BERICHTE DES NEGZ NR. 7

SICHERHEITSANFORDERUNGEN UND -NACHWEISE BEI CLOUD-DIENSTEN — GRUNDLAGEN FÜR ÖFFENTLICHE AUFTRAGGEBER

Stefanie Köhl
Heidrun Müller

SHI STEIN HARDENBERG INSTITUT

NEGZ Nationales E-Government Kompetenzzentrum e.V.

Für einen modernen Staat

Das Nationale E-Government Kompetenzzentrum vernetzt Experten aus Politik, Verwaltung, Wissenschaft und Wirtschaft und ist die zentrale, unabhängige Plattform für Staatsmodernisierung und Verwaltungstransformation in Deutschland.

Herausgegeben und gefördert vom
Nationalen E-Government Kompetenzzentrum e. V.
Berlin 2019

INHALT

ZUSAMMENFASSENDE EMPFEHLUNGEN

Das Ziel dieser Kurzstudie ist es, einen einführenden Überblick über die gängigsten Sicherheitsstandards für Cloud-Dienste zu geben und somit öffentlichen Institutionen und Nicht-Experten im Bereich IT- und Cloud-Sicherheit in die Lage zu versetzen, Anforderungen an eine Cloud-Lösung zu beschreiben, diese zu überprüfen und somit eine fundierte Entscheidung für oder gegen eine bestimmte Cloud-Lösung zu treffen. Denn Cloud-Systeme bieten eine neue und ressourcensparende Form der IT-Bereitstellung, erfordern aber auch eine neuartige IT-Steuerung und verändern bzw. erhöhen ggf. die Anforderungen an Sicherheit, weil eine neuartige Komplexität und Verantwortungsketten entstehen. Eine der größten Herausforderungen, um Cloud Computing im öffentlichen Sektor voranzutreiben, ist die sichere und datenschutzrechtlich konforme Verarbeitung von personenbezogenen Daten.

Die wesentlichen Erkenntnisse und Empfehlungen der Kurzstudie lauten:

Die Landschaft der existierenden (de facto) Standards zu IT-Sicherheit und Datenschutz bei Cloud-Diensten ist komplex. Zertifikate bieten zwar Orientierung, sind jedoch schwer zu beurteilen, da eine allgemein anerkannte Basis-Linie für Sicherheit im Cloud Computing noch nicht existiert.

Die vom BSI formulierten Mindestanforderungen lenken zwar den Blick auf wichtige Aspekte bei Sicherheit in der Cloud, sind allerdings für eine Leistungs- und Anforderungsbeschreibung zu vage und abstrakt, da sie auf einer oberen Ebene bleiben und nicht spezifiziert werden.

Die in der Kurzstudie beschriebenen Kriterienkataloge können dazu dienen, die Anforderungen an IT-Sicherheit und Datenschutz zu definieren, da sie sie sehr dezidiert und genau die Mindestanforderungen des BSI operationalisieren. Wichtig ist, dass die wesentlichen Aspekte genauestens formuliert sind und einen Nachweis der Erfüllung seitens des Cloud-Anbieters ermöglichen.

Sollten mehrere Kriterienkataloge herangezogen werden, sind die einzelnen Kriterien voneinander abzugrenzen bzw. zu matchen. Denn die meisten Kataloge decken zum größten Teil identische Aspekte ab, sind aber unter Umständen anders formuliert. Hier kann es sinnvoll sein, die Unterstützung des IT-Dienstleisters zu nutzen und sich selbst zu informieren, um ein besseres Gefühl für das Thema zu bekommen. Nur so können informierte Entscheidungen getroffen werden.

Liegen entsprechende Angebote von möglichen Cloud-Anbietern vor, sind die Angebote miteinander zu vergleichen und vor allem zu überprüfen, ob und wie die definierten Anforderungen, insbesondere bzgl. der Sicherheit, jeweils erfüllt werden. Ein Weg ist, auf die vom Anbieter ausgewiesenen Zertifizierungen und Testate zu vertrauen.

In aller Regel kann man sich als Anwender auf Zertifikate verlassen, weil diese meist von unabhängigen und akkreditierten Dritten ausgestellt werden. Dennoch wird Kommunen und öffentlichen Verwaltungen dringend geraten, auch den Prüfbericht zu lesen oder zumindest sich über den genauen Gegenstand und Umfang der Zertifizierung umfassend zu informieren, um diesen mit den eigenen Anforderungen abzugleichen.

Die zunehmend an Bedeutung gewinnenden Selbsterklärungen auf Basis von anerkannten Verhaltenskodizes sollten kein Misstrauen wecken. Sie bilden die Einstiegsstufe des Nachweises, den man häufig bei kleineren Anbietern findet, da Zertifizierungen durch Dritte teuer und aufwändig ist.

Der Weg zu einer Auftraggeberkompetenz führt über die Auseinandersetzung mit entsprechenden Anforderungen an IT-Sicherheit und Datenschutz in der Cloud, welche nicht nur für die Auftragsvergabe, sondern auch für die spätere Steuerung des Dienstleisters notwendig ist.

Diese Auftraggeberkompetenz im Bereich Cloud und Cloud-Sicherheit ist vor dem Hintergrund der weiteren technischen Entwicklung dringend erforderlich, um auch die Abhängigkeit von IT-Anbietern und -Beratern von vornherein zu verringern. Nur so kann die dringend erforderliche Konsolidierung insbesondere der kommunalen IT erreicht werden.

Um diesen Kompetenzaufbau zu unterstützen, sollten in einem nächsten Schritt die zahlreichen Anforderungen konsolidiert und anwendergerecht operationalisiert werden. Auf diesem Weg werden öffentliche Verwaltungen und Kommunen besser als bisher in die Lage versetzt, die Prüfung der Sicherheitsanforderungen möglichst selbstständig vorzunehmen.

