

DIN ISO/IEC 19086-1

ICS 35.210

Einsprüche bis 2017-05-24

Entwurf

**Informationstechnik –
Cloud Computing –
Dienstgütevereinbarung (SLA) Rahmenwerk –
Teil 1: Übersicht und Konzepte (ISO/IEC 19086:2016);
Text Deutsch und Englisch**

Information technology –
Cloud computing –
Service level agreement (SLA) framework –
Part 1: Overview and concepts (ISO/IEC 19086:2016);
Text in German and English

Technologies de l'information –
Informatique en nuage –
Cadre de travail de l'accord du niveau de service –
Partie 1: Aperçu général et concepts (ISO/IEC 19086:2016);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-03-24 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 86 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Literaturhinweise	4
Einleitung	5
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen.....	12
5 Übersicht über SLA für Cloud-Dienste	12
6 Beziehung zwischen der Cloud-Dienstleistungsvereinbarung und Cloud-Dienstgütevereinbarung (Cloud-SLA).....	14
7 Bewährte Methoden des Cloud-SLA-Managements	15
7.1 Allgemeines	15
7.2 Entwurf.....	15
7.3 Beurteilung und Annahme	16
7.4 Einführung und Umsetzung.....	16
7.5 Änderungen an der Cloud-SLA.....	16
8 Die Funktion von Cloud-Dienstgütezielen, Qualitätszielen des Cloud-Dienstes, Metriken, Rechtsmitteln und Ausnahmen in der Cloud-SLA.....	17
8.1 Allgemeines	17
8.2 Metriken.....	17
8.3 SLO und SQO	17
8.3.1 Dienstgüten.....	17
8.3.2 Cloud-Dienstgüteziele.....	18
8.3.3 Qualitätsziele des Cloud-Dienstes	18
8.4 Rechtsmittel und Forderungen	18
8.4.1 Rechtsmittel.....	18
8.4.2 Forderungsprozess	18
8.5 Ausnahmen	19
9 Komponenten der Cloud-SLA	19
9.1 Allgemeines	19
9.2 Komponente der betroffenen Dienste	19
9.2.1 Beschreibung.....	19
9.2.2 Relevanz.....	19
9.3 Komponente der Cloud-SLA-Definitionen	20
9.3.1 Beschreibung.....	20
9.3.2 Relevanz.....	20
9.4 Komponente der Dienstüberwachung.....	20
9.4.1 Beschreibung.....	20
9.4.2 Relevanz.....	20
9.4.3 Qualitätsziele des Cloud-Dienstes	20
9.5 Komponente der Rollen und Zuständigkeiten.....	20
9.5.1 Beschreibung.....	20
9.5.2 Relevanz.....	20

10	Inhaltsbereiche der Cloud-SLA und ihre Komponenten	21
10.1	Allgemeines	21
10.2	Inhaltsbereich der Zugänglichkeit.....	21
10.2.1	Komponente der Zugänglichkeit	21
10.3	Inhaltsbereich der Verfügbarkeit.....	22
10.3.1	Komponente der Verfügbarkeit.....	22
10.4	Inhaltsbereich der Leistungsfähigkeit des Cloud-Dienstes	22
10.4.1	Allgemeines	22
10.4.2	Komponente der Antwortzeit des Cloud-Dienstes.....	22
10.4.3	Komponente der Kapazität des Cloud-Dienstes.....	23
10.4.4	Komponente der Elastizität.....	24
10.5	Inhaltsbereich des Schutzes personenbezogener Informationen (PII).....	25
10.5.1	Komponente des Schutzes von PII	25
10.6	Inhaltsbereich der Informationssicherheit.....	26
10.6.1	Komponente der Informationssicherheit	26
10.7	Inhaltsbereich der Kündigung des Dienstes.....	27
10.7.1	Komponente der Kündigung des Dienstes.....	27
10.8	Inhaltsbereich des Cloud-Supports.....	29
10.8.1	Komponente des Cloud-Supports.....	29
10.9	Inhaltsbereich der Governance	31
10.9.1	Komponente der Governance	31
10.10	Inhaltsbereich der Änderungen an den Eigenschaften und Funktionen des Cloud-Dienstes.....	33
10.10.1	Komponente der Änderungen an den Eigenschaften und Funktionen des Cloud-Dienstes	33
10.11	Inhaltsbereich der Dienstverlässlichkeit.....	33
10.11.1	Allgemeines	33
10.11.2	Komponente der Resilienz/Fehlertoleranz des Dienstes	33
10.11.3	Komponente der Sicherung und Wiederherstellung von Kundendaten.....	34
10.11.4	Komponente der Notfallwiederherstellung	36
10.12	Inhaltsbereich des Datenmanagements.....	37
10.12.1	Allgemeines	37
10.12.2	Komponente der Schutz- und Urheberrechte (IPR)	38
10.12.3	Komponente der Cloud-Kundendaten.....	38
10.12.4	Komponente der Cloud-Dienstleisterdaten.....	39
10.12.5	Komponente der Kontodaten	39
10.12.6	Komponente der abgeleiteten Daten	39
10.12.7	Komponente der Datenübertragbarkeit.....	40
10.12.8	Komponente der Datenlöschung	41
10.12.9	Komponente des Datenstandorts.....	41
10.12.10	Komponente der Datenprüfung	42
10.12.11	Komponente des Zugriffs durch Strafverfolgungsbehörden	42
10.13	Inhaltsbereich der Bescheinigungen, Zertifikate und Audits	43
10.13.1	Komponente der Bescheinigungen, Zertifikate und Audits.....	43
	Literaturhinweise.....	44

Nationales Vorwort

Diese Deutsche Norm ist die Übersetzung der Internationalen Norm ISO/IEC 19086-1:2016, die im Technischen Komitee ISO/IEC JTC 1, „Information technology“, Unterkomitee 38 „Cloud computing and distributed platforms“, in Zusammenarbeit mit ITU-T erarbeitet wurde.

Eine Liste aller Teile von ISO/IEC 19086 ist auf der ISO-Internetseite zu finden.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-01-38 AA „Verteilte Anwendungsplattformen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des ISO/IEC 19086-1 entsprechend der diesbezüglich durch ISO erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen ISO-Text.

Die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 17788:2014	siehe DIN ISO/IEC 17788:2016-04
ISO 9241-171:2008	siehe DIN EN ISO 9241-171:2008-10
ISO/IEC 27001	siehe DIN ISO/IEC 27001
ISO/IEC 27002	siehe DIN ISO/IEC 27002
ISO/IEC 27040	siehe DIN EN ISO/IEC 27040

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9241-171:2008-10, *Ergonomie der Mensch-System-Interaktion — Teil 171: Leitlinien für die Zugänglichkeit von Software (ISO 9241-171:2008); Deutsche Fassung EN ISO 9241-171:2008*

DIN ISO/IEC 17788:2016-04, *Informationstechnik — Cloud Computing — Übersicht und Vokabular (ISO/IEC 17788:2014)*

DIN ISO/IEC 27001, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Management-systeme — Anforderungen*

DIN ISO/IEC 27002, *Informationstechnologie — IT-Sicherheitsverfahren — Leitfaden für Informationssicherheits-Maßnahmen*

DIN ISO/IEC 27040, *Informationstechnologie — IT-Sicherheitsverfahren — Speichersicherheit*

Informationstechnik — Cloud Computing — Dienstgütevereinbarung (SLA) Rahmenwerk — Teil 1: Übersicht und Konzepte

Einleitung

Dieses Dokument liefert eine Übersicht, grundlegende Konzepte sowie Definitionen für das SLA-Rahmenwerk. ISO/IEC 19086 baut auf den in ISO/IEC 17788 und ISO/IEC 17789 definierten Konzepten des Cloud Computing auf. Dieses Dokument legt ein gemeinsames Rahmenwerk fest, das Organisationen hilft, den Zweck sämtlicher Teile von ISO/IEC 19086 sowie die Beziehungen zwischen diesen Teilen nachzuvollziehen. Zudem identifiziert es andere Dokumente, die in Beziehungen mit ISO/IEC 19086 stehen und für das Verständnis von Cloud-SLA nützlich sind.

Dieses Dokument kann von jeglicher Organisation oder Einzelperson genutzt werden, die an der Erstellung oder der Änderung einer Cloud-Dienstgütevereinbarung nach ISO/IEC 19086 beteiligt ist oder sich mit deren Inhalt befasst. Die Cloud-SLA sollte die Hauptmerkmale eines Dienstes des Cloud Computing berücksichtigen und soll ein gemeinsames Verständnis zwischen Cloud-Dienstleistern und Cloud-Dienstleistungskunden vereinfachen.

Insbesondere definiert es die folgenden Grundlagen und Konzepte des Cloud-SLA-Rahmenwerks:

- Cloud-Dienstleistungsvereinbarung (en: Cloud Service Agreement, CSA)
- Cloud-Dienstgütevereinbarung (en: Cloud Service Level Agreement, Cloud-SLA)
- Cloud-Dienstgüteziele (en: Cloud Service Level Objectives, SLO)
- Qualitätsziele des Cloud-Dienstes (en: Cloud Service Qualitative Objectives, SQO)

Dieses Dokument beschreibt darüber hinaus die Inhaltsbereiche und Komponenten, die aus einer Liste von SLO und SQO bestehen.

- ISO/IEC 19086-2 gibt das Metrikmodell vor, das für die Erstellung von in SLO und SQO verwendeten Metriken anzuwenden ist.
- ISO/IEC 19086-3 gibt die wichtigsten Konformitätsanforderungen vor, die von den in diesem Dokument definierten SLO und SQO abgeleitet sind.

- ISO/IEC 19086-4 baut auf den in diesem Dokument beschriebenen grundlegenden Konzepten und Definitionen auf, indem sie spezifische Komponenten sowie die Konformitätsanforderungen für SLO und SQO im Bereich Sicherheit und Datenschutz beschreibt.

Im engeren Sinne dient dieses Dokument dazu,

- a) die Kohäsion zwischen den einzelnen Teilen von ISO/IEC 19086 zu fördern, indem es die in sämtlichen Teilen verwendeten Begriffe erklärt,
- b) zum Verständnis von ISO/IEC 19086 beizutragen, indem es die Beziehungen zwischen sämtlichen Teilen verdeutlicht, und
- c) eine Übersicht über andere Internationale Normen zu geben, die in Verbindung mit ISO/IEC 19086 verwendet werden kann.

