloud-Services erarbeitet und Akzeptanzstudien mit relevanten Akteuren am Markt durchgeführt. Die Ergebnisse dieser Forschung werden in diesem Buch zusammengefasst vorgestellt.

Dieses Buch adressiert insbesondere die Problematik, dass Kriterienkataloge von Cloud-Service-Zertifizierungen von den meisten Anbietern von Zertifizierungen als proprietäres Eigentum behandelt werden und daher nur auf einem sehr abstrakten Level veröffentlicht sind. Somit müssen Cloud-Kunden nicht nur den Cloud-Service vertrauen, sondern auch in die Umfänglichkeit der Zertifizierung. Wenn Cloud-Kunden sehr spezifische Anforderungen haben, reicht ein solch abstraktes Informationslevel jedoch nicht aus. Ob spezifische Anforderungen von Cloud-Kunden im Rahmen der Zertifizierung überprüft worden sind, ist somit nicht immer ersichtlich. Dieses Buch stellt eine umfangreiche Sammlung von Kriterien zur Zertifizierung von Cloud-Services mit Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen bereit. Es dient somit als zentrales Nachschlagewerk für (potenzielle) Kunden von Cloud-Services, Anbieter von Cloud-Services sowie Anbieter von Cloud-Service-Zertifizierungen. Potenzielle Cloud-Service-Kunden können den Kriterienkatalog als Entscheidungshilfe heranziehen, um Cloud-Angebote zu bewerten, vergleichen und auszuwählen. Der Kriterienkatalog kann dazu verwendet werden, Anforderungslisten für Cloud-Services zu erstellen bzw. existierende Listen zu ergänzen. Als umfassende Anforderungsliste, die auf etablierten Cloud-Standards aufbaut und mit Experten aus dem Cloud-Umfeld praxisnah geschärft wurde, können insbesondere kleine und mittelständische Unternehmen, die noch wenig Erfahrungen im Cloud-Umfeld gesammelt haben, auf einer umfangreichen und soliden Basis Cloud-Services vergleichen und vermeiden somit, dass eventuell wichtige sicherheitskritische oder regulatorische Anforderungen übersehen werden. Die Gestaltungsempfehlungen können dazu herangezogen

werden, Cloud-Service-Zertifikate aus Kundensicht zu bewerten und bspw. Cloud-Services zu vergleichen, die mit unterschiedlichen Zertifikaten zertifiziert worden sind. Cloud-Service-Anbieter können den Kriterienkatalog zum Self-Assessment und zur Verbesserung eigener Services nutzen sowie zur Vorbereitung auf eine Auditierung ihrer Services. Dazu bietet der Kriterienkatalog in diesem Buch eine konkrete Anwendungsrichtlinie, in der beschrieben wird, welche Anforderungen von Cloud-Services erfüllt werden müssen und welche technischen, organisatorischen und rechtlichen Rahmenbedingungen zu beachten sind. Cloud-Service-Zertifizierungsanbietern dienen der Kriterienkatalog und die Gestaltungsempfehlungen zum Assessment und zur Verbesserung des eigenen Kriterienkatalogs und Zertifizierungsrahmenwerks.