Schlagworte: Cloud, Cloudsicherheit, DSGVO Compliance, Anforderungen, Zertifizierung

1. ARBEITEN IN DER CLOUD — REALITÄT, KEINE ZUKUNFTS-MUSIK?!

Die IT-Nutzung in der öffentlichen Verwaltung der letzten Jahre ist vor allem durch zwei Trends gekennzeichnet: Mobiles bzw. verteiltes Arbeiten sowie Konsolidierung bzw. Modernisierung der IT-Infrastruktur. Der Trend der IT-Konsolidierung wird vor allem angestoßen von den Anforderungen, moderne Arbeitsprozesse und Leistungen zu entwickeln sowie trotz schrumpfender Ressourcen im Personalbereich (weiterhin) eine sichere und leistungsfähige IT-Infrastruktur mit hoher Verfügbarkeit von Daten zu gewährleisten. Die Konsolidierung betrifft nicht nur die Reduzierung des Fachverfahrensportfolios und damit der Komplexität für den operativen Betrieb, sondern auch die Erneuerung und Bereitstellung von Hardware und Basis-Anwendungen für Arbeitsplätze, auch an verteilten Standorten. Aus diesem Grund sind Cloud-Dienste für öffentliche Verwaltungen attraktiv, da die Kosten und Aufwände für IT-Infrastruktur und zugehörigem Endbenutzersupport bedeutend verringert werden können. Auch für öffentliche IT-Dienstleister mit ihren Rechenzentren bieten Cloud-Technologien die Möglichkeit, Ressourcen zu konsolidieren sowie besser zu steuern und damit ihren Kundenkommunen und -behörden schnell und unkompliziert anforderungsgerecht Services und Applikationen bereitzustellen. Zusätzlich zu den Kosteneinsparungen lässt sich durch Cloud Computing auch die Qualität von IT-Leistungen steigern: Services können schnell und unkompliziert an veränderte Mengenanforderungen angepasst und durch neue Versionen ersetzt werden. Auch kleinere Kommunen mit rückläufiger Bevölkerungs- und Wirtschaftsentwicklung können so komplett IT-unterstützt ein vollständiges Leistungsangebot vor Ort anbieten.

Die Nutzung mobiler Geräte, wie Tablet-Geräte oder Smartphones, setzt sich insbesondere auf kommunaler Ebene zunehmend durch, um z.B. Distanzen in großen Landkreisen besser überbrücken zu können. Dieser Einsatz erfolgt häufig, ohne dass Konzepte und Regelungen für eine sichere Datenhaltung bzw. Bereitstellung von Daten entwickelt wurden, bzw. nutzen die Beschäftigten private Geräte mit den darauf verfügbaren Apps bzw. Cloud-Diensten, wie Dropbox und Google Drive, zum Austausch und zur Ablage von Dateien. Ebenso werden Dienste „as a Service“ wie Videokonferenzsysteme und Chat-Programme, z.B. Skype oder WhatsApp, verwendet, um sich mit Kollegen einfach und schnell austauschen zu können. Damit sind Daten der öffentlichen Verwaltung (zumindest kurzfristig) auf Speichersystemen in den USA bzw. bei US-amerikanischen Unternehmen abgelegt, die möglicherweise US-Behörden Zugang zu Daten gewähren müssen, selbst wenn die Daten im EU-Raum gespeichert wurden.[1]

Die Empirie zeigt es deutlich: Die Cloud ist im Einsatz – bewusst oder unbewusst, gesteuert oder ungesteuert, ganz einfach, weil es funktioniert. Diese Entwicklung gilt es, auch vor dem Hintergrund der erhöhten Sicherheitsanforderungen zukünftig besser zu steuern. Cloud-Systeme bieten eine neue und ressourcensparende Form der IT-Bereitstellung, erfordern aber auch eine neuartige

1 z.B. auf Basis des CLOUD Act (Clarifying Lawful Overseas Use of Data Act), https://www.congress.gov/bill/115th-congress/house-bill/4943 (letzter Zugriff: 15.03.2019)

IT-Steuerung und verändern bzw. erhöhen ggf. die Anforderungen an Sicherheit, weil eine neuartige Komplexität und Verantwortungsketten entstehen. Eine der größten Herausforderungen, um Cloud Computing im öffentlichen Sektor voranzutreiben, ist u.a. die sichere und datenschutzrechtlich konforme Verarbeitung von personenbezogenen Daten. Es sind zahlreiche Cloud-Lösungen am Markt vorhanden, auch öffentliche IT-Dienstleister bieten solche an. Dennoch ist es für Entscheidungsträger, auch in den IT-Bereichen, oft schwierig zu beurteilen, ob diese Lösungen den Anforderungen entsprechen. Standards und Zertifizierungen bieten eine Orientierung, sind jedoch schwer zu beurteilen, da sie häufig aus dem ausländischen Raum stammen bzw. auf Selbstregulierung basieren, was dem deutschen Rechtsverständnis eher fremd ist.

Die Landschaft der existierenden (de facto) Standards zu IT-Sicherheit und Cloud-Diensten ist komplex, vielfältig und von Intransparenz und Unverständlichkeit geprägt. Dabei ist es notwendig, für Entscheider, die in der Regel keine Experten sind, ein angemessenes Maß an Verständnis und Wissen herzustellen, welche Mindestanforderungen zu erfüllen sind, um eine Beschaffungsentscheidung treffen zu können. Daher ist es das Ziel dieser Kurzstudie, einen einführenden Überblick über die gängigsten Sicherheitsstandards für Cloud-Dienste zu geben und öffentlichen Institutionen damit Richtlinien an die Hand zu geben, auf welche Aspekte bei der Cloud-Nutzung zu achten ist. Insbesondere geht es darum, Kommunen in die Lage zu versetzen, Anforderungen an eine Cloud-Lösungen zu beschreiben und besser beurteilen zu können, ob ein Cloud-Anbieter diese Anforderungen erfüllt. Dazu werden in der Kurzstudie zunächst der Cloud-Ansatz beschrieben sowie ein grundlegendes Verständnis von Informationssicherheit und Datenschutz geschaffen. Anschließend werden wesentliche Standards zur Konformität mit Informationssicherheit und Datenschutz kurz beschrieben. Im Ergebnis werden Hinweise abgeleitet, die Nicht-Experten im Bereich IT- und Cloud-Sicherheit in die Lage versetzen sollen, Anforderungen an eine Cloud-Lösung zu beschreiben, diese zu überprüfen und somit eine fundierte Entscheidung für oder gegen eine bestimmte Cloud-Lösung zu treffen.