Bild 1 gibt eine Übersicht über den Inhalt von ISO/IEC 19086 sowie über die Beziehungen zwischen den einzelnen Teilen von ISO/IEC 19086 und anderen Internationalen Normen mit Bezug zu Cloud Computing.

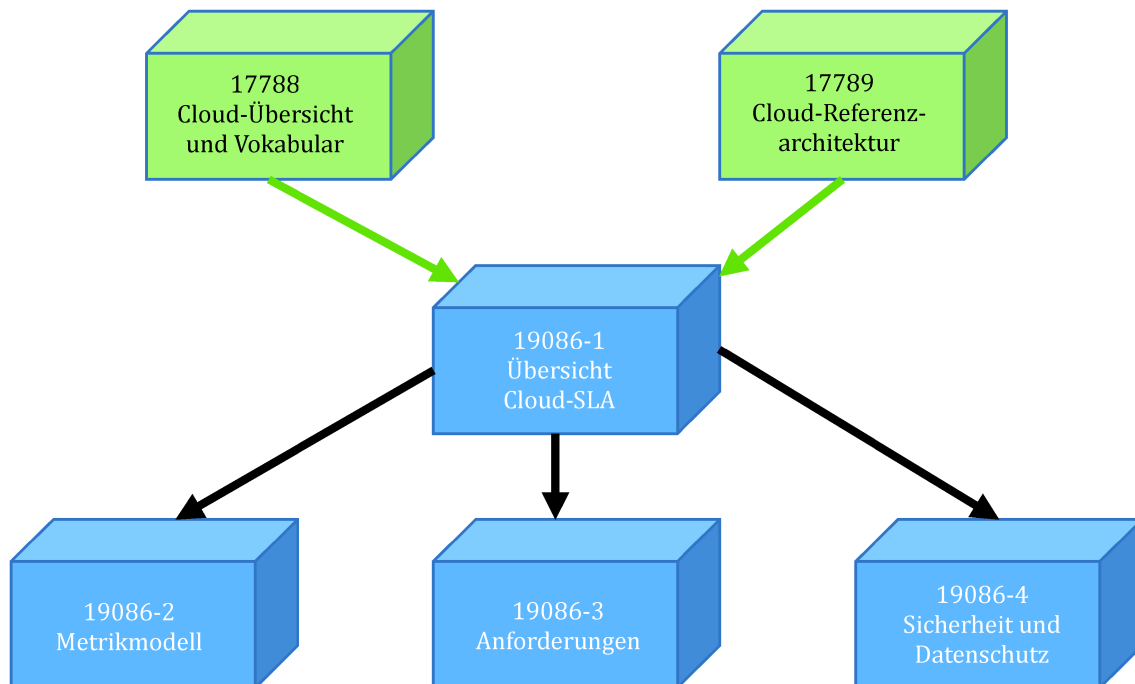


Bild 1 — Beziehung zwischen Teilen der ISO/IEC 19086 und anderen Normen zum Cloud Computing

Dieses Dokument behandelt die Inhalte einer Cloud-SLA in zwei Hauptgruppierungen: SLA-Komponenten, die in Abschnitt 9 behandelt werden, und SLA-Inhaltsbereiche, die in Abschnitt 10 behandelt werden, wie in Bild 2 dargestellt.

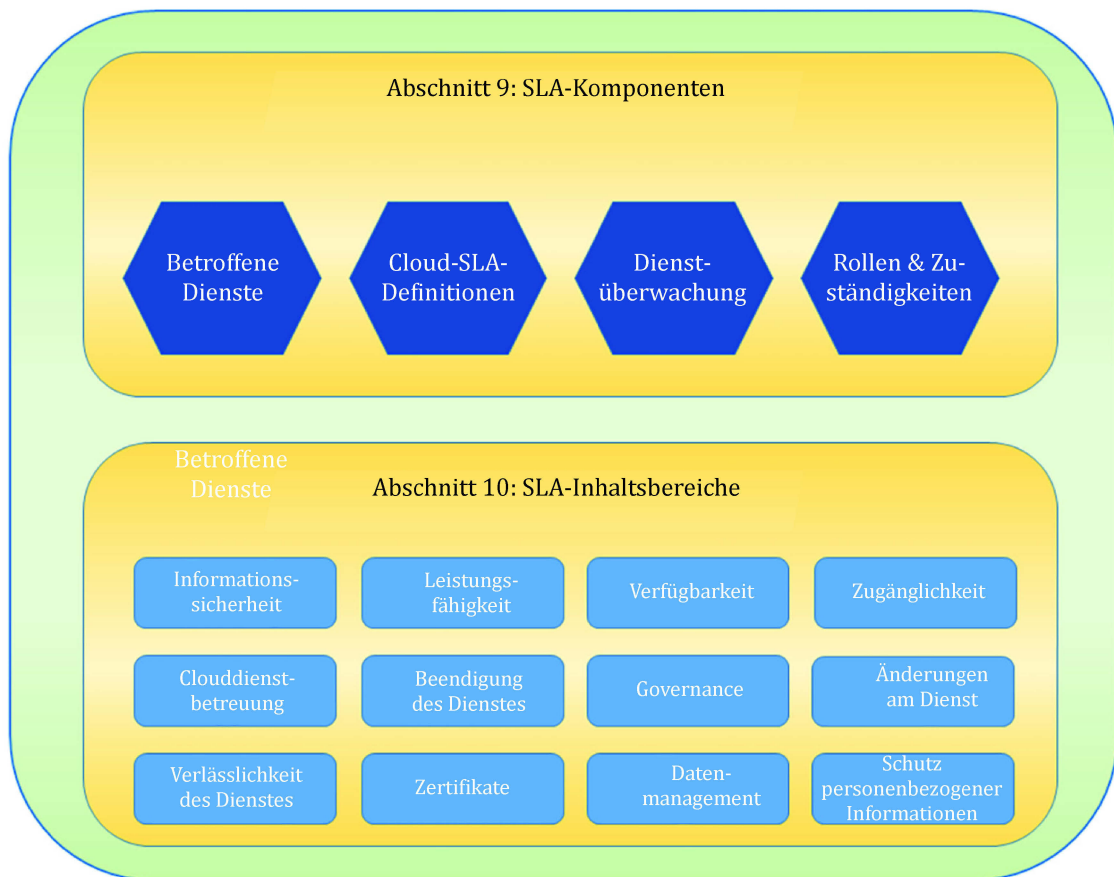


Bild 2 — SLA-Komponenten und SLA-Inhaltsbereiche

1 Anwendungsbereich

Dieses Dokument legt verschiedene gemeinsame Cloud-SLA-Bausteine (Konzepte, Begriffe, Definitionen, Kontexte) fest, die zur Erstellung von Cloud-Dienstgütevereinbarungen (Cloud-SLA) verwendet werden können.

Dieses Dokument beinhaltet Folgendes:

- a) eine Übersicht über Cloud-SLA,
- b) eine Darstellung der Beziehung zwischen der Cloud-Dienstleistungsvereinbarung und der Cloud-SLA,
- c) Konzepte, die zur Erstellung von Cloud-SLA verwendet werden können, und
- d) üblicherweise in Cloud-SLA verwendete Begriffe.

Dieses Dokument dient dem Nutzen von und der Nutzung durch Cloud-Dienstleister(n) und Cloud-Dienstleistungskunden. Ziel ist es, Verwechslungen bzw. Missverständnisse zu vermeiden sowie ein gemeinsames Verständnis zwischen Cloud-Dienstleistern und Cloud-Dienstleistungskunden zu vereinfachen. Cloud-Dienstleistungsvereinbarungen und ihre dazugehörigen Cloud-SLA variieren je nach Cloud-Dienstleister; in manchen Fällen können verschiedene Cloud-Dienstleistungskunden für den gleichen Cloud-Dienst beim gleichen Cloud-Dienstleister unterschiedliche Vertragsbedingungen vereinbaren. Ziel dieses Dokuments ist es, Cloud-Dienstleistungskunden beim Vergleich von Cloud-Diensten verschiedener Cloud-Dienstleister zu unterstützen.

Dieses Dokument liefert keine Standardstruktur, die für eine Cloud-SLA verwendet werden kann, und keine standardmäßige Liste mit Cloud-Dienstgütezielen (SLO) und Qualitätszielen des Cloud-Dienstes (SQO), die für alle Cloud-Dienste oder alle Cloud-Dienstleister gelten würde. Dieser Ansatz bietet Cloud-Dienstleistern Flexibilität bei der individuellen Anpassung ihrer Cloud-SLA an die jeweiligen Merkmale der angebotenen Cloud-Dienste.

Dieses Dokument ersetzt keinerlei gesetzliche Bestimmungen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17788 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Zugänglichkeit

Gebrauchstauglichkeit eines Produkts, einer Dienstleistung, einer Umgebung oder einer Einrichtung für eine in Bezug auf ihre Fähigkeiten möglichst weit gefasste Gruppe von Menschen

Anmerkung 1 zum Begriff: Der Begriff der Zugänglichkeit betrifft den gesamten Bereich der Fähigkeiten der Benutzer und ist nicht auf Benutzer beschränkt, die formell als behindert gelten.

Anmerkung 2 zum Begriff: Der auf Gebrauchstauglichkeit ausgerichtete Begriff der Zugänglichkeit zielt darauf ab, unter Berücksichtigung der gesamten Bandbreite der Fähigkeiten, über die die einzelnen Benutzer innerhalb der Gesamtheit verfügen, ein im Hinblick auf den betreffenden Nutzungskontext möglichst hohes Ausmaß an Effektivität, Effizienz und Zufriedenstellung zu erreichen.

Anmerkung 3 zum Begriff: Im Rahmen von ISO/IEC 19086 ist es wichtig, zwischen der besonderen Bedeutung von „Zugänglichkeit“, wie hierin definiert, und dem Begriff „zugänglich“ in seiner Wörterbuchdefinition von „erreichbar oder betretbar“ zu unterscheiden.