Ferner adressiert dieses Buch die Problematik, dass eine langjährige Gültigkeit von Zertifizierungen im Cloud-Computing-Umfeld aufgrund von inhärenter Dynamik und der ständigen (technischen) Weiterentwicklung von Cloud-Services kritisch zu betrachten ist. Insbesondere kann die Einhaltung bestimmter Anforderungen und Kriterien über die Gültigkeitsdauer der Zertifizierungen von ein bis drei Jahren gefährdet sein, bspw. durch das Auftreten von schwerwiegenden Sicherheitsvorfällen oder Änderungen an der Konfiguration des Cloud-Services. Um die Glaubwürdigkeit ausgestellter Zertifikate zu erhöhen und um kontinuierlich sicherzustellen, dass Cloud-Services sicher und zuverlässig angeboten werden, stellt dieses Buch daher Grundlagen für kontinuierliche Zertifizierungen von Cloud-Services dar, welches es ermöglichen kritische Anforderungen an Cloud-Services kontinuierlich und (teil-)automatisiert zu überprüfen. Dabei zeigt es den Bedarf und den Mehrwert von kontinuierlichen Zertifizierungen für Cloud-Service-Kunden auf. Ferner werden Vorteile für Cloud-Service-Anbieter aufgezeigt, Maßnahmen zur Teilnahme an einer kontinuierlichen Zertifizierung vorgestellt und Lösungsansätze zur Bewältigung möglicher Herausforderungen bei einer Teilnahme diskutiert. Außerdem unterstützt das Buch durch die umfassende Einführung und Diskussion von kontinuierlichen Zertifizierungsverfahren die Anbieter von Cloud-Service-Zertifizierungen, indem aufgezeigt wird, wie sie zukünftig ihre Prozesse zur Überprüfung automatisieren können, um eine neue Generation von transparenten und fortlaufend gültigen Zertifizierungen anbieten zu können. Die Forschungsergebnisse dieses Buches adressieren somit die Marktteilnehmer im Cloud-Service-Zertifizierungsumfeld ganzheitlich und tragen dadurch zur Steigerung der Transparenz am Cloud-Markt bei.

Dieses Buch ist wie folgt aufgebaut. Im Kap. 2 werden zunächst die Grundlagen zum Cloud-Computing und zur Zertifizierung von Cloud Services erläutert. In Kap. 3 werden Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen beschrieben. Kap. 4 beschreibt den detaillierten Kriterienkatalog zur Zertifizierung

von Cloud-Services. Kap. 5 führt in die Durchführung von kontinuierlichen Zertifizierungsverfahren ein und Kap. 6 beschreibt Rahmenbedingungen und Anforderungen an diese Verfahren. Kap. 7 beschreibt Metriken und Messverfahren zur automatisierten Beurteilung von Zertifizierungskriterien, während Kap. 8 das monitoring-basierte Zertifizierungsverfahren im Detail betrachtet. Kap. 9 schließt mit einem Ausblick auf das Marktpotenzial von kontinuierlichen Zertifizierungen. Kap. 10 schließt dieses Buch mit einem Fazit und einem Ausblick ab. Die Vorgehensweise zur Herleitung des Kriterienkatalogs ist im Anhang beschrieben.

Literatur

Benlian A, Kettinger WJ, Sunyaev A, Winkler TJ (2018) The transformative value of cloud computing: a decoupling, platformization, and recombination theoretical framework. J Manag Inf Syst 35(3):719–739. https://doi.org/10.1080/07421222.2018.1481634

Fernandes DB, Soares LB, Gomes J, Freire M, Inácio PM (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170. https://doi.org/10.1007/s10207-013-0208-7

Lins S, Grochol P, Schneider S, Sunyaev A (2016) Dynamic certification of cloud services: trust, but verify! IEEE Secur Priv 14(2):67–71. https://doi.org/10.1109/MSP.2016.26

Mell P, Grance T (2011) SP 800-145. The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Schneider S, Sunyaev A (2016) Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. J Inf Technol 31(1):1–32. https://doi.org/10.1057/jit.2014.25

Sunyaev A, Schneider S (2013) Cloud services certification. Commun ACM (CACM) 56(2):33–36. https://doi.org/10.1145/2408776.2408789

Grundlagen zur Zertifizierung von Cloud-Services

2

Zusammenfassung

In diesem Kapitel werden die Grundlagen zu Cloud-Computing und der Zertifizierung von Cloud-Services kurz erläutert. Es werden die grundlegenden Charakteristiken des Cloud-Computings, die Service- und Bereitstellungsmodelle beschrieben sowie Risiken beim Einsatz von Cloud-Services erörtert. Anschließend wird eine kurze Einführung zur Zertifizierung von Cloud-Services gegeben, in welcher der Nutzen von Zertifizierungen für Cloud-Service-Anbieter und -Kunden dargelegt wird, gefolgt von einer Marktübersicht zu existierenden Cloud-Service-Zertifizierungen.