2. EINORDNUNG: CLOUD-ANSATZ, DATENSCHUTZ UND INFORMATIONSSICHERHEIT HINTERGRUND

Die Cloud hat spezifische Eigenschaften, woraus sich differenzierte Bereitstellungsmodelle und Servicetypen ergeben, die im folgenden Abschnitt kurz beschrieben werden. Dabei muss auch immer Sicherheit gewährleistet werden, was bei der Cloud schwieriger ist als bei Systemen, die physisch „im Haus" stehen. Damit Cloud funktioniert, sind Konzepte für IT-Sicherheit erforderlich, auch Informationssicherheitsmanagementsysteme (ISMS) genannt, sowie insbesondere für den öffentlichen Sektor auch ein angemessener Datenschutz zu gewährleisten, idealerweise mit einem Datenschutzmanagementsystem (DSMS). Aufgrund begrifflicher Unschärfen werden Informationssicherheit und Datenschutz kurz erläutert.

2.1 Cloud-Eigenschaften

„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software".[2] Diese weltweit verbreitete Definition verweist gleichzeitig auf die konstituierenden Eigenschaften[3], wodurch sich die Technologie von einer „normalen" Auslagerung von IT-Aufgaben bzw. den Bezug von IT-Services und -Produkten unterscheidet, z.B. über ein kommunales Gebietsrechenzentrum per Überlassungsvertrag.[4] So können Nutzer netzwerkbasiert über Standardtechnologien (Netzwerkbasierter Real-Zugang), z.B. Internet oder Virtual Private Networks (VPN), automatisiert und selbstständig, d.h. ohne menschliche Interaktion auf Anbieterseite, auf IT-Ressourcen zugreifen (Automatische Diensterbringung auf Anforderung). Diese Ressourcen sind so konfiguriert, dass eine parallele Leistungserbringung für viele Kunden möglich ist (Ressourcenpooling) und sie dynamisch an die Bedürfnisse der Kunden angepasst werden können, wodurch der Benutzer innerhalb eines gering bemessenen Zeitrahmens Zugriff auf unendlich erscheinende Ressourcen erhält (Elastizität). Monitoring- und Messfunktionen erlauben eine automatisierte optimierte Ressourcennutzung und Validierung der Servicequalität durch den Nutzer (Messbare Dienstequalität). Der Kunde bezahlt nur für die Ressourcen, die tatsächlich genutzt werden, wobei auch Flatrate-Modelle üblich sind (Pay-per-use).

2 BSI o.J.

3 vgl. NIST 2011, S. 2.

4 vgl. z.B. KGSt 2018, S. 6.

Infokasten: Bedeutung der konstituierenden Eigenschaften der Cloud aus kommunaler Sicht

Bedeutung der konstituierenden Eigenschaften aus der Perspektive einer Kommune bzw. öffentlichen Institution

Automatische Diensterbringung auf Anforderung: Keine langwiergen Vergabeverfahren für neue Services, insb. Infrastruktur, Middleware, Sicherheitsgeprüft

Netzwerkbasierter Real-Zugang: Schneller und standardisierter Zugriff von Arbeitsplätzen etc. auf Fachverfahren und Daten → keine eigenverantwortlichen Updates mit Teststellungen etc. mehr erforderlich; keine Sonderverfahren mit proprietären Schnittstellen

Ressourcenpooling: Problematisch im Hinblick auf Anforderungen des Datenschutzes und der Sicherheit der öffentlichen IT → ggf. über entsprechende technische Vorkehrungen und Nachweise der Anbieter lösbar

Schnelle Elastizität: Schnelle Aufstockung von Ressourcen, z.B. zum Austausch großer Datenmengen, oder zum Anschluss neuer Arbeitsplätze nach Fusion

Messbare Dienstequalität: Nachverfolgbarkeit der Datenverarbeitung und damit Transparenz für die Datenschutz- und IT-Sicherheitsanforderungen

Pay-per-Use: Ressourcen müssen nicht mehr vorgehalten und kosten- und personalbindend gepflegt werden

Über die „Cloud“ können verschiedene Arten von Services bezogen werden, die typischerweise in drei Ebenen eingeteilt werden: Software-, Platform- und Infrastructure-„as a Service“. Software-as-a-Service (SaaS) bietet Zugang zu Anwendungen, wie CRM-Systeme, über Platform-as-a-Service (PaaS) werden Entwicklungs- und Laufzeitumgebunden bereitgestellt für die Bereitstellung und Ausführung eigener Anwendungen. Infrastructure-as-a-service (IaaS) sind virtualisierte Rechnerressourcen, Speicher etc. Dabei nehmen die Eingriffs- und Steuerungsmöglichkeiten für verwendete jeweils darunterliegende Ressourcen typischerweise ab. Diese reduzierten Eingriffs- und Sanktionsmöglichkeiten könnten für den öffentlichen Sektor ein zu großes Risiko darstellen, so dass für bestimmte Leistungen Cloud-Technologien gar nicht bzw. nur bestimmte Bereitstellungsmodelle in Frage kommen. Bei den Bereitstellungsmodellen werden grob drei Modelle sowie ein Kombinationsmodell unterschieden.[5] Jedes der Modelle birgt jedoch Herausforderungen für die öffentliche Verwaltung, auf die überblicksartig eingegangen wird.

- **Öffentliche Clouds** sind die bekanntesten Modelle, da v.a. im persönlichen Alltag verwendet Vertragsabschlüsse und die Dienstenutzung laufen weitgehend automatisiert ab. Datensicherheit wird in öffentlichen Clouds zum Problem, Nutzer sollten über umfassende Konzepte und Sicherungsmechanismen hinsichtlich der Auslagerung schützenswerter Daten „in die Cloud“ verfügen.

5 Vgl. auch im Folgenden: Deussen/Strick/Peters 2010, S. 15f.

- Bei einer **privaten Cloud**, bei der sich Anbieter und Nutzer in derselben Organisation befinden, sind Aspekte hinsichtlich Datensicherheit und -schutz weniger zu beachten. Ob mit einer privaten Cloud die Potenziale der Cloud-Technologien hinsichtlich Ressourceneffizienz und -ersparnis gehoben werden können, ist genau zu prüfen.