[QUELLE: ISO 9241-171:2008, 3.2]

3.2

Aufrechterhaltung der Betriebsfähigkeit

Fähigkeit einer Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einem Zwischenfall mit Betriebsunterbrechung auf akzeptablen, zuvor festgelegten Niveaustufen fortzusetzen

[QUELLE: ISO/IEC 22301:2012, 3.3]

3.3

Cloud-Dienstleistungsvereinbarung

dokumentierte Vereinbarung zwischen dem Cloud-Dienstleister und dem Cloud-Dienstleistungskunden über den/die betroffenen Dienst(e)

Anmerkung 1 zum Begriff: Eine Cloud-Dienstleistungsvereinbarung kann aus einem oder mehreren Teilen bestehen, der/die in einem oder mehreren Dokumenten festgehalten ist/sind.

3.4

Cloud-Dienstgütevereinbarung

Cloud-SLA

(en: cloud service level agreement)

Teil der Cloud-Dienstleistungsvereinbarung (3.3), der Cloud-Dienstgüteziele (3.5) sowie Qualitätsziele des Cloud-Dienstes (3.6) für den/die betroffenen Cloud-Dienst(e) beinhaltet

3.5

Cloud-Dienstgüteziel

SLO

(en: cloud service level objective)

Selbstverpflichtung eines Cloud-Dienstleisters im Hinblick auf ein bestimmtes quantitatives Merkmal eines Cloud-Dienstes, wobei der Wert der Intervallskala (3.9) oder Verhältnisskala (3.17) folgt

Anmerkung 1 zum Begriff: Eine SLO-Selbstverpflichtung darf als Bereich dargestellt werden.

3.6

Qualitätsziel des Cloud-Dienstes

SQO

(en: cloud service qualitative objective)

Selbstverpflichtung eines Cloud-Dienstleisters im Hinblick auf ein bestimmtes qualitatives Merkmal eines Cloud-Dienstes, wobei der Wert der *Nominalskala* (3.11) oder *Ordinalskala* (3.12) folgt

Anmerkung 1 zum Begriff: Ein Qualitätsziel des Cloud-Dienstes darf als Aufzählung dargestellt werden.

Anmerkung 2 zum Begriff: Qualitative Merkmale erfordern üblicherweise menschliche Interpretation.

Anmerkung 3 zum Begriff: Die Ordinalskala ermöglicht eine Einteilung in besteht/besteht nicht.

3.7

Notfallwiederherstellung

(en: disaster recovery)

Fähigkeit der IKT-Elemente einer Organisation, ihre kritischen Geschäftsfunktionen innerhalb eines vorgegebenen Zeitraums nach einem Notfall in akzeptablem Maße aufrechtzuerhalten

[QUELLE: ISO/IEC 27031:2011, 3.7]

3.8

Leitlinie zur Mitteilung von Ausfällen

(en: failure notification policy)

Leitlinie, in der die Prozesse spezifiziert werden, nach denen der Cloud-Dienstleistungskunde und der Cloud-Dienstleistungspartner den Cloud-Dienstleister über einen Dienstaussfall in Kenntnis setzen können und nach denen der Cloud-Dienstleister den Cloud-Dienstleistungskunden und den Cloud-Dienstleistungspartner darüber in Kenntnis setzen kann, dass ein Dienstaussfall aufgetreten ist

Anmerkung 1 zum Begriff: Die Leitlinie darf zudem den Prozess zur Bereitstellung aktueller Meldungen zu Dienstaussfällen beinhalten, Angaben dazu, wer Mitteilungen und aktuelle Meldungen erhält, die größtmögliche Zeitspanne zwischen der Feststellung eines Dienstaussfalls und der Herausgabe einer Mitteilung über den Dienstaussfall, das größtmögliche Zeitintervall zwischen aktuellen Meldungen zu Dienstaussfällen sowie Angaben dazu, wie aktuelle Meldungen zu Dienstaussfällen beschrieben werden.

3.9

Intervallskala

(en: interval scale)

kontinuierliche Skala oder diskrete Skala mit äquidistanten Skalenpunkten und einem willkürlichen Nullpunkt

[QUELLE: ISO 3534-2:2006, 1.1.8]

3.10

Metrik

(en: metric)

Messstandard, der die Bedingungen und Regeln zur Durchführung der Messung und zum Verständnis der Ergebnisse einer Messung definiert

Anmerkung 1 zum Begriff: Eine Metrik setzt ein bestimmtes abstraktes Metrikkonzept um.

Anmerkung 2 zum Begriff: Eine Metrik ist in der Praxis innerhalb eines bestimmten Kontextes anzuwenden, der die Messung bestimmter Eigenschaften zu (einer) bestimmten Zeit(en) für ein bestimmtes Ziel erfordert.

3.11

Nominalskala

(en: nominal scale)

Skala mit ungeordneten gekennzeichneten Kategorien oder mit durch Übereinkunft geordneten Kategorien

[QUELLE: ISO 3534-2:2006, 1.1.6]

3.12

Ordinalskala

(en: ordinal scale)

Skala mit geordneten, gekennzeichneten Kategorien

[QUELLE: ISO 3534-2:2006, 1.1.7]

3.13

personenbezogene Informationen

PII

(en: personally identifiable information)

Informationen, die (a) dazu verwendet werden können, die betroffene Person, auf die sie sich beziehen, zu identifizieren, oder (b) direkt oder indirekt mit einem Betroffenen verknüpft sind oder verknüpft werden können

Anmerkung 1 zum Begriff: Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise vom Akteur, der die zu schützenden Daten hält, oder von einer anderen Partei angewendet werden können, um die natürliche Person zu identifizieren.

[QUELLE: ISO/IEC 29100:2011, 2.9]

3.14

PII-Beauftragter

(en: PII controller)

Datenschutz-Akteur (oder Datenschutz-Akteure), der/die die Zwecke und Mittel für die Verarbeitung der personenbezogenen Informationen (PII) festlegt/festlegen und nicht (eine) natürliche Person(en) ist/sind, die Daten für persönliche Zwecke nutzt/nutzen

[QUELLE: ISO/IEC 29100:2011, 2.10]

3.15

betroffene Person

(en: PII principal)

natürliche Person, auf die sich die personenbezogenen Informationen (PII) beziehen

[QUELLE: ISO/IEC 29100:2011, 2.11]

3.16

PII-Verarbeiter

(en: PII processor)

Datenschutz-Akteur, der personenbezogene Informationen (PII) im Auftrag eines PII-Beauftragten sowie in Übereinstimmung mit dessen Anweisungen verarbeitet

[QUELLE: ISO/IEC 29100:2011, 2.12]

3.17

Verhältnisskala

(en: ratio scale)

kontinuierliche Skala mit äquidistanten Skalenwerten und einem absoluten oder natürlichen Nullpunkt

[QUELLE: ISO 3534-2:2006, 1.1.9]

3.18

Rechtsmittel

(en: remedy)

Entschädigung, die dem Cloud-Dienstleistungskunden zur Verfügung steht, für den Fall, dass der Cloud-Dienstleister ein vorgegebenes Cloud-Dienstgüteziel (3.5) nicht erreicht

Anmerkung 1 zum Begriff: Die originalsprachliche (englische) Definition des Begriffs („remedy“) geht von der Bedeutung „legal reparation“ aus, wie sie im Wörterbuch The Shorter Oxford English Dictionary definiert ist.

3.19

Resilienz

(en: resilience)

Fähigkeit eines Cloud-Dienstes, nach Auftreten eines Fehlers zeitnah die Betriebsbedingungen wiederherzustellen

4 Symbole und Abkürzungen

BLOB	Binary Large Object (de: großes binäres Objekt)
CSA	Cloud Service Agreement (de: Cloud-Dienstleistungsvereinbarung)
CSC	Cloud Service Customer (de: Cloud-Dienstleistungskunde)
CSP	Cloud Service Provider (de: Cloud-Dienstleister)
IKT	Informations- und Kommunikationstechnik
IPR	Intellectual Property Rights (de: Schutz- und Urheberrechte)
IT	Information Technology (de: Informationstechnik)
PII	Personally Identifiable Information (de: personenbezogene Informationen)
RPO	Recovery Point Objective (de: Wiederherstellungszeitpunkt)
RTO	Recovery Time Objective (de: Wiederherstellungsdauer)
SLA	Service Level Agreement (de: Dienstgütevereinbarung)
SLO	Cloud Service Level Objective (de: Cloud-Dienstgüteziel)
SQO	Cloud Service Qualitative Objective (de: Qualitätsziel des Cloud-Dienstes)
VM	Virtual Machine (de: virtuelle Maschine)

5 Übersicht über SLA für Cloud-Dienste

Eine Cloud-Dienstgütevereinbarung (Cloud-SLA) ist ein Teil der Cloud-Dienstleistungsvereinbarung, der Cloud-Dienstgüteziele sowie Qualitätsziele des Cloud-Dienstes für den/die betroffenen Cloud-Dienst(e) beinhaltet. Die Cloud-SLA sollte die Schlüsselmerkmale des Cloud Computing nach ISO/IEC 17788:2014, 6.2 berücksichtigen, die folgende Aspekte beinhalten.

- **Anforderungsbasierte Selbstbedienung** — Ein CSC kann ohne menschliche Interaktion mit dem CSP Zugang zu Cloud-Diensten erlangen. Die Cloud-Dienstleistungsvereinbarung (CSA) (siehe Abschnitt 6) und die dazugehörige Cloud-SLA können über Software-Werkzeuge und automatisierte finanzielle Vereinbarungen vorgelegt und geschlossen werden.