2.1 Cloud-Computing

In der Fachliteratur existieren eine Vielzahl von Definitionen und Erklärungsansätzen von Cloud-Computing (Leimeister et al. 2010; Marston et al. 2011). Dabei hat sich die Definition des National Institute of Standards and Technology (NIST) in der Fachwelt als Grundlage etabliert. Nach dieser Definition bezeichnet Cloud-Computing ein Modell, welches einen flexiblen und bedarfsorientierten Zugriff auf eine gemeinsam genutzte Sammlung von konfigurierbaren IT-Ressourcen ermöglicht, die über das Internet oder einem Netzwerk abgerufen werden (Mell und Grance 2011). Darunter fällt beispielsweise der Zugriff auf Netzwerke, Server, Speicher oder Anwendungen. Cloud-Services werden mit minimalem Managementaufwand und geringer Interaktion mit dem Cloud-Service-Anbieter schnell

S. Lins et al., *Cloud-Service-Zertifizierung*,
https://doi.org/10.1007/978-3-662-58857-4_2

bereitgestellt und können möglichst automatisch an den individuellen Bedarf der Cloud-Service-Kunden angepasst werden. Ferner zeichnet sich Cloud-Computing durch fünf spezielle Charakteristiken aus und man unterscheidet drei Service- und sechs Bereitstellungsmodelle. Diese werden im Folgenden erläutert.

2.1.1 Charakteristiken

Die für Cloud-Computing kennzeichnenden Charakteristiken sind der bedarfsgerechte Zugriff, eine Netzwerkanbindung, die Möglichkeit zur Ressourcenbündelung, eine hohe Skalierbarkeit und eine verbrauchsabhängige Bezahlung (Mell und Grance 2011).

Bedarfsgerechter Zugriff (On-demand Self-service)
Der bedarfsgerechte Zugriff ermöglicht es Cloud-Service-Kunden selbstständig und nahezu unmittelbar Leistungsparameter der in Anspruch genommenen Cloud-Services anzupassen. Dies kann insbesondere automatisch und ohne menschliche Interaktion mit den jeweiligen Cloud-Service-Anbietern durchgeführt werden. So ist es beispielsweise möglich, je nach aktuellem Bedarf, erhaltene Rechen-, Speicher- oder Bandbreitenkapazitäten zu erhöhen oder zu reduzieren.

Netzwerkanbindung (Broad Network Access)
Cloud-Services werden über ein Breitbandnetzwerk bereitgestellt, in der Regel über das Internet. Cloud-Services nutzen standardisierte Kommunikationsschnittstellen und können mit einer Vielzahl von Endgeräten benutzt werden, darunter beispielsweise Smartphones, Tablets oder Laptops.

Ressourcenbündelung (Resource Pooling)
Die vom Cloud-Service-Anbieter bereitgestellten Ressourcen werden durch eine Multi-Mandanten-Architektur von mehreren Cloud-Service-Kunden gleichzeitig genutzt. Dabei werden die physischen und virtuellen Ressourcen je nach Bedarf dynamisch den verschiedenen Cloud-Service-Kunden zugeteilt. Cloud-Service-Kunden können hierbei nicht immer den exakten Standort feststellen, an dem sich die genutzten Ressourcen befinden. Jedoch ist eine grobe Eingrenzung hinsichtlich des Landes, der Region oder des Rechenzentrums in einigen Fällen möglich.

Skalierbarkeit (Rapid Elasticity)
Bereitgestellte Ressourcen können flexibel und schnell, in einigen Fällen vollautomatisch, erhöht oder freigegeben werden, um so die Ressourcen auf den aktuellen

Bedarf abzustimmen. Unter anderem deshalb entsteht für den Cloud-Service-Kunden der Eindruck, dass Ressourcen nahezu unbegrenzt scheinen und zu jeder Zeit in jedem Ausmaß verfügbar sind.

Verbrauchsabhängige Bezahlung (Measured Service)
Um Cloud-Services messbar und transparent zu gestalten, kontrollieren und optimieren Cloud-Services den Ressourcenverbrauch anhand von serviceabhängigen Kennzahlen, beispielsweise dem Speicherplatz, der Rechenleistung oder der Bandbreite. Dadurch kann eine bedarfsgerechte Abrechnung angeboten und durchgeführt werden. Zudem wird die Ressourcennutzung überwacht, kontrolliert, protokolliert und kommuniziert, sodass sowohl für den Cloud-Service-Kunden, als auch für den Cloud-Service-Anbieter, Transparenz über die Nutzung geschaffen wird.