- Bei einer **Community-Cloud** schließen sich mehrere Anbieter zusammen, um für einen bestimmten Kundenkreis unter Berücksichtigung von dessen spezifischen Anforderungen Leistungen anzubieten. Bezogen auf den öffentlichen Sektor könnte dies bedeuten, dass sich verschiedene öffentliche IT-Dienstleister zusammenschließen und Cloud-Leistungen über alle Servicemodelle bereitstellen. Vorteil für die öffentlichen Kunden ist, dass sie standardisierte Services, wie Fachverfahren, Middleware und Speicher, aus einer öffentlichen Sektor spezifischen Cloud beziehen, die den Datenschutz- und Geheimnisschutzanforderungen entsprechen, ohne Ressourcen für den operativen IT-Betrieb vorhalten zu müssen.

- Bei **Hybrid-Clouds** als Kombinationsmodell werden private bzw. Community-Cloud mit öffentlichen Clouds bei Bedarf verbunden, z.B. um Lastspitzen und Ausfallzeiten abzufangen. Das Kombinationsmodell ist v.a. auch datenschutzrechtlich besonders problematisch, da das Beziehungsgeflecht zwischen Auftraggebern und Anbietern sehr komplex werden kann.

Folgende Grafik fasst die Eigenschaften der Cloud noch einmal zusammen:

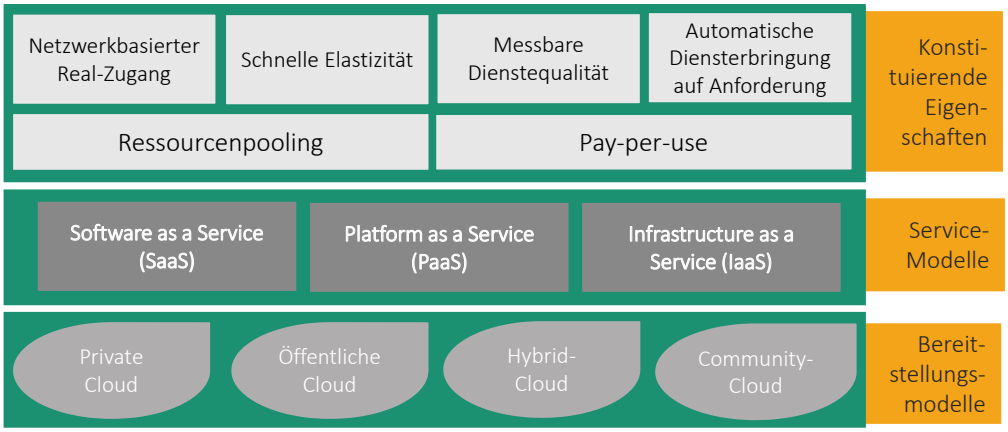

Abbildung 1: Cloud im Überblick (eigene Darstellung, in Anlehnung an CSA 2017, Deussen/Peters/Strick 2010)

2.2 Begriffsabgrenzung: Privacy, Informationssicherheit und Datenschutz

Das kommunale IT-Umfeld ist von hohen Anforderungen an Datenschutz und IT-Sicherheit geprägt, so verarbeiteten nach einer Untersuchung von Dataport 2014 über 90 Prozent der Kundenverfahren personenbezogene Daten.[6] Dabei fällt in der Diskussion auf, dass eine begriffliche Unschärfe besteht, wenn es darum geht, Privacy, Informationssicherheit und Datenschutz voneinander abzugrenzen. Folgende Tabelle gibt einen Überblick über das Schutzziel, den Schutzbereich, mögliche Gefahren und den Fokus der Konzepte.

6 vgl. Meints 2014.

	Privacy („Privatsphäre“)	Datenschutz	Informations-sicherheit
Schutzziel	• Grundrecht • Schutz des Individuums vor dem Staat bzw. vor Dritten durch den Staat • Bezieht sich auf persönliche Sphäre, wie persönliche Kommunikation und „persönliches Territorium“	• Verarbeitung personenbezogener Daten • Individuen entscheiden selbst über Verwendung der Daten	• Vorkehrungen für die Sicherheit von Hard- und Software • Missbrauch von Daten verhindern
Geschützt werden	Natürliche Personen	Natürliche Personen	Hardware, Software, Daten, Dokumente
Gefahr durch	Physische und anderen Eingriff	Verletzung der Persönlichkeitsrechte	Verlust, Zerstörung und Missbrauch durch Unbefugte
Fokus	Einzelne Person	Einzelne Person	Organisationen

Tabelle 1: Abgrenzung Privacy, Datenschutz, Informationssicherheit

Privacy und Datenschutz weisen konzeptionell-inhaltlich große Überschneidungen auf, sind aber nicht synonym. Der Begriff bzw. das dahinterstehende Konzept „Privacy“, wie es in der Diskussion um Datenschutz etc. verwendet wird, kommt aus dem angloamerikanischen Kultur- und Rechtsraum und wird dort als „Right to be let alone“ verstanden.[7] Vor diesem Hintergrund wird Datenschutz als ein Teil des Schutzes der Privatsphäre verstanden.[8] Eine universell und weltweit geltende Definition gibt es nicht. Daher entstehen die Unschärfen bei der Übersetzung und der Verwendung.

Derzeit wird auf EU-Ebene die so genannte ePrivacy-Verordnung (offiziell: Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications) erarbeitet, welche die Privatsphäre von Bürgern online stärken und den Datenschutz intensiver regulieren soll. Die ePrivacy-Verordnung soll die veraltete ePrivacy-Richtlinie ersetzen und die Datenschutz-Grundverordnung flankieren.