- **Ressourcenreservoir** — Die öffentlichen Cloud-Bereitstellungsmodelle ermöglichen die gemeinsame Nutzung von Ressourcen durch mehrere CSC, die in keiner Beziehung zueinander stehen. Die privaten Cloud-Modelle ermöglichen Benutzern die gemeinsame Nutzung von Ressourcen innerhalb der gleichen Organisation. Die hybriden Cloud-Modelle ermöglichen Benutzern die gemeinsame Nutzung mancher Ressourcen innerhalb der gleichen Organisation und mancher Ressourcen durch mehrere CSC, die nicht notwendigerweise in einer Beziehung zueinander stehen. Die gemeinschaftlichen Cloud-Bereitstellungsmodelle ermöglichen die gemeinsame Nutzung von Ressourcen durch CSC, die in gewisser Weise in Beziehung zueinander stehen.
- **Mandantenfähigkeit** — Cloud-Umgebungen werden durch groß angelegte Virtualisierung von Servern, Speichern und Netzwerken ermöglicht. Die allgemeine Systemnutzung erfolgt üblicherweise durch viele verschiedene CSC. Mandantenfähigkeit ermöglicht die gemeinsame Nutzung von Ressourcen in einer Art und Weise, dass mehrere Mandanten und deren Rechenprozesse und Daten voneinander getrennt und füreinander unzugänglich sind. Cloud-Umgebungen verfügen üblicherweise über keinerlei permanente Beziehung zwischen bestimmten physischen Ressourcen und ihrer Nutzung durch CSC. Die CSC sind zugewiesene virtuelle Ressourcen, und die Nutzungserfassung erfolgt auf dieser Abstraktionsebene.
- **Zeitgerechte Elastizität und Skalierbarkeit** — Eine Eigenschaft des Cloud Computing, die beschreibt, wie physische oder virtuelle Ressourcen teilweise automatisiert schnell und elastisch angepasst werden können, um die Zuteilung von Ressourcen bedarfsgerecht zu erhöhen oder zu reduzieren.
- **Kompromiss zwischen Kosten und Kontrolle** — Groß angelegte, standardisierte Cloud-Dienste können zu niedrigen Einheitskosten der Versorgung in Verbindung mit standardisierten Verträgen und Cloud-SLA bereitgestellt werden. Fordert ein CSC mehr Kontrolle und Benutzeranpassung von Cloud-Diensten als von einem Standardmodell geboten, so kann dies zu zusätzlichen Kosten und über eine spezifische Cloud-SLA bereitgestellt werden.
- **Messbarer Dienst** — Ein Merkmal, das beschreibt, dass bei der Erbringung von Cloud-Diensten deren Nutzung überwacht, gesteuert und abgerechnet werden und eine Berichterstattung vorgenommen werden kann. Dies ist ein wichtiges Merkmal, das zur Optimierung und Validierung der erbrachten Cloud-Dienste notwendig ist. Der Fokus dieses Schlüsselmerkmals liegt auf dem Umstand, dass der CSC nur für die Ressourcen zu zahlen braucht, die er tatsächlich genutzt hat.
- **Allgemeiner Netzwerkzugang** — Die Tauglichkeiten von Cloud-Diensten werden über das Netzwerk zur Verfügung gestellt und der Zugriff auf diese erfolgt üblicherweise über Standardmechanismen, die die Verwendung heterogener Client-Plattformen (wie z. B. Zugriff über Mobiltelefone, Laptops und Arbeitsstationen) unterstützen.

Details von Cloud-SLA, SLO und SQO können für unterschiedliche Cloud-Dienstkategorien, Cloud-Tauglichkeitstypen und unterschiedliche Cloud-Bereitstellungsmodelle variieren (siehe ISO/IEC 17788). Cloud-SLA in diesem Dokument sollen für CSC und CSP über die Vielzahl von Cloud-Dienstkategorien und Cloud-Bereitstellungsmodellen hinweg nützlich sein. Da die Definitionen von SLO und SQO unabhängig von der Technologie und dem Geschäftsmodell sein sollen, gelten nicht alle dieser SLO oder SQO für jeden Cloud-Dienst, und diejenigen, die tatsächlich gelten, dürfen auf unterschiedliche Weise strukturiert und unterschiedlich auf die jeweiligen Cloud-Dienste angewendet werden. So kann z. B. die Dienstverfügbarkeit auf verschiedene Weisen gemessen werden, von denen manche vom jeweiligen Cloud-Dienst abhängen: Ein rechenintensiver Cloud-Dienst unterscheidet sich von einem E-Mail-Cloud-Dienst, weshalb die Dienstverfügbarkeit für diese unterschiedlich berechnet wird.

6 Beziehung zwischen der Cloud-Dienstleistungsvereinbarung und Cloud-Dienstgütevereinbarung (Cloud-SLA)

Cloud-Dienste, insbesondere öffentliche Cloud-Dienste, beinhalten üblicherweise eine Vereinbarung zwischen dem CSC und dem CSP in Bezug auf den Erwerb und die Nutzung der Cloud-Dienste. Für die Anwendung dieses Dokuments wird die rechtliche Vereinbarung als „Cloud-Dienstleistungsvereinbarung“ oder CSA bezeichnet. Die CSA verfügt über mehrere Synonyme, wie z. B. „Rahmenvereinbarung“, „Kundenvereinbarung“, „Nutzungsbedingungen“ oder lediglich „Vereinbarung“.

Eine CSA umfasst einen oder mehrere Teile, der/die in einem oder mehreren Dokumenten festgehalten ist/sind. Inhalte jedes Teils können in mehr als einem Dokument erscheinen. Es besteht keine normative Beziehung zwischen Teilen und Dokumenten, d. h. ein Teil muss nicht in einem einzigen Dokument enthalten sein und ein Dokument muss keinen vollständigen Teil beinhalten. Es existiert weder eine genormte Benennungskonvention für die Teile oder Dokumente einer CSA noch eine genormte Struktur für die Dokumente oder Teile.

Übliche Teile von CSA können z. B. folgende sein.

- Cloud-Dienstgütevereinbarung (Cloud-SLA)

Die Cloud-SLA beinhaltet üblicherweise eine Sammlung von mehreren SLO und SQO in Bezug auf den Cloud-Dienst, die verschiedene Aspekte des Dienstes abdecken. Hierzu können Verfügbarkeit, Verlässlichkeit, Leistungsfähigkeit, Sicherheit, Datenschutz, Konformität und Datenverarbeitung gehören.

- Nutzungsbedingungen

Die Nutzungsbedingungen definieren üblicherweise Grenzen für die Nutzung des Cloud-Dienstes durch den CSC. Hierzu können Einschränkungen gehören, die den CSC davon abhalten, Schadsoftware im Cloud-Dienst zu installieren, oder die die Art der speicherbaren Daten begrenzen.

- Sicherheitsleitlinie

Die Sicherheitsleitlinie beschreibt üblicherweise für den CSC und den CSP geltende Verantwortlichkeiten, SLO und SQO, die der CSP in Bezug auf Sicherheit auf den Cloud-Dienst anwendet, und gibt gegebenenfalls an, welche Sicherheitszertifikate oder Normen vom Cloud-Dienst eingehalten werden.

- Datenschutzbestimmungen

Die Datenschutzbestimmungen behandeln üblicherweise den Umgang mit personenbezogenen Daten oder sensiblen Daten durch den Cloud-Dienst, einschließlich SQO für spezifische Datenschutzmaßnahmen und Datenschutzzertifikate oder -normen, die für den Dienst gelten.

- Leitlinie zur Aufrechterhaltung der Betriebsfähigkeit

Die Leitlinie zur Aufrechterhaltung der Betriebsfähigkeit behandelt üblicherweise die Resilienzaspekte des Cloud-Dienstes und kann Maßnahmen beinhalten, die vom CSP umgesetzt werden, um Datenverlust zu vermeiden und mit Ausfällen umzugehen, wie z. B. Datensicherungen und redundante Komponenten.

- Upgrade-Leitlinie

Die Upgrade-Leitlinie deckt üblicherweise Änderungen an den Eigenschaften und Funktionen für die betroffenen Dienste sowie damit zusammenhängende Änderungen an der Management-Schnittstelle ab. Regelmäßige Aktualisierungen werden üblicherweise ebenfalls in der Upgrade-Leitlinie behandelt.

— Kündigungsbestimmungen

Die Kündigungsbestimmungen behandeln üblicherweise die Themen, die im Falle einer Beendigung der Nutzung eines oder mehrerer Cloud-Dienste durch einen CSC aufkommen. Die Kündigungsbestimmungen beinhalten gegebenenfalls verschiedene SQO für Themen wie Mitteilungen, Reversibilität und Löschung von Daten.

Der Inhalt jedes einzelnen Teils sowie die Anzahl an Teilen in der CSA kann zwischen verschiedenen Cloud-Diensten variieren – jedes einzelne Element, einschließlich der in diesem Dokument beschriebenen SLO und SQO, kann bei unterschiedlichen Diensten in unterschiedlichen Teilen erscheinen. So werden z. B. SLO und SQO in Bezug auf Sicherheit gegebenenfalls entweder in den Sicherheitsvorschriften beschrieben oder erscheinen in der Cloud-SLA. Für den CSC ist es jedoch wichtig, sämtliche Dokumente, denen der Cloud-Dienst unterliegt, zu kennen, während in der CSA auf sämtliche geltenden Dokumente verwiesen werden soll.

7 Bewährte Methoden des Cloud-SLA-Managements

7.1 Allgemeines

Das Cloud-SLA-Management deckt die Themen in Bezug auf den Entwurf, die Beurteilung, die Verhandlung und Annahme, die Einführung und Umsetzung sowie auf Änderungen an der Cloud-SLA ab. CSC sollten sicherstellen, dass Cloud-SLA und andere relevante Dokumente auf ihre Geschäftsfälle und allgemeine Strategie ausgerichtet sind. CSC sollten sich darüber bewusst sein, dass ein Cloud-Dienst gegebenenfalls verschiedenen Dokumenten unterliegt. Weitere Informationen sind in Abschnitt 6 aufgeführt.

7.2 Entwurf

Eine Cloud-SLA gilt für die in der Cloud-SLA angegebenen betroffenen Dienste. Eine einzelne Cloud-SLA darf für mehrere CSC oder für einen einzelnen CSC gelten. In Fällen, in denen die Cloud-SLA vom CSC und dem CSP gemeinsam entworfen wird, sollten beide Parteien die in 7.2 dargestellten Schritte gemeinsam durchführen. Ein CSP sollte die Cloud-SLA so entwerfen, dass diese den Bedürfnissen seiner CSC gerecht wird und auf die Tauglichkeiten der betroffenen Dienste ausgerichtet sind.