2.1.2 Service-Modelle

Im Cloud-Computing kann ferner zwischen den drei grundlegenden Service-Modellen Software as a-Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS) unterschieden werden (Mell und Grance 2011).

Software as a Service
Der Cloud-Service-Kunde kann mittels verschiedener Geräte entweder über ein Thin-Client-Interface, beispielsweise einem Web-Browser, oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen. Der Cloud-Service-Kunde hat hierbei keine Kontrolle über die zugrunde liegende Cloud-Infrastruktur, sondern kann nur spezifische Anwendungseinstellungen vornehmen.

Platform as a Service
Der Cloud-Service-Kunde kann selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Service-Anbieters installieren und betreiben. Hierzu werden Programmiersprachen, Programmbibliotheken oder weitere vom Cloud-Service-Anbieter unterstützte Dienste und Werkzeuge genutzt. Ähnlich wie bei dem Software-as-a-Service-Modell hat der Cloud-Service-Kunde keine Kontrolle über die zugrunde liegende Cloud-Infrastruktur. Auf der anderen Seite kann er eigene installierte oder ausgeführte Anwendungen verwalten und kann gegebenenfalls eine limitierte Anzahl von Einstellungen in der entsprechenden technischen Anwendungsumgebung durchführen.

Infrastructure as a Service
Der Cloud-Service-Kunde erhält Zugang zu Hardwareressourcen des Cloud-Service-Anbieters, darunter fallen beispielsweise Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger Software verwenden, beispielsweise Betriebssysteme oder Anwendungen. Ihm obliegt die Kontrolle über Betriebssysteme, Speicher und installierten Anwendungen, gegebenenfalls auch über ausgewählte Netzwerkressourcen, beispielsweise über Firewalls, jedoch nicht über die zugrunde liegende Cloud-Infrastruktur.

Darüber hinaus finden sich in der Praxis und Literatur eine Vielzahl von weiteren Service-Modellen, beispielsweise Database as a Service oder Security as a Service. Tab. 2.1 listet beispielhaft weitere Service-Modelle auf und ordnet sie den grundlegenden Modellen Infrastructure, Platform und Software as a Service zu. Im Folgenden wird nur zwischen diesen drei Modellen unterschieden.

Diese Service-Modelle repräsentieren gemeinsam den technischen Grundansatz von Cloud-Computing, in dem Software, Plattform und Infrastruktur als aufeinander aufbauende Schichten verstanden werden (sogenannter ‚Cloud-Stack'). Hierbei ermöglicht und unterstützt die Infrastruktur eine Plattform, während eine Plattform zur Ausführung von Software genutzt wird. Basierend auf dem Cloud-Stack können die Einflussmöglichkeiten des Cloud-Service-Kunden und des -Anbieters für die grundlegenden Cloud-Service-Modelle detailliert beschrieben werden. Tab. 2.2 stellt die Einflussmöglichkeiten schematisch dar.

In Tab. 2.2 wird deutlich, dass bei der Nutzung eines SaaS-Dienstes, der Cloud-Service-Kunde keine technischen Änderungsmöglichkeiten beim Cloud-Service hat. Es ist lediglich möglich, dass ein Cloud-Service-Kunde gewisse Konfigurationen oder Einstellungen bei bezogenen Cloud-Anwendungen durchführen kann, wie beispielsweise das Ein- und Ausschalten gewisser Funktionalitäten oder das Anpassen von grafischen Benutzeroberflächen. Zudem sei anzumerken, dass der Cloud-Service-Nutzer Sorge zu tragen hat, dass die Cloud-Anwendung sicher und

Tab. 2.1 Weitere Cloud-Service-Modelle und deren Zuordnung zu den grundlegenden Service-Modellen Software, Platform und Infrastructure as a Service