7 Glancy 1979, S. 3.

8 vgl. die Zusammenfassung unter: https://www.heise.de/tp/features/Vom-Menschenrecht-in-Ruhe-gelassen-zu-werden-3451029.html (letzter Zugriff, 29.03.2019)

2.3 Herausforderung: Umsetzung in der öffentlichen Verwaltung

Akteure in einer Cloud sind grundsätzlich cloud user/customer (Nutzer/Kunden[9]) und cloud service provider (CSP, Cloud-Dienste-Anbieter[10]). Ein Nutzer/Kunde bezieht Leistungen aus der „Cloud", die ein CSP anbietet und liefert. Aus Sicht von Kommunen als Nutzer gibt es folgende „Ketten", wie Leistungen aus der Cloud bezogen werden können: Jede dieser „Cloud-Ketten" hat Vor- und Nachteile.[11] Im ersten Model bezieht eine Kommune direkt Cloud-Services von einem kommerziellen Anbieter, wählt diesen also selbständig nach bestimmten Kriterien aus und schließt einen Vertrag über die Nutzung ab. Dieses Nutzungsmodell werden wahrscheinlich eher größere Kommunen wählen, wenn der Anbieter Anforderungen der IT-Sicherheit nachweisen kann.

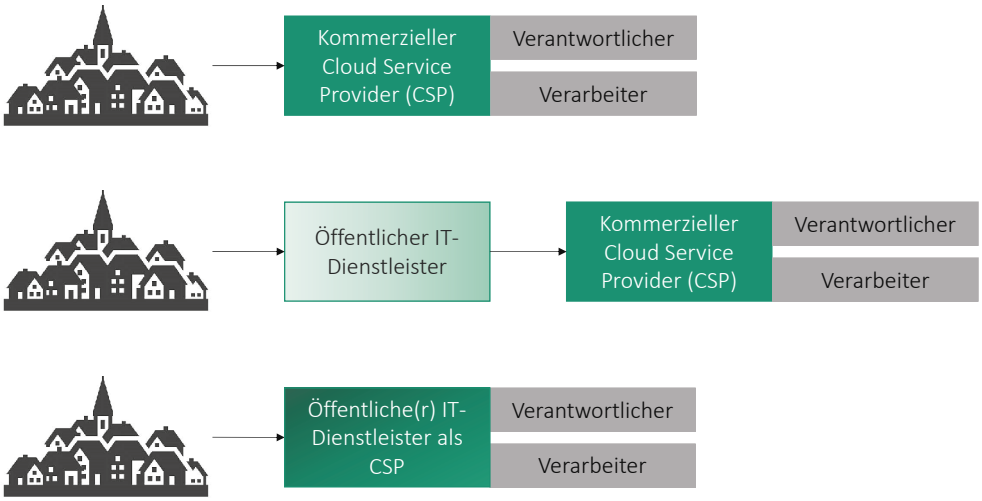

Abbildung 2: Nutzungsmodelle von Cloud im kommunalen Bereich (Quelle: KGSt 2018, S. 20)

Beim zweiten Modell agiert ein öffentlicher IT-Dienstleister als „Mittler" zwischen einer Kommune und einem oder mehreren öffentlichen oder privaten CSPs und beraten die Kommune in Bezug darauf, ob eine Lösung oder ein Anbieter geeignet sind. Genauso gut können sie als Mittler selbst Leistungen von öffentlichen/privaten CSPs und stellen sie Kommunen zur Verfügung. In beiden Fällen stellen sie mit ihrer Expertise sicher, dass die Services den Anforderungen an Sicherheit und Datenschutz entsprechen.

Im dritten Modell treten ein oder mehrere öffentliche IT-Dienstleister gemeinsam als Cloud-Dienstleister auf, bilden eine Community Cloud und bieten darüber Leistungen für Kommunen an.

Um Kommunen und öffentliche Verwaltungen auf dem Weg in die Cloud zu unterstützen, hat das Fraunhofer Institut FOKUS mit dem Papier „Fahrplan in die Cloud" bereits im Jahr 2014 ein Stufenmodell mit fünf wesentlichen Schritte entwickelt.[12] Bei Auslagerung/Verlagerung auf

9 Cloud-Kunde („Herr der Daten") ist Verantwortlicher gemäß Art. 28 DSGVO, Regelfall: Cloud Computing = Auftragsverarbeitung gemäß Art. 28 DSGVO

10 CSP kann folgende Rollen haben: Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter, Unterauftragsverarbeiter gemäß DSGVO. Diese Rollen können bei jeder angebotenen Leistung variieren.

11 Modelle in Anlehnung an KGSt 2018, S. 20.

12 Die fünf wesentlichen Schritte sind: (1) Bedarfsanalyse, (2) Risikoanalyse, (3) Wahl des Ausschreibungsverfahrens, (4) Auftragsvergabe, (5) Migration), weitere Informationen siehe Deussen et al. 2014, S. 21ff.

Lieferanten (CSP) werden die verwendeten IT-Ressourcen oft von Unterauftragnehmern betrieben, deren Provenienz dem Kunden nicht transparent ist. Solche Probleme dürfen bei der Risikoanalyse nicht unbeachtet bleiben. Wichtig zu betonen ist, dass bei Auslagerung/Verlagerung auf Lieferanten die auftraggebende Organisation die Verantwortung für die Aufgabenerfüllung als Ganzes behält. Schadenfälle schlagen auf jeden Fall auf die Organisation durch (geringste Schadensstufe „nur Imageschaden"). Es stellt sich also zunächst die Frage, ob man als auftraggebende Organisation überhaupt Unterauftragnehmer zulässt. Falls ja, könnte man dem Lieferanten aufgeben, seine Unterauftragnehmer zu benennen und sicherzustellen, dass alle vertraglichen Vorgaben durchgereicht werden, d.h. die gesamte Kette muss über verbindliche Vorgaben verfügen, die im Einklang mit der Lieferantenvereinbarung stehen. Diesbezüglich sollte der primäre Auftragnehmer nachweispflichtig sein. Besteht die Tätigkeit in der Lieferung von IT-Produkten, so kann es erforderlich werden, einen Herkunftsnachweis zu bekommen bzw. entsprechende Einschränkungen vorzugeben.