Der Entwurfsprozess der Cloud-SLA sollte die entsprechenden Rollen berücksichtigen. ISO/IEC 17789 kann als Referenzdokument für die Bestimmung der entsprechenden Schlüsselrollen verwendet werden. Schlüsselrollen für den Entwurfsprozess der Cloud-SLA, auf den in ISO/IEC 17789 näher eingegangen wird, beinhalten

- den Cloud-Dienstleistungskunden als Partei, mit der zum Zweck der Nutzung von Cloud-Diensten eine Geschäftsbeziehung besteht,
- den Cloud-Dienstleister als Partei, die Cloud-Dienste bereitstellt, und
- den Cloud-Dienstleistungspartner als Partei, die in Unterstützung oder Ergänzung der Aktivitäten des CSP und/oder des CSC handelt.

ISO/IEC 17789 beinhaltet Konzepte, die bei Erarbeitung einer Cloud-SLA verwendet werden können. Die Wahl von in einer Cloud-SLA mit einzubindenden Konzepten ist abhängig vom Cloud-Dienst und dem Geschäftskontext. Der Prozess zur Änderung der Cloud-SLA sowie zur Benachrichtigung der CSC über Änderungen sollte von der Cloud-SLA oder einem anderen geltenden Dokument abgedeckt werden.

Die Entwurfsphase sollte zudem die Mechanismen berücksichtigen, die der CSC und der CSP nutzen können, um jedes Dienstmerkmal zu überwachen und nicht eingehaltene SLO- und SQO-Selbstverpflichtungen zu melden.

7.3 Beurteilung und Annahme

CSC können dieses Dokument bei der Beurteilung von Cloud-SLA als Referenzdokument nutzen. CSC können sämtliche Konzepte prüfen und bestimmen, welche für ihre Geschäftsziele entscheidend sind. CSC können dann die Cloud-SLA (und Rechtsmittel) des CSP bei der Beurteilung, ob die Dienste des CSP den Geschäftszielen des CSC entsprechen, berücksichtigen.

CSC können Cloud-SLA im Kontext der Geschäftsleitlinien ihrer Organisation und anderer Anforderungen prüfen und so bestimmen, welche SLO, SQO und Diensteseigenschaften für jeden ihrer Anwendungsfälle wichtig sind. Auf Normenreihen wie z. B. ISO/IEC 20000 und ISO/IEC 27000 darf in Cloud-SLA oder anderer Dokumentation verwiesen werden. In manchen Fällen lassen CSP ihre Konformität mit bestimmten Industrienormen zertifizieren. CSC können bestimmen, welche Normen für ihre Geschäftsziele wichtig oder für ihre Governance wünschenswert sind, und feststellen, ob die Übereinstimmung eines Cloud-Dienstes mit dieser Norm zertifiziert wurde, oder ob in der Cloud-SLA oder anderer Dokumentation darauf verwiesen wird. CSC können festlegen, wie sie Merkmale von Cloud-Diensten überwachen und nicht eingehaltene SLO- und SQO-Selbstverpflichtungen melden, indem sie sich, sofern vorhanden, mit der Leitlinie zur Mitteilung von Ausfällen des CSP vertraut machen. Verfahren zur Überwachung und Meldung beinhalten Managementsysteme, Anwendungen angeschlossener Geräte, Web-Portale, E-Mails, Textnachrichten, Telefonnachrichten und Posts auf Seiten sozialer Medien.

Die Annahme einer Cloud-SLA darf durch Aktivieren eines Kontrollkästchens auf einer Webseite, durch eine Registrierung für den Cloud-Dienst oder durch eine formelle Unterzeichnung der Vereinbarung durch beide Parteien erfolgen. Jede Partei sollte sicherstellen, dass sie bereit ist, die Einführung und Umsetzung der Cloud-SLA vorzunehmen, unabhängig von der Art der Annahme. Im Falle einer Vereinbarung mit Sonderbestimmungen sollten beide Parteien sicherstellen, dass sie bereit sind, die Einführung und Umsetzung dieser Bestimmungen zu unterstützen.

7.4 Einführung und Umsetzung

Die Einführung einer Cloud-SLA beinhaltet die Einrichtung von Prozessen zur Überwachung und Verwaltung von Merkmalen des Cloud-Dienstes, zur Meldung jeglicher nicht eingehaltener SLO und SQO sowie zur Geltendmachung jeglicher Rechtsmittel. In manchen Fällen ist bei der Einführung der Cloud-SLA gegebenenfalls eine Zusammenarbeit des CSP mit dem CSC erforderlich. CSC sollten die Cloud-SLA auch in ihre interne Governance aufnehmen. Die Wahl der Konzepte, die in die Überwachungs- und Auditprozesse der Cloud-SLA eingebunden werden sollen, ist abhängig vom Cloud-Dienst und dem Geschäftskontext.

Die Umsetzung der Cloud-SLA beinhaltet die Bereitstellung und den Betrieb des Cloud-Dienstes durch den CSP, einschließlich des Managements und der Überwachung der Dienstgüte. Ist ein CSC der Ansicht, dass ein SLO oder SQO nicht eingehalten wurde, so darf der CSC die Leitlinie zur Mitteilung von Ausfällen befolgen.

7.5 Änderungen an der Cloud-SLA

Änderungen bilden einen unverzichtbaren Teil jedes IKT-Systems, und Cloud-SLA sind hierbei keine Ausnahme, ob aufgrund von Änderungen an Tauglichkeiten oder geänderter Anforderungen des CSC. Der CSP kann ein Verfahren einbeziehen, anhand dessen Änderungen an der Cloud-SLA vorgenommen und dies den CSC mitgeteilt wird. Der CSP kann zudem Mechanismen aufnehmen, die es CSC ermöglichen, Änderungen an der Cloud-SLA anzufordern.

CSC können die Prozesse für Änderungen an der Cloud-SLA und diesbezügliche Mitteilungen in der Beurteilungs- und Annahmephase beurteilen. CSC können zudem bestimmen, ob die aktuelle SLA oder vorgeschlagene SLA ihren Geschäftszielen entspricht, und, wenn nicht, Änderungen an der SLA anfordern.

8 Die Funktion von Cloud-Dienstgütezielen, Qualitätszielen des Cloud-Dienstes, Metriken, Rechtsmitteln und Ausnahmen in der Cloud-SLA

8.1 Allgemeines

Die Möglichkeit einer Überwachung des Cloud-Dienstes ist von entscheidender Bedeutung, damit sichergestellt wird, dass die SLO und SQO der Cloud-SLA eingehalten werden. Es ist wichtig, dass innerhalb der Cloud-SLA oder einem zugehörigen Dokument Rechtsmittel für den Fall beschrieben werden, dass ein Ziel nicht eingehalten wird. Außerdem treten möglicherweise auch Ereignisse oder Vorfälle auf, die zu Ausnahmen erklärt werden. In solchen Fällen wird das entsprechende Rechtsmittel nicht ausgelöst, auch wenn ein SLO oder SQO nicht eingehalten wird.

8.2 Metriken

Die Definition und Nutzung von angemessenen Metriken und ihrer zugrunde liegenden Messungen und Messergebnisse sind ein wesentlicher Aspekt der Cloud-SLA. Die Metriken werden dazu genutzt, die Grenzen und Fehlergrenzen, die der CSP einhält, sowie deren Einschränkungen festzulegen. Diese Metriken dürfen zur Laufzeit für die Dienstüberwachung oder für Abhilfemaßnahmen genutzt werden.

Cloud-Dienstmetriken gehen auf folgende Erfordernisse ein (Aufzählung nicht vollständig):

- Bestimmung, ob SLO eingehalten werden;
- Kategorisierung von Diensttauglichkeiten;
- Festlegung eines Zwecks für Messungen und Messergebnisse;
- Bereitstellung einer einheitlichen Darstellung von Informationen zu Messungen und Messergebnissen;
- Verknüpfung von Eigenschaften, Messungen und Metriken;
- Ermöglichung eines Vergleichs der Überwachung unterschiedlicher Dienste;
- Bestimmung der Effektivität von Cloud-Diensten im Hinblick auf Geschäftsziele.

Cloud-Dienstmetriken sollen im Kontext der Cloud-SLA und eines bestimmten Cloud-Dienstes genutzt werden. Metriken helfen bei der Definition der zu messenden Eigenschaften von Cloud-Diensten. Die Metrik kann hinsichtlich ihrer entsprechenden Messungen, Messergebnisse, relevanten Parameter und Berechnungsformeln definiert werden sowie in Form von Messregeln. Die Metriken können zur Bestimmung dessen genutzt werden, ob die an einem bestimmten Punkt erfolgte Messung einer Eigenschaft eines Cloud-Dienstes innerhalb der angegebenen Grenzen der Eigenschaft liegt. Die Verwendung eines genormten Satzes von Metriken in der Cloud-SLA vereinfacht und beschleunigt die Definition von Cloud-SLA und SLO sowie den Vergleich von Cloud-SLA untereinander.

Ohne ordnungsgemäße Metriken ist die Durchsetzung einer Cloud-SLA schwierig oder sogar unmöglich.

8.3 SLO und SQO

8.3.1 Dienstgüten

Dienstgüten sind Messergebnisse für bestimmte Attribute des Cloud-Dienstes, die sich während des Betriebs des Dienstes verändern können. Dienstgüten werden mithilfe von Metriken ausgedrückt, die auf einer einzelnen Messung beruhen oder anhand verschiedener Messungen berechnet werden dürfen.

Dienstgütern werden für ein oder mehrere SLO erfasst (die üblicherweise während der Dienstnutzung festgelegt werden) und werden oftmals im Kontext des betroffenen Dienstes beschrieben. So könnte z. B. die Dienstgüte der Dienstverfügbarkeit für Rechendienste als SLO der Betriebszeit erfasst werden, wobei hier die Betriebszeit im Kontext von Berechnungskapazitäten als Instanzen beschrieben würde, die auf Anforderung durch eine berechnete Einheit zugänglich und nutzbar sind, während ein SLO der Dienstverfügbarkeit für Speicherdienste als SLO der Betriebszeit erfasst werden könnte, beschrieben im Kontext von Anforderungen an das gespeicherte Objekt, die zu Fehlern führen. Bestimmte SLO, und auch Rechtsmittel, sind kontextgesteuert und werden in der Cloud-SLA eindeutig definiert.