	Grundlegende Service-Modelle			
Service-Modell	SaaS	PaaS	IaaS	Beispielhafte Literatur
Security as a Service	•	–	–	Sharma et al. (2016)
Search as a Service	•	–	–	Dašić et al. (2016)
Testing as a Service	–	•	–	Linthicum (2009)
Database as a Service	–	•	–	Linthicum (2009)
Network as a Service	–	–	•	Soares et al. (2011)
Rendering as a Service	–	–	•	Annette et al. (2015)

Tab. 2.2 Einflussmöglichkeiten nach dem Schichtenmodell, adaptiert von Singh et al. (2016); European Network and Security Agency (2012)

Akteur	IaaS	PaaS	SaaS	Beschreibung der Schicht
Cloud-Service-Kunde	Sichere Anwendungsnutzung			Der Cloud-Service-Kunde ist für eine sichere Nutzung der Anwendung verantwortlich.
	Nutzerspezifika			Kundenindividuelle Einstellungen oder Konfigurationen von genutzten Anwendungen.
	Anwendung		Anwendung	Angebotene Softwarelösungen.
	Softwaresicherheit		Softwaresicherheit	Mechanismen zur Erhöhung der Sicherheit von angebotenen Anwendungen.
	Administration und Support der Software		Administration und Support der Software	Administration der angebotenen Software sowie Behandlung von Support-Anfragen durch den Cloud-Service-Kunden.
	Betriebssystem	Betriebssystem	Betriebssystem	Grundlegende Software zum Betrieb von Anwendungen.
	Laufzeitumgebung	Laufzeitumgebung	Laufzeitumgebung	Die Laufzeitumgebung führt Applikationen aus, für welche die Laufzeitumgebung geeignet ist.
	Datenbank	Datenbank	Datenbank	Software zur Verwaltung und Strukturierung von Daten.
	Plattformsicherheit	Plattformsicherheit	Plattformsicherheit	Mechanismen zur Erhöhung der Sicherheit von angebotenen Plattformen.
	Administration und Support der Plattform	Administration und Support der Plattform	Administration und Support der Plattform	Administration der angebotenen Plattform sowie Behandlung von Support-Anfragen durch den Cloud-Service-Kunden.
	Virtuelle Maschinen	Virtuelle Maschinen		Virtuelle Repräsentation von Rechnerressourcen wie bspw. Server oder CPUs.
Cloud-Service-Anbieter	Virtualisierungsschicht	Virtualisierungsschicht		Mechanismen zur Erstellung und Verwaltung von Virtuellen Maschinen.
	Berechnungs-komponenten	Berechnungskomponenten		Komponenten zur Durchführung von Berechnungen oder Verarbeitung von Daten im Cloud-Service.
	Speicher	Speicher		Mechanismen zur Speicherung von Daten.
	Netzwerk	Netzwerk		Mechanismen zum Transport von Daten.
	Infrastruktur-sicherheit	Infrastruktursicherheit		Mechanismen zur Erhöhung der Sicherheit von angebotenen Ressourcen.
	Administration und Support für die Infrastruktur	Administration und Support für die Infrastruktur		Administration der angebotenen Infrastruktur sowie Behandlung von Support-Anfragen durch den Cloud-Service-Kunden.
	Hardware			Die physische Hardware zur Erbringung des Cloud-Services.
	Gebäude, Einrichtung und Equipment			Die physische Einrichtung des Cloud-Service.
	Konnektivität- und Netzanbindung			Die physische Konnektivität des Rechenzentrums.
	Rechenzentrumsicherheit			Mechanismen zur Erhöhung der Sicherheit des Rechenzentrums, darunter Gebäudeverantwortliche mit Wachpersonal und physische Sicherungssysteme.

Legende:

Cloud-Service-Kunde
SaaS-Kerngeschäft
PaaS-Kerngeschäft
IaaS-Kerngeschäft
Full-Stack-Anbieter oder Sub-Provider

konform genutzt wird. Zum Kerngeschäft des SaaS-Anbieters gehören die Entwicklung, der Betrieb und die Administration der Softwareanwendung sowie die Sicherstellung der Softwaresicherheit.