In der Kurzstudie konzentrieren wir uns auf den Aspekt der Sicherheit und Konformität mit geltenden datenschutzrechtlichen Regelungen sowie Anforderungen an die IT-Sicherheit. Bei der Entscheidung für oder gegen eine Cloud-Lösung ist insbesondere der Schutzbedarf der im Rahmen der bereitgestellten Services verarbeiteten Daten zu berücksichtigen[13]. Grundsätzlich gilt: „es gibt keine absolute Sicherheit" und „erhöhte Sicherheit verursacht erhöhte Kosten". Doch nicht alle Daten und Prozesse haben ein gleichermaßen hohes Schutzniveau. Der Betrieb einer öffentlich zugänglichen Webseite, die allgemeine Bürgerinformationen zur Verfügung stellt, wird anders zu bewerten sein als die Speicherung von personenbezogenen Daten. Je höher der Schutzbedarf der zu verarbeitenden Daten ist, desto höher ist der Bedarf an direkter Kontrolle der Verarbeitung durch den Dateneigentümer.

Mit Ausnahme der privaten Cloud sind für alle Bereitstellungsmodelle bezogen auf die Sicherheit und Steuerung u.a. folgende Aspekte zu berücksichtigen und in eine Risikoabwägung einzubeziehen, um zu entscheiden, ob die „Cloud" geeignet ist. Die Steuerung erfolgt über Verträge, z.B. Service Level Agreements. Zudem ist das IT-Sourcing so auszurichten, dass kein Lock-In-Effekt entsteht, damit immer Zugriff auf IT-Services und Daten besteht, selbst wenn ein Anbieter bestimmte Services nicht mehr anbietet. Hinsichtlich des Zugriffs auf Leistungen und Services sollte zu jeder Zeit ein sicherer Zugang gewährleistet sein und Daten verschlüsselt sein, so dass ein Anbieter niemals auf Daten eines Kunden zugreifen kann. Gleichzeitig müssen die Ressourcen eines Anbieters so ausgelegt sein, dass ein schnelles Up-Scaling möglich ist, ohne dass vereinbarte Sicherheitsmechanismen verletzt werden. Aufgrund der Spezifität der Cloud-Technologien können Kunden eines Cloud Service Providers (CSP) (Cloud-DiensteAnbieter) die Sicherheitsmechanismen kaum mehr „durch eigene Anschauung" überprüfen. Vielmehr sind neue Formen und Mechanismen erforderlich, wie Zertifizierungen und Qualitätssiegel.

13 vgl. im Folgenden Arbeitsgemeinschaft der Leiter der Landesrechenzentren 2014, S. 7.

3 AUSGEWÄHLTE STANDARDS FÜR SICHERHEIT IM CLOUD-KONTEXT

Die Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) weist darauf hin, dass Cloud-Anbieter entsprechende Zertifizierungen vorweisen sollten, welche eine angemessene Informationssicherheit bestätigen, die dem Niveau des Vertragsgegenstands gerecht wird[14]. Daher werden im weiteren Verlauf wichtige Prüfstandards in Bezug auf Cloud-Sicherheit und Datenschutz dargestellt. Die Auswahl erfolgte nach Verbreitungsgrad und u.a. Berücksichtigung bei Aufsichts- bzw. Sicherheitsbehörden, wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Ergebnis der Anwendung dieser Prüfstandards sind Nachweise verschiedener Arten, die vorab näher definiert werden.

3.1 Begriffsklärung: Testat, Zertifizierung, Selbsteinschätzung

Auch wenn umgangssprachlich häufig von Zertifizierung und Prüfsiegeln gesprochen wird, bestehen Unterschiede zwischen den Nachweisarten. Eine saubere Abgrenzung ist wichtig, da die Prüfergebnisse je nach Art des Reports eine unterschiedliche Aussagekraft aufweisen. Im Folgenden werden die wichtigsten drei Nachweistypen kurz beschrieben.

Testat: Ein Testat als Nachweis wird von Wirtschaftsprüfern vergeben. Dabei bestätigt ein Wirtschaftsprüfer, dass Jahresabschluss und Buchführung den gesetzlichen Vorschriften entsprechen und dass der Lagebericht keine falschen Vorstellungen von der Lage der Unternehmung erweckt.[15] Da sich die Überprüfungen von Wirtschaftsprüfern auch auf digitale Systeme, z.B. für die so genannten internen Kontrollsysteme (IKS), erstrecken, wurde diese Form des Konformitätsnachweises auch für Cloud-Systeme als geeignet ausgewiesen.

Zertifizierung: Eine Zertifizierung ist eine Sonderform der Konformitätsbewertung.[16] Der Begriff Konformität beschreibt dabei eine Überprüfung der Erfüllung definierter Anforderungen, die an ein Produkt, ein System, einen Prozess oder auch an Personen gestellt werden. Eine Konformitätsbewertung kann beispielsweise durch eine Herstellererklärung oder eine unabhängige Zertifizierungsstelle erfolgen. Das Deutsche Institut für Normung DIN definiert Zertifizierung wie folgt: „Maßnahme durch einen unparteiischen Dritten, die aufzeigt, dass ein angemessenes Vertrauen besteht, dass ein ordnungsgemäß bezeichnetes Erzeugnis, Verfahren oder eine ordnungsgemäß bezeichnete Dienstleistung in Übereinstimmung mit einer bestimmten Norm oder einem bestimmten anderen normativen Dokument ist.“[17] Damit ist die Herstellererklärung nicht ausreichend für einen Nachweis der Konformität.

14 vgl. KGSt 2018, S. 15.

15 vgl. Beeck, o.J.

16 vgl. DIN/ISO o.J.

17 vgl. DIN KonRat 2013.

Selbsteinschätzung: Während die beiden ersten Formen jeweils den Einbezug eines unabhängigen Dritten erfordern, um die Konformität mit Anforderungen nachweisen, ist auch eine Selbsteinschätzung zunehmend verbreitet, die sich jedoch von der „einfachen" Herstellererklärung unterscheidet. Hierbei überprüfen die Unternehmen selbst anhand eines Prüfkatalogs, der z.B. von einer Branchenorganisation entwickelt wurde, ob sie konform mit anerkannten Prüfkriterien sind. Die Selbstbewertungen werden dann von den Branchenorganisationen veröffentlicht und können von jedem Interessierten eingesehen werden.[18] Zum Nachweis der Konformität bzw. der veröffentlichten Selbstbewertung werden häufig Siegel oder andere Kennzeichnungen wie Trust Marks vergeben.