Cloud-SLO und Inhalte von Cloud-SLA können für unterschiedliche Cloud-Bereitstellungsmodelle und unterschiedliche Cloud-Dienstkategorien variieren.

8.3.2 Cloud-Dienstgüteziele

Bei SLO handelt es sich um Selbstverpflichtungen eines CSP hinsichtlich bestimmter quantitativer Merkmale eines Cloud-Dienstes. Jede Dienstgüte verfügt gewöhnlich über eine Zielselbstverpflichtung, deren Einhaltung der CSP zusagt und die üblicherweise entweder aus einem einzelnen Grenzwert oder einem Wertebereich besteht. So könnte z. B. das SLO für die Dienstgüte der Dienstverfügbarkeit die Betriebszeit sein, wobei das Ziel als Prozentsatz (Betriebszeit im Verhältnis zur Gesamtzeit) ausgedrückt und eine untere Grenze der Dienstgüte darstellen würde, oder das SLO könnte die Ausfallzeit sein, wobei das Ziel ein Prozentsatz oder eine bestimmte Zeit innerhalb eines Zeitintervalls wäre und damit eine obere Grenze der Dienstgüte darstellen würde.

Der CSP darf verschiedene SLO und entsprechende Rechtsmittel anbieten.

8.3.3 Qualitätsziele des Cloud-Dienstes

SQO sind Selbstverpflichtungen eines CSP im Hinblick auf ein bestimmtes qualitatives Merkmal eines Cloud-Dienstes, wobei der Wert der Nominalskala oder Ordinalskala folgt. Die Ordinalskala berücksichtigt Fälle, in denen die Eigenschaft entweder besteht oder nicht besteht (z. B. „trifft zu oder trifft nicht zu“).

SQO-Beobachtungen erfordern menschliche Interpretation und können nicht algebraisch manipuliert werden. So könnte z. B. das Sicherheitszertifikat ein SQO darstellen und die entsprechende Aussage „CSP verfügt jederzeit über ein aktuelles Zertifikat nach ISO/IEC 27001“ lauten. Die Überprüfung einer solchen Aussage könnte über die Bereitstellung einer gescannten Kopie des Zertifikats erfolgen. Die Überprüfung der Erfüllung einer Aussage in Bezug auf ein SQO darf auf viele verschiedene Weisen erfolgen, einschließlich rechtlicher Offenlegungspflicht.

8.4 Rechtsmittel und Forderungen

8.4.1 Rechtsmittel

Rechtsmittel dürfen dem CSC vom CSP für den Fall angeboten werden, dass der Cloud-Dienst die in der Cloud-SLA definierten SLO oder SQO nicht einhält. Rechtsmittel für nicht erreichte, in der Cloud-SLA aufgeführte SLO oder SQO dürfen verschiedene Formen annehmen, wie z. B. Rückerstattungen von Gebühren, kostenlose Dienste oder andere Entschädigungsformen.

8.4.2 Forderungsprozess

Der Forderungsprozess beschreibt den Prozess für einen CSC zur Einforderung eines Rechtsmittels, wenn ein SLO oder SQO nicht eingehalten wird. Gegebenenfalls ist es Aufgabe des CSC, zu bestimmen, wann der Cloud-Dienst seine SLO oder SQO nicht eingehalten hat, und dem CSP Forderungen zu melden, während in anderen Fällen der CSP die Dienstgüte überwacht und automatisch Forderungen einleitet. Ist der CSP mit der Überwachung betraut, so erfordern Forderungen (oder unterlassene Forderungen) im Hinblick auf die Cloud-SLA gegebenenfalls eine Überprüfung.

8.5 Ausnahmen

Ausnahmen beschreiben die Umstände, unter denen die SLO, SQO und ihre jeweiligen Rechtsmittel nicht gelten. Diese können je nach Vereinbarung variieren und unterliegen gegebenenfalls den Gesetzen einer bestimmten Gerichtsbarkeit. Beispiele für Ausnahmen beinhalten geplante Unterbrechungen, Naturkatastrophen und andere Faktoren außerhalb des Einflussbereichs des CSP.

9 Komponenten der Cloud-SLA

9.1 Allgemeines

Die in Abschnitt 9 und 10 beschriebenen Komponenten der Cloud-SLA definieren Konzepte, die üblicherweise in Cloud-SLA verwendet werden. Ein gemeinsames Verständnis dieser Konzepte zwischen dem CSC und CSP ist von entscheidender Bedeutung. Zudem ist es wichtig, anzuerkennen, dass diese Konzepte und ihre jeweiligen Begriffe und Metriken von dem Kontext abhängig sind, der auf Grundlage des abgedeckten Cloud-Diensts gebildet wird. Aufgeführte SLO und ihre jeweiligen Metriken sowie die SQO, die in den Komponenten der Cloud-SLA aus Abschnitt 9 und Abschnitt 10 aufgeführt werden, verstehen sich nicht als Vorschriften oder vollständige Aufstellung für CSP zur Verwendung in ihren Cloud-SLA.

Für jede Komponente werden eine Beschreibung, ihre Relevanz sowie die dazugehörigen SLO und SQO aufgeführt. Manche SLO und SQO werden als Aussagen formuliert, die beschreiben, was in der Cloud-SLA enthalten wäre, während andere SLO und SQO als Beschreibung der jeweiligen Konzepte formuliert werden.

Wie in Abschnitt 6 erwähnt, dürfen die nachfolgend aufgeführten Komponenten der Cloud-SLA in mehreren Dokumenten, aus denen eine CSA besteht, vorhanden sein.

9.2 Komponente der betroffenen Dienste

9.2.1 Beschreibung

Die Komponente der betroffenen Dienste identifiziert die Cloud-Dienste, die von der Cloud-SLA betroffen sind. Alle weiteren Teile der Cloud-SLA gelten für die Dienste, die in der Komponente der betroffenen Dienste identifiziert werden.

Eine Cloud-SLA darf z. B. folgende Aussage beinhalten:

„Diese Dienstgütevereinbarung gilt für folgende(n) Dienst(e) der XYZ Inc.:

- XYZ Online Mail
- XYZ BLOB Storage”

Deckt eine Cloud-SLA mehrere Dienste ab, ist gegebenenfalls eine getrennte Auflistung der SLO und SQO für jeden einzelnen betroffenen Dienst erforderlich.

9.2.2 Relevanz

Ein CSP darf eine beliebige Anzahl an Cloud-Diensten anbieten, die von einer oder mehreren Cloud-SLA betroffen sind. Für den CSC ist es wichtig, genau zu wissen, welche Cloud-Dienste von einer bestimmten Cloud-SLA betroffen sind.

9.3 Komponente der Cloud-SLA-Definitionen

9.3.1 Beschreibung

Die Komponente der Definitionen beinhaltet Begriffe, die CSP-spezifisch sind oder für das Verständnis der Vereinbarung besonders wichtig sind. Von der Komponente der Definitionen wird erwartet, dass darin, wenn möglich, Definitionen aus Industrienormen verwendet werden.

9.3.2 Relevanz

Es ist wichtig, dass der CSC die Definitionen von Begriffen, die für die Cloud-SLA von Bedeutung sind, sowie Begriffe, deren Definitionen SLA-spezifisch sind, versteht.

9.4 Komponente der Dienstüberwachung

9.4.1 Beschreibung

Die Komponente der Dienstüberwachung listet für die betroffenen Dienste die Parameter auf, die vom CSP überwacht werden, sowie die dem CSC bereitgestellten Daten. Diese Parameter können die in diesem Dokument beschriebenen sowie andere Parameter beinhalten.

9.4.2 Relevanz

CSP dürfen Berichterstattungsfunktionen oder Überwachungswerkzeuge für CSC zur Überwachung der Leistungsfähigkeit des Dienstes bereitstellen. Berichterstattungsfunktionen und Überwachungswerkzeuge ermöglichen es CSC gegebenenfalls, zu bestimmen, ob ein SLO eingehalten wird oder nicht.

9.4.3 Qualitätsziele des Cloud-Dienstes

Parameter der Überwachung

Dem CSC werden eine Auflistung von Parametern für die betroffenen Dienste, die vom CSP überwacht werden, und die Daten zur Verfügung gestellt.

Überwachungsmechanismen

Eine Auflistung von dem CSC zur Verfügung stehenden Mechanismen, wie z. B. Protokolle, die eine Beschreibung der überwachten Parameter beinhaltet sowie eine Beschreibung jeglicher Bestimmungen, denen die Verfügbarkeit dieser Mechanismen unterliegt.

9.5 Komponente der Rollen und Zuständigkeiten

9.5.1 Beschreibung

Die Komponente der Rollen und Zuständigkeiten liefert eine Beschreibung der Rollen und Zuständigkeiten des CSP und auch des CSC. Cloud Computing beinhaltet zahlreiche Rollen sowohl seitens des CSC als auch seitens des CSP. Viele dieser Rollen sind in ISO/IEC 17789 beschrieben. Eine klare Beschreibung der Rollen mit Relevanz für einen bestimmten Cloud-Dienst sowie der Zuständigkeiten dieser Rollen sind für die erfolgreiche Nutzung und den erfolgreichen Betrieb des Cloud-Dienstes von entscheidender Bedeutung.

9.5.2 Relevanz

Eine klare Beschreibung der Aufteilung der Rollen und Zuständigkeiten zwischen dem CSC und dem CSP kann helfen, Verwechslungen und Missverständnisse zu vermeiden.

10 Inhaltsbereiche der Cloud-SLA und ihre Komponenten

10.1 Allgemeines

Die im Folgenden beschriebenen Inhaltsbereiche der Cloud-SLA sind Bereiche, in denen ein CSP eine Cloud-SLA anbieten könnte. Ein Inhaltsbereich einer Cloud-SLA wird durch eine oder mehrere SLA-Komponenten beschrieben. Der Inhalt einer Cloud-SLA sowie die dazugehörigen SLO, SQO und Metriken sind abhängig vom Kontext, der vom jeweils genutzten Cloud-Dienst gebildet wird.