Im Falle eines PaaS-Dienstes betreibt ein Cloud-Service-Kunde eigene Anwendungen auf einer angebotenen Cloud-Plattform. Somit ist der Cloud-Service-Kunde

für die Erstellung und den Betrieb der Anwendungen verantwortlich. Zudem muss der Cloud-Service-Kunde die Sicherheit der Anwendung verantworten, um beispielsweise Cross-Site-Scripting oder Softwareschwachstellen zu verhindern. Zum Kerngeschäft des PaaS-Anbieters gehören die Entwicklung, der Betrieb und die Administration der Plattform (beispielsweise der angebotenen Betriebssysteme oder Datenbanken) sowie die Sicherstellung der Plattformsicherheit.

Beim Angebot eines IaaS-Dienstes ist der Cloud-Service-Anbieter für die korrekte und sichere Virtualisierung und die Bereitstellung der notwendigen physischen Ressourcen zuständig. Ein Cloud-Service-Kunde trägt die Verantwortung über angemietete Virtuelle Maschinen und darauf ausgeführten Anwendungen, Datenbanken, Betriebssystemen und Laufzeitumgebungen. Zudem übernimmt der Cloud-Service-Kunde die Verantwortung über Software- und Plattformsicherheit. Die notwendige physische Hardware, Einrichtungen und Equipment können durch einen IaaS-Anbieter bereitgestellt werden oder bei einem Rechenzentrum eines Sub-Anbieters bezogen werden.

Als weiterführende Literatur sei auf die NIST ‚*Cloud Security Reference Architecture*' verwiesen, welche im Anhang D eine detaillierte Betrachtung der Einflussmöglichkeiten für die verschiedenen Service-Modelle auflistet (NIST Cloud Computing Security Working Group 2013).

2.1.3 Bereitstellungsmodelle

Zusätzlich zu den oben definierten Service-Modellen wird zwischen den vier grundlegenden Bereitstellungsmodellen (engl.: „Deployment Models") Private-, Community-, Public- und Hybrid-Cloud unterschieden (Mell und Grance 2011). Darüber hinaus werden die Bereitstellungsmodelle Virtual-Private-Cloud und Multi-Cloud oft in der Literatur und Praxis angeführt (Dillon et al. 2010; Amazon Web Services 2015; Grozev und Buyya 2014).

Private-Cloud
Die Cloud-Infrastruktur wird nur durch eine einzelne Organisation und deren Mitglieder genutzt. Sie kann sowohl von der Organisation, Dritter oder einer Kombination dieser besessen, verwaltet und betrieben werden. Ferner muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation befinden.

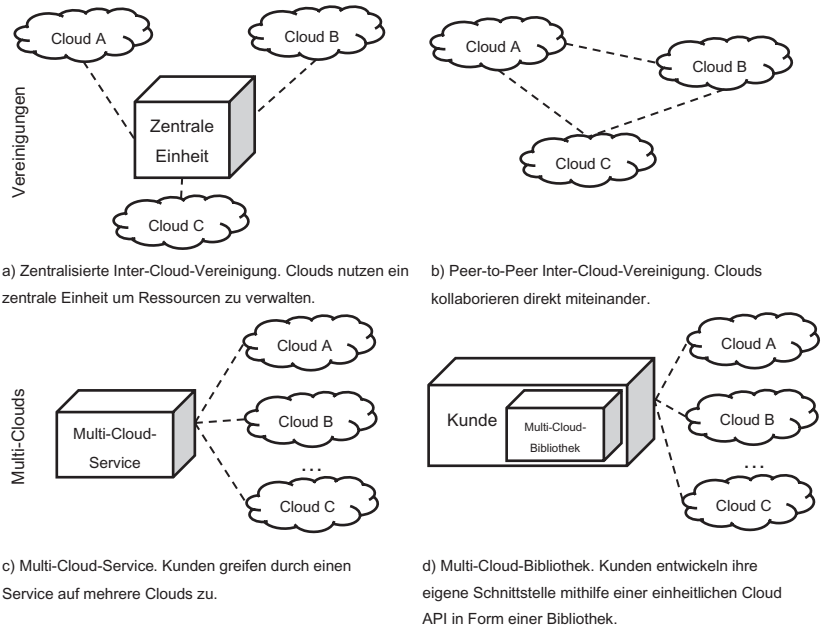
Public-Cloud
Die Cloud-Infrastruktur kann durch die allgemeine Öffentlichkeit genutzt werden. Unternehmen, akademische oder staatliche Organisationen, oder eine Kombination dieser besitzen, verwalten und betreiben die Cloud-Infrastruktur.