3.2 IT-Sicherheitsbezogene Konformität

Insgesamt mangelt es in der Branche nicht an Sicherheitsempfehlungen, Standards und Zertifikaten[19]. Die Standards weisen auch trotz unterschiedlicher Blickwinkel auf die Cloud-Sicherheit eine hohe inhaltliche Übereinstimmung auf. Eine allgemein anerkannte Basis-Linie für Sicherheit im Cloud Computing existiert aber noch nicht. Die Gängigsten werden im Folgenden näher beschrieben.

3.2.1 Informationssicherheitsstandard ISO 27001

Bei der ISO 27001 handelt es sich um die international führende Norm für Informationssicherheits-Managementsysteme (ISMS). Sie bietet Organisationen aller Art und Größe klare Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung ihrer Informationssicherheit. Cloud-Dienste fallen unter die so genannten Lieferantenbeziehungen, die in Control A 15 geregelt sind.[20] Gemäß der Norm behält die auftraggebende Organisation bei Auslagerung/Verlagerung auf Lieferanten bzw. Unterauftragnehmern, d.h. auf CSP, die Verantwortung für die Aufgabenerfüllung als Ganzes. Schadenfälle schlagen auf jeden Fall auf die Organisation durch (geringste Schadensstufe „nur Imageschaden").

Zwar existiert für Cloud Services die Norm ISO 27018, die jedoch eine separate Zertifizierung der CSP nach ISO nicht vorsieht[21]. Eine Zertifizierung eines Unternehmens wird auf der Basis von ISO/IEC 27001 in Umsetzung der ISO/IEC 27018 vorgenommen. Daher nutzen viele Cloud Anbieter die umfassende Zertifizierung nach ISO 27001. Unternehmen erhalten als Nachweis der Erfüllung aller Anforderungen ein Zertifikat von akkreditierten Institutionen (bspw. TÜV).

3.2.2 C5 – Cloud Computing Compliance Controls Catalogue des BSI

Der Anforderungskatalog (C5) zur Beurteilung der Informationssicherheit von Cloud-Diensten bestimmt eine Basislinie für Cloud-Sicherheit. D.h. es wird festgelegt, welche Anforderungen die Cloud-Anbieter erfüllen müssen bzw. auf welche Anforderungen der Cloud-Anbieter mindestens verpflichtet werden sollte.

Ziel ist es, für potenzielle Cloud-Kunden Transparenz zu ermöglichen, ob gesetzliche Vorschriften (wie z.B. Datenschutz), die eigenen Richtlinien oder auch die Gefährdungslage bezüglich Wirtschaftsspionage die Nutzung des jeweiligen

18 beispielhaft siehe Microsoft CSA STAR Selbstbewertung: https://www.microsoft.com/de-de/TrustCenter/Compliance/csa-self-assessment (letzter Zugriff, 15.03.2019)

19 Eine umfassende Übersicht bietet Trusted Cloud 2016.

20 Kersten et al. 2016, S. 183ff.

21 vgl. ISO/IEC o.J.

Cloud-Dienstes als geeignet erscheinen lassen. Der Anforderungskatalog[22] richtet sich in erster Linie an professionelle Cloud-Diensteanbieter, deren Prüfer und Kunden.

Der Katalog ist in 17 thematische Bereiche (z.B. Organisation der Informationssicherheit, Physische Sicherheit) unterteilt. Dabei bedient sich das BSI bei anerkannten Sicherheitsstandards wie ISO/IEC 27001, der Cloud Controls Matrix der Cloud Security Alliance sowie Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und übernimmt ggf. deren Anforderungen. Diese wurden, wenn als notwendig erachtet, weiter konkretisiert. Existierten keine Anforderungen aus anderen Standards, wurden neue erstellt. Neben diesen Basis-Anforderungen enthält der Katalog auch weitergehende Anforderungen, die entweder besonders die Vertraulichkeit oder die Verfügbarkeit oder beides zugleich adressieren. Zusätzlich wurde der Anforderungskatalog auf die oben genannten Standards referenziert, um einen schnellen Überblick darüber zu geben, wo die Anforderungen des Kataloges in anderen Standards zu finden sind und ob die Anforderungen über die anderen Standards hinaus gehen oder nicht. Ein Unterschied zu anderen Sicherheitsstandards sind die sogenannten Umfeldparameter. Sie geben Auskunft über Datenlokation, Diensterbringung, Gerichtsstandort, Zertifizierungen und Ermittlungs- und Offenbarungspflichten gegenüber staatlichen Stellen und enthalten eine Systembeschreibung. Die so geschaffene Transparenz erlaubt es potenziellen Cloud-Kunden zu entscheiden, ob gesetzliche Vorschriften (wie z.B. Datenschutz), die eigenen Richtlinien oder auch die Gefährdungslage bezüglich Wirtschaftsspionage die Nutzung des jeweiligen Cloud-Dienstes als geeignet erscheinen lassen.

Der Anforderungskatalog (C5) wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und kostenlos bereitgestellt.

Der Nachweis, dass ein Cloud-Anbieter die Anforderungen des Katalogs einhält und die Aussagen zur Transparenz korrekt sind, wird durch einen so genannten SOC 2-Bericht erbracht. Dieser basiert auf dem international anerkannten Testierungsregime der ISAE 3000, das von Wirtschaftsprüfern verwendet wird.[23] Damit erhält der überprüfte CSP ein Testat über eine anerkannte Wirtschaftsprüfungsgesellschaft, was in der Regel mit erheblichem finanziellen Aufwand für das zu prüfende Unternehmen einhergeht. Insbesondere kleinere und mittlere Unternehmen scheuen den Aufwand[24] und es gibt kein öffentliches Register, welche Unternehmen ein solches Testat haben. Das BSI informiert lediglich per Pressemitteilung, wem ein C5-Testat erteilt wurde.