10.2 Inhaltsbereich der Zugänglichkeit

10.2.1 Komponente der Zugänglichkeit

10.2.1.1 Beschreibung

Die Komponente der Zugänglichkeit (3.1) beschreibt die unterstützenden Technologien, die der CSP als Teil der betroffenen Dienste einsetzt.

10.2.1.2 Relevanz

Weltweit gibt es Millionen von Menschen mit Behinderungen, die ihnen die Nutzung von Informations- und Kommunikationstechnik (IKT) erschweren. Unterstützende Technologien, wie z. B. Lupen, Bildschirmleseprogramme (en: Screenreader), Braille-Lesegeräte und alternative Eingabegeräte stehen für Client-Datenverarbeitungsplattformen zur Verfügung, um die Nutzung von IKT, einschließlich Cloud-Dienste, für Menschen mit Behinderungen zu vereinfachen.

Es existieren Normen, die zur Bereitstellung von Cloud-Diensten für Menschen mit Behinderungen genutzt werden können. Hierzu gehören u. a.:

- W3C-Richtlinien für die Barrierefreiheit von Web-Inhalten (WCAG) 2.0, auch veröffentlicht als ISO/IEC 40500:2012;
- ISO/IEC TR 29138 (alle Teile) — Accessibility considerations for people with disabilities (de: Berücksichtigung der Zugänglichkeit für Personen mit Behinderungen) und
- ISO/IEC Guide 71 — Guide for addressing accessibility in standards (de: Leitfaden zur Berücksichtigung von Barrierefreiheit in Normen).

Darüber hinaus verfügen Regierungen über Leitlinien und Anforderungen in Bezug auf zugängliche IKT, wie z. B. Abschnitt 508 des Rehabilitation Act von 1973 in den Vereinigten Staaten von Amerika und EN 301 549 — Anforderungen an die Barrierefreiheit für öffentliche Beschaffung von IKT-Produkten und -Dienstleistungen in Europa.

10.2.1.3 Qualitätsziele des Cloud-Dienstes

Zugänglichkeitsnormen

Eine Aufstellung der Normen in Bezug auf Zugänglichkeit, nach denen sich der CSP bei den betroffenen Diensten richtet.

Zugänglichkeitsleitlinien

Eine Aufstellung der Leitlinien und Regulierungen für zugängliche IKT, nach denen sich der CSP bei den betroffenen Diensten richtet.

10.3 Inhaltsbereich der Verfügbarkeit

10.3.1 Komponente der Verfügbarkeit

10.3.1.1 Beschreibung

Verfügbarkeit ist die Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich¹⁾ und nutzbar zu sein (ISO/IEC 17788). Die Komponente der Verfügbarkeit spezifiziert das Verfahren zur Feststellung, dass die betroffenen Dienste zugänglich und nutzbar sind.

10.3.1.2 Relevanz

Verfügbarkeit liefert CSC einen hochwertigen Indikator dafür, dass die betroffenen Dienste auf Anfragen antworten und die in der Dienstbeschreibung aufgeführten Funktionen zu einem bestimmten Zeitpunkt erfüllen.

Zeiträume, in denen der Cloud-Dienst nicht verfügbar ist, werden üblicherweise als „Ausfallzeiten“ bezeichnet. Es entstehen gegebenenfalls Situationen, wie z. B. „geplante Ausfallzeiten“, in denen der Cloud-Dienst aus nicht fehlerbedingten Gründen nicht verfügbar ist. Zeiträume, in denen der Cloud-Dienst nicht verfügbar ist, die jedoch nicht als Ausfallzeit gerechnet werden, werden als „zulässige Ausfallzeiten“ bezeichnet.

Verfügbarkeit wird oftmals als die Gesamtzeit in einem definierten Intervall abzüglich der Ausfallzeit während dieses Zeitintervalls ausgedrückt.

10.3.1.3 Cloud-Dienstgüteziele

Verfügbarkeit

Die Menge oder der Prozentsatz an Zeit innerhalb eines bestimmten Zeitraums, in der/dem der Cloud-Dienst zugänglich und nutzbar ist.

Verfügbarkeit darf als Gesamtzeit über verschiedene definierte Intervalle abzüglich der Gesamtausfallzeit während der einzelnen Intervalle berechnet werden und darf zulässige Ausfallzeiten ausschließen.

Für weitere Informationen siehe ISO/IEC 19086-2.

10.4 Inhaltsbereich der Leistungsfähigkeit des Cloud-Dienstes

10.4.1 Allgemeines

Die Leistungsfähigkeit des Cloud-Dienstes beinhaltet individuelle Komponenten, die in einer Cloud-SLA verwendet werden können, um die Leistungsfähigkeit eines Cloud-Dienstes auszudrücken. Es ist anzumerken, dass die Definition von Leistungsfähigkeit in Abhängigkeit des Cloud-Dienstes, des CSP und (möglicherweise) des CSC variieren kann. Die hier aufgeführten Komponenten verstehen sich nicht als Vorschriften.

10.4.2 Komponente der Antwortzeit des Cloud-Dienstes

10.4.2.1 Beschreibung

Es gibt verschiedene Eigenschaften in Bezug auf die Ansprechbarkeit des Cloud-Dienstes, die in die Cloud-SLA mit aufgenommen werden können.

Die Antwortzeit ist die Zeit zwischen einem Impuls an den Cloud-Dienst und der Antwort des Dienstes auf den Impuls.

1) Im Kontext von Verfügbarkeit bedeutet zugänglich, dass auf den Cloud-Dienst über seine Schnittstellen erfolgreich zugegriffen werden kann.

10.4.2.2 Relevanz

Ein Impuls kann von verschiedenen Quellen, wie z. B. von CSC, Partnern, CSP und programmatischen Ereignissen, ausgelöst werden.

Ausfallzeiten können zwischen verschiedenen Cloud-Diensten variieren, selbst wenn die Kombination aus Client-System, Arbeitsbelastung und Transaktionen identisch ist. Beim Vergleich von Antwortzeiten ist zu berücksichtigen, ob (a) die gleichen Metrikdefinitionen verwendet werden und (b) andere Variablen (wie z. B. Netzwerklatenz, Netzwerkdurchsatz, Übertragungsverzögerung, Latenz in der Weiterleitung) bei diesen Vergleichen als gleichwertig angesehen werden können.

Für weitere Informationen siehe ISO/IEC 19086-2.

10.4.2.3 Cloud-Dienstgüteziele

beobachtete längste Antwortzeit des Cloud-Dienstes

Die längstmögliche Zeit zwischen einem definierten Impuls an oder einer definierten Eingabe in den Cloud-Dienst und einem definierten Zeitpunkt innerhalb der Antwort.

Mittelwert der Antwortzeit des Cloud-Dienstes

Statistisches Mittel über eine Reihe beobachteter Antwortzeiten des Cloud-Dienstes.

Die Spezifikation des Verfahrens zur Berechnung des Mittelwerts ist für mit dem Cloud-Dienst in Verbindung stehende Metriken definiert.

Varianz in der Antwortzeit des Cloud-Dienstes

Statistische Varianz beschreibt, wie weit die Antwortzeiten innerhalb einer Reihe beobachteter Antwortzeiten des Cloud-Dienstes wahrscheinlich vom Mittelwert entfernt sind.

Varianz wird oftmals als Standardabweichung vom Mittelwert einer Reihe von Messungen beschrieben.

Dieses SLO kann dazu verwendet werden, die Stabilität der Antwortzeit über eine Zeitspanne anzugeben — es zeigt an, wie viel Varianz oder statistische Streuung ausgehend von der durchschnittlichen Antwortzeit besteht.

Die Varianz der Antwortzeit ist auch dann von Bedeutung, wenn der Benutzer die Systemleistung bei verschiedenen Belastungsstufen messen möchte und wenn der Benutzer die Systemleistung für ein bestimmtes Ereignis messen möchte.

10.4.3 Komponente der Kapazität des Cloud-Dienstes

10.4.3.1 Beschreibung

Dieser Unterabschnitt gibt Erklärungen zu Diensteigenschaften in Bezug auf die Kapazität des Dienstes, die in die Cloud-SLA aufgenommen werden können. Diese Eigenschaften in Bezug auf Kapazität beinhalten nicht nur die Kapazität der Cloud-Ressourcen (wie z. B. Speicherplatz, Verarbeitungsleistung), sondern auch die Kapazität des Netzwerks, das für den Zugriff auf die Ressourcen verwendet wird.

10.4.3.2 Relevanz

Da sich die Kapazität eines Cloud-Systems ändern kann, ist es wichtig, zu wissen, welche Kapazität besteht und wie diese durch den CSC nutzbar ist. In herkömmlichen gerätebasierten Systemen ist die Kapazität feststehend, während die Kapazität in einem Cloud-System dynamisch ist und nachverfolgt werden muss, um sicherzustellen, dass das System die Anforderungen des CSC erfüllt. Die Gebührenabrechnung für den Cloud-Dienst darf auch auf Kapazität und/oder Kapazitätsgrenzen beruhen.

10.4.3.3 Cloud-Dienstgüteziele

Grenze gleichzeitiger Verbindungen mit dem Cloud-Dienst

Größtmögliche Anzahl an gleichzeitigen Verbindungen, die vom Cloud-Dienst unterstützt wird.

Grenze der verfügbaren Ressourcen des Cloud-Dienstes

Größtmögliche Kapazität von verfügbaren Ressourcen, d. h. Speicherplatz, CPU-Leistung, Arbeitsspeichergröße, Seitenansicht usw.

Durchsatz des Cloud-Dienstes

Die Anzahl an Eingaben oder die Anzahl an voneinander abhängigen Eingabesätzen (d. h. eine Transaktion), die vom Cloud-Dienst je Zeiteinheit verarbeitet werden kann. Diese wird üblicherweise als Web-Anforderungen pro Sekunde, Seitenelemente pro Sekunde und Transaktionen pro Sekunde gemessen.

Bandbreite des Cloud-Dienstes

Die Menge an Daten, die innerhalb eines bestimmten Zeitraums übertragen werden kann.