Community-Cloud
Die Cloud-Infrastruktur wird ausschließlich durch eine Gruppe von Organisationen genutzt, welche ähnliche Anforderungen an den Cloud-Service stellen. Eine oder mehrere Organisationen der Community, Dritte oder eine Kombination dieser Parteien besitzen, verwalten und betreiben die Cloud-Infrastruktur. Auch hierbei muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation bzw. den Organisationen befinden.

Hybrid-Cloud
Die Cloud-Infrastruktur besteht aus einer Kombination von zwei oder mehreren der oben beschriebenen Modelle. Die einzelnen Infrastrukturen bleiben als Einheit erhalten, werden jedoch durch standardisierte oder proprietäre Technologien verbunden. Dies ermöglicht die Übertragbarkeit von Daten und Anwendungen zwischen den angebundenen Infrastrukturen.

Virtual-Private-Cloud
Erstmals wurde der Begriff „Virtual-Private-Cloud“ von Amazon Web Services (AWS) eingeführt, als deren neues Produkt „Amazon VPC“ vorgestellt wurde (Amazon Web Services 2015). Beim Virtual-Private-Cloud-Modell wird die Infrastruktur de facto für eine einzelne Organisation bereitgestellt, die mehrere Nutzer (zum Beispiel Geschäftsbereiche) umfassen kann (Dillon et al. 2010). Der Zugriff auf die Cloud wird unter der Verwendung eines Virtual Private Networks (VPN) realisiert. Die Cloud-Infrastruktur ist das Eigentum eines Cloud-Service-Anbieters. Sie wird durch den Cloud-Service-Anbieter betrieben und verwaltet, wobei der Cloud-Service-Kunde die vollständige Kontrolle über die virtuelle Netzwerkumgebung behält.

Multi-Cloud
Werden Cloud-Services verschiedener Cloud-Service-Anbieter aggregiert und zusammengefasst, kann dies als Multi-Cloud verstanden werden (Grozev und Buyya 2014). Hierbei können sowohl Cloud-Service-Anbieter ihre Cloud-Infrastrukturen und Services mit anderen Cloud-Service-Anbietern freiwillig vernetzen, oder ein Cloud-Service-Broker tritt auf dem Markt auf, welcher verschiedene Cloud-Services von (unterschiedlichen) Cloud-Service-Anbietern aggregiert und einen separaten Zugriff zu ihnen ermöglicht. Abb. 2.1 stellt beispielhafte Multi-Cloud-Szenarien dar. Die Unterscheidung zwischen einer Multi-Cloud und einer Hybrid-Cloud stellt sich als schwierig und uneinheitlich dar. Im Gegensatz zu einer Hybrid-Cloud, bei der üblicherweise die Cloud-Infrastrukturen verbunden sind und gemeinsam arbeiten (Orchestrierung), werden bei Multi-Clouds gezielt nur bestimmte Cloud-Komponenten eines Cloud-Services von einem weiteren Cloud-Services-Anbieter



a) Zentralisierte Inter-Cloud-Vereinigung. Clouds nutzen ein zentrale Einheit um Ressourcen zu verwalten.

b) Peer-to-Peer Inter-Cloud-Vereinigung. Clouds kollaborieren direkt miteinander.

c) Multi-Cloud-Service. Kunden greifen durch einen Service auf mehrere Clouds zu.

d) Multi-Cloud-Bibliothek. Kunden entwickeln ihre eigene Schnittstelle mithilfe einer einheitlichen Cloud API in Form einer Bibliothek.

Abb. 2.1 Beispielhafte Formen einer Multi-Cloud (Grozev und Buyya 2014)

genutzt. So kann ein Cloud-Service-Anbieter einer Multi-Cloud beispielsweise die Berechnungs- und Netzwerkoperationen in einer AWS-Cloud durchführen, während die Speicherung allein durch eine Microsoft Azure-Cloud durchgeführt wird.

2.1.4 Risiken beim Einsatz von Cloud-Services

Unternehmen die ihre Prozesse und Daten in die Cloud auslagern möchten oder planen Cloud-Services zu integrieren, müssen ein umfassendes Verständnis über mögliche Risiken von Cloud-Services entwickeln, um so potenzielle Gefahren besser beurteilen und gegebenenfalls auf ihren Eintritt angemessen reagieren zu können. Auch Cloud-Service-Anbieter müssen ein weitreichendes Verständnis von Risiken besitzen, um Vorkehrungen zur Vermeidung oder Kompensation eventueller Risiken zu treffen. Wenn sie beispielsweise nachweisen können, dass sie es durch spezielle Sicherheitsmaßnahmen schaffen eine Auswahl von Risiken zu minimieren, kann dies als Alleinstellungsmerkmal oder Wettbewerbsvorteil angesehen werden (Subashini und Kavitha 2011).

Bei der Betrachtung der Risiken von Cloud-Computing ergeben sich für jedes Service- und Bereitstellungsmodell individuelle Risiken (European Network and Security Agency 2012; Subashini und Kavitha 2011). Zudem erfordern die einzigartigen Eigenschaften von Cloud-Computing, wie beispielsweise die Vielzahl an Speicherlokationen und die Multi-Mandanten-Architektur, gesonderte Risikobewertungen und angepasste Bewältigungsstrategien (Fernandes et al. 2014). So zeigt sich unter anderem, dass aufgrund der Speicherung großer Datenmengen von vielen verschiedenen Cloud-Service-Kunden, die Cloud als ein hochwertiges Ziel für Angriffe angesehen wird (Subashini und Kavitha 2011). Darüber hinaus sind beim Cloud-Computing viele Risiken inhärent, die auch bei der traditionellen Beschaffung externer IT-Dienstleistungen sowie bei der Verwendung von Webtechnologien zum Tragen kommen. Im Folgenden werden verschiedene Risiken gegliedert in Kategorien aufgeführt, die bei der Adoption von Cloud-Services berücksichtigt werden sollten. Für eine umfassende Klassifizierung von Risiken im Cloud-Computing sei beispielsweise auf Fernandes et al. (2014) verwiesen.

Organisatorische Risiken

Bei der Nutzung von Cloud-Services besteht das Risiko des Kontrollverlusts, da die Überwachung der genutzten Cloud-Services, insbesondere hinsichtlich verschiedener Sicherheitsaspekte, überwiegend dem Cloud-Service-Anbieter obliegt und daher vom Cloud-Service-Kunde nur eingeschränkt verfolgt und beeinflusst werden kann (Marston et al. 2011; Armbrust et al. 2010). Auch hat der Cloud-Service-Kunde eine unzureichende Kontrolle über die Datenlokation, zukünftigen Updates und Wartungsarbeiten. Ebenfalls kann eine eigenständige Kontrolle der eigenen Prozesse oder gespeicherten Daten nur eingeschränkt möglich sein (European Network and Security Agency 2012).

In der Beziehung zwischen Cloud-Service-Anbieter und -Kunde könnten Unklarheiten über die Verteilung der Verantwortlichkeiten vorliegen, da Maßnahmen zur Erhöhung der Sicherheit sowohl vom Cloud-Service-Anbieter übernommen aber auch dem Cloud-Service-Kunden übertragen werden können (Heiser und Nicolett 2008). Sind die Verantwortlichkeiten nicht transparent verteilt, kann es zu Sicherheitslücken kommen.

Eine sorgfältige Auswahl der Mitarbeiter und eine fortlaufende Schulung von Mitarbeitern des Cloud-Services sind erforderlich um sicherzustellen, dass das notwendige Knowhow zum Betrieb und zur Administration des Cloud-Services vorhanden ist sowie alle gesetzlichen Regelungen eingehalten werden (Fernandes et al. 2014). Fahrlässiges Fehlverhalten, beispielsweise bei dem Umgang mit personenbezogenen Daten im Rahmen von Kundensupportanfragen, kann zu einer Verletzung der Service-Level-Agreements oder geltender Datenschutzgesetzte