22 BSI 2017.

23 In einem SOC-Report geht es um interne Kontrollen in Bezug auf Sicherheit, Verfügbarkeit, Integrität und Vertraulichkeit (Datenschutz) der verarbeiteten Daten und Prozesse. Es findet eine Beurteilung und Berichterstattung zum Kontrolldesign im Hinblick auf die Angemessenheit der Definition der Ziele und der zugehörigen Kontrollen zu einem bestimmten Zeitpunkt statt (Typ I). Eine Prüfung nach Typ II (SOC 2) prüft darüber hinaus auch noch die Wirksamkeit der eingerichteten Kontrollen und beinhaltet die Testszenarien und das Ergebnis dieser Tests im Bericht – in der Regel für das zurückliegende Jahr. ISAE ist ein international anerkannter Wirtschaftsprüferstandard, der von den nationalen Organisationen übernommen wird.

24 Gemäß der Umsetzungshinweise des BSI zur Nutzung externer Cloud-Dienste kann der Nachweis der C5-Konformität durch geprüfte Partner beigebracht werden. Dies ermöglicht die Teilnahme an Ausschreibungen der öffentlichen Verwaltung, in denen ausdrücklich ein C5-Testat gefordert wird, ohne ein solches Testat zu haben.

3.2.3 Trusted Cloud Kriterienkatalog

Der Trusted-Cloud-Kriterienkatalog[25] für Cloud Services definiert die Mindestanforderungen, die ein Cloud Service zur Erlangung des Trusted-Cloud-Labels und damit für die Listung auf dem Trusted-Cloud-Portal erfüllen muss. Der Katalog ist speziell vor dem Hintergrund der Bedarfe von Anwendern im Hinblick auf Transparenz, Sicherheit, Qualität und Rechtskonformität von Cloud-Diensten entwickelt worden.

Der Kriterienkatalog ist öffentlich zugänglich und gliedert sich in die Abschnitte Anbieter, Service, Subunternehmer/Rechenzentren, Zertifikate, Vertrag, Sicherheit, Datenschutz/Compliance, operative Prozesse, Interoperabilität/Portabilität und Architektur. Entspricht ein Anbieter den Anforderungen erhält er das Label „Trusted Cloud für vertrauenswürdige Cloud Services".

Träger des Labels ist der Verein „Kompetenznetzwerk Trusted Cloud e.V.", der aus dem gleichnamigen Technologieprogramm des Bundesministeriums für Wirtschaft und Energie (BMWi) hervorgegangen ist[26]. Der Verein wird weiterhin gefördert durch das BMWi. Über die Vergabe des Labels und die Listung von Cloud Services entscheidet der unabhängig besetzte Trusted-Cloud-Beirat. Derzeit sind zehn Dienstleister und 16 Cloud Services gelistet. Mit zunehmender Digitalisierung kommen auch Anbieter von Beratungsdienstleistungen im Cloud-Umfeld, wie Systemhäuser, stärker in den Fokus. Um auch hier Transparenz für die Anwender herzustellen, wird ein Directory von Dienstleistern bereitgestellt[27]. Mit den Zertifizierungsanbietern Zeker-OnLine (Niederlande) und Label Cloud (Frankreich) besteht eine Zusammenarbeit.[28]

3.2.4 CCM – Cloud Controls Matrix der Cloud Security Alliance

Ziel der Cloud Controls Matrix (CCM) ist es, grundlegende Sicherheitsprinzipien bereitzustellen, die Cloud-Anbieter leiten und potenzielle Cloud-Kunden bei der Evaluierung von Sicherheitsmaßnahmen von Cloud-Anbietern unterstützen.

Als Rahmen bietet die CCM die erforderliche Struktur, Detaillierung und Klarheit in Bezug auf Informationssicherheit, die auf die Cloud-Branche zugeschnitten ist. Die CCM gliedert sich in 16 sicherheitsrelevante Bereiche wie Anwendungssicherheit, Identitäts- und Zugriffsmanagement oder Betrieb von Rechenzentren. Auch mehrere Branchenstandards, Regulierungsvorschriften und andere rechtliche Rahmen[29] werden berücksichtigt, die Unternehmen beachten müssen.[30] Die CCM stärkt bestehende Informationssicherheitskontrollumgebungen, indem die Anforderungen an die Kontrolle der Geschäftsinformationssicherheit betont, konsistente Sicherheitsbedrohungen und -schwachstellen in der Cloud reduziert und identifiziert, standardisiertes Sicherheits- und operatives Risikomanagement bietet und darauf abzielt, die in der Cloud implementierten Sicherheitserwartungen, Cloud-Taxonomie und -Terminologie sowie Sicherheitsmaßnahmen zu harmonisieren. Die CCM ist Teil einer Sammlung von Standards für

25 siehe Trusted Cloud 2016a.

26 vgl. Trusted Cloud, o.J.

27 vgl. Trusted Cloud 2017.

28 vgl. Dosch/Karlstetter 2017.

29 etwa ISO 27001/27002, PCI DSS (Standard u.a. für Kreditkartendaten), HIPAA (U.S. Health Insurance Portability and Accountability Act, d.h. für Gesundheitsdaten) oder COBIT (international anerkannter Rahmen zur IT-Governance).

30 CSA 2013.

Cloud-Computing mit der Bezeichnung GRC-Stack[31]. Zu dessen Werkzeugen zählen CloudAudit, das Cloud Trust Protocol und der Consensus Assessments Initiative Questionnaire (CAIQ), ein Katalog von Fragen zum Thema Sicherheit, die Kunden Cloud-Providern stellen können. Die CCM steht kostenlos zum Download zur Verfügung.[32]

Die CCM wurde von der Cloud Security Alliance (CSA) entwickelt. Die Cloud Security Alliance (CSA) wurde in den USA von Cloud-Anbietern gegründet, mit dem Ziel, Expertise für eine sichere Nutzung von Technologien zu bündeln. Mitglieder sind u.a. AWS, Microsoft und Google. Seit Herbst 2018 gibt es eine Europazentrale in Berlin.

Als Nachweis, dass die Anforderungen aus der CCM erfüllt sind, gibt es drei Stufen. Die Stufe 1 ist die Selbsteinschätzung und ist kostenlos für die Unternehmen. Das Ergebnis