10.4.4 Komponente der Elastizität

10.4.4.1 Beschreibung

Die Komponente der Elastizität beschreibt die Fähigkeit eines Cloud-Dienstes, die Menge an Ressourcen, die einer Instanz des Dienstes zugeordnet sind, dynamisch anzupassen. Die Anpassung erfolgt auf der Grundlage der aktuellen Arbeitslast der Instanz des Cloud-Dienstes, d. h. dass eine gesteigerte Arbeitslast zur Zuweisung von mehr Ressourcen führt, während eine geringere Arbeitslast zur Freigabe von Ressourcen führt.

Somit ist die Elastizität abhängig von der Verfügbarkeit eines Verfahrens, das Schwankungen in der Arbeitslast überwacht und auf diese reagiert, indem mehr Ressourcen zugewiesen oder Ressourcen, die nicht mehr gebraucht werden, freigegeben werden. Das Verfahren kann entweder manuell oder automatisch erfolgen. Im Falle des manuellen Verfahrens ist es Aufgabe des CSC, die Menge der benötigten Ressourcen in Abhängigkeit der sich ändernden Arbeitslast zu bestimmen. Das automatische Verfahren erfolgt ohne direkte Interaktion des CSC oder des CSP. Im Falle des automatischen Verfahrens kann dieses entweder reaktiv erfolgen, d. h. auf der Grundlage der Überwachung der tatsächlichen Veränderungen in der aktuellen Arbeitslast, oder proaktiv, d. h. unter Zuhilfenahme eines Algorithmus zur Vorhersage der zukünftigen Auslastungssituation, oder aber eine Kombination aus beiden darstellen.

Die Elastizität steht mit einem oder mehreren Ressourcentypen in Beziehung. Eine virtuelle Maschine kombiniert z. B. die folgenden Ressourcen: Anzahl an Prozessoren einer bestimmten Spezifikation, Arbeitsspeichergröße, Anzahl an Netzwerkschnittstellen, Festplattengröße usw. Bei Ressourcen für einen web-basierten Anwendungsdienst kann es sich um die Anzahl an parallelen Benutzersitzungen und/oder die Anzahl an parallelen Transaktionen handeln.

10.4.4.2 Relevanz

Elastizität ist eines der Hauptmerkmale von Cloud-Diensten. CSC müssen während der Dienstkonfiguration nicht eine ausreichende Menge an Ressourcen für den Cloud-Dienst zuweisen, sondern können sich auf die Fähigkeit des Cloud-Systems verlassen, Ressourcen im Laufe der Zeit nach Bedarf aufzustocken und Ressourcen, die nicht mehr gebraucht werden, zu verringern. Der CSC darf Ressourcen manuell hinzufügen und reduzieren oder Werkzeuge des CSP nutzen, die es dem CSC ermöglichen, Regeln für das Aufstocken oder Verringern von Ressourcen festzulegen. Somit vermeiden CSC eine Überprovisionierung von Ressourcen für den Cloud-Dienst und müssen demzufolge nicht kontinuierlich für Ressourcen bezahlen, die sie ausschließlich im Falle von Arbeitslastspitzen nutzen.

10.4.4.3 Cloud-Dienstgüteziele

Elastizität

Die Charakterisierung der Elastizität eines Cloud-Dienstes kann im Hinblick auf zwei Ziele beurteilt werden:

Geschwindigkeit der Elastizität

Die Geschwindigkeit der Elastizität beschreibt, wie schnell ein Cloud-Dienst in der Lage ist, auf eine Ressourcenanforderung zu reagieren, wenn

- der CSC eine Neuzuweisung einer Ressource anfordert (im Falle manueller Elastizität) oder
- sich die Arbeitslast ändert (im Falle automatischer Elastizität).

Die Geschwindigkeit kann innerhalb von Schwellenwerten ausgedrückt werden. Diese Geschwindigkeit kann über einen Messprozess festgelegt werden und definiert somit eine Metrik.

Präzision der Elastizität

Die Präzision der Elastizität beschreibt, wie präzise die Ressourcenzuweisung den tatsächlichen Ressourcenbedarf zu einem bestimmten Zeitpunkt erfüllt.

- Im manuellen Fall hängt die Präzision von der Detailgenauigkeit der Ressourcenzuweisung ab, d. h. von der Mindestmenge an Ressourcen, die neu zugewiesen werden können. Somit stellt die Präzision im manuellen Fall ein technisches Merkmal des Cloud-Dienstes dar, das keine Messungen erfordert (d. h. damit ist keine Metrik verbunden).
- Im automatischen Fall bezieht sich Präzision auf den Unterschied zwischen der Menge an zugewiesenen Ressourcen und der Menge an Ressourcen, die tatsächlich erforderlich ist (der Optimalzustand), um einer bestimmten Arbeitslast gerecht zu werden. Die tatsächliche Ressourcenzuweisung ist gegebenenfalls überprovisioniert (d. h. es sind mehr Ressourcen zugewiesen als tatsächlich benötigt werden) oder unterprovisioniert (d. h. die Menge an tatsächlich zugewiesenen Ressourcen ist nicht ausreichend, um der tatsächlichen Arbeitslast gerecht zu werden). Im Gegensatz zum manuellen Fall kann im automatischen Fall der Unterschied zwischen der zugewiesenen und der tatsächlich benötigten Menge an Ressourcen durch einen Messprozess bestimmt werden, wofür eine Metrik mit einbezogen wird.

Die Präzision kann innerhalb von Schwellenwerten ausgedrückt werden.

10.5 Inhaltsbereich des Schutzes personenbezogener Informationen (PII)

10.5.1 Komponente des Schutzes von PII

Beschreibung

Personenbezogene Informationen (PII) sind Informationen, die dazu verwendet werden können, die betroffene Person, auf die sie sich beziehen, zu identifizieren, oder direkt oder indirekt mit einer betroffenen Person verknüpft werden können. Die betroffene Person ist die Person, auf die sich die PII beziehen. Der PII-Beauftragte bestimmt den Zweck und die Mittel zur Verarbeitung von PII, während ein PII-Verarbeiter PII im Auftrag von einem PII-Beauftragten und in Übereinstimmung mit dessen Anweisungen verarbeitet. (Siehe ISO/IEC 29100 und ISO/IEC 27018 für Erklärungen zu den hier beschriebenen Konzepten.)

Ein Verlust, eine unbefugte Offenlegung oder unbefugte Änderung von PII kann den betroffenen Personen schaden. Es ist deshalb üblich, dass Gesetze und Regulierungen den Umgang mit PII regeln, außerdem kann aus einem falschen Umgang mit PII zusätzlich eine ruf- oder geschäftsschädigende Wirkung entstehen. Im Allgemeinen obliegt die Sicherstellung des ordnungsgemäßen Umgangs mit PII hauptsächlich dem PII-Beauftragten.

Im Falle des Cloud Computing handelt es sich bei dem PII-Beauftragten im Allgemeinen um einen CSC, während es sich bei dem PII-Verarbeiter im Allgemeinen um einen CSP handelt.

Wie in Abschnitt 6 erwähnt, dürfen manche der nachfolgend beschriebenen Komponenten in anderen Dokumenten als dem der Cloud-SLA, die Bestandteil der CSA sind, dargestellt werden, wie z. B. in Datenschutzbestimmungen.

Für weitere Informationen zu Cloud-SLA und dem Schutz von PII siehe ISO/IEC 19086-4.

Relevanz

Grundsätze des Schutzes von PII sind in ISO/IEC 29100 dargestellt, ihre Anwendung für öffentliche Cloud-Dienste ist in ISO/IEC 27018 beschrieben. Die Umsetzung dieser Grundsätze, insbesondere im Kontext von Cloud-Diensten, ist abhängig von der/den für die jeweilige Gerichtsbarkeit spezifischen Gesetzgebung oder Regulierungen sowie von den in der CSA und der Cloud-SLA enthaltenen Bestimmungen.

Es bestehen nationale und internationale Normen, die vom CSP und/oder dem CSC verwendet werden können, um Bestimmungen für die CSA und die Cloud-SLA abzuleiten. Beispiele hierfür sind ISO/IEC 29151 und ISO/IEC 27018 (beide auf der Grundlage von ISO/IEC 27001), JIS Q15001, NIST/SP 800-53:2013, Anhang J und BS 10012. Manche der zuvor genannten Normen liefern Vokabular und Ratschläge zu den spezifischen PII-Themen, das/die in die CSA und Cloud-SLA eingebunden werden könnten. Siehe auch ISO/IEC 19086-4 zu Zertifikaten und Konformität.

Cloud-Dienstgüteziele

Spezifische SLO in Bezug auf die Komponente des Schutzes von PII werden in ISO/IEC 19086-4 beschrieben.

10.5.1.1 Qualitätsziele des Cloud-Dienstes

Spezifische SQO in Bezug auf die Komponente des Schutzes von PII werden in ISO/IEC 19086-4 beschrieben.

10.6 Inhaltsbereich der Informationssicherheit

10.6.1 Komponente der Informationssicherheit

10.6.1.1 Beschreibung

Der Inhaltsbereich der Informationssicherheit behandelt SLO und SQO, die sich auf Informationssicherheit für Cloud-Dienste beziehen. ISO/IEC 27017 und ISO/IEC 27018 gehen auf die Informationssicherheit für Cloud-Dienste bzw. auf den Datenschutz für Cloud-Dienste ein, wobei diese Normen wiederum auf den in ISO/IEC 27002 enthaltenen Sicherheitszielen und Sicherheitsmaßnahmen beruhen.

Informationssicherheit ist ein so allgemeines und so durchdringendes Thema, dass sie eine Vielzahl von Komponenten der Cloud-SLA für Cloud-Dienste betrifft, mit dem Ergebnis, dass zahlreiche SLO und SQO in Bezug auf Informationssicherheit über die verschiedenen in diesem Dokument beschriebenen Komponenten verteilt sind. So stellt z. B. die Verfügbarkeit ein Schlüsselthema der Informationssicherheit dar und bildet in diesem Dokument eine eigene Komponente.

Wie in Abschnitt 6 erwähnt, dürfen manche der nachfolgend beschriebenen Komponenten in anderen Dokumenten als dem der Cloud-SLA, die Bestandteil der CSA sind, dargestellt werden, wie z. B. in Sicherheitsvorschriften.

Für weitere Informationen zu Cloud-SLA und Informationssicherheit siehe ISO/IEC 19086-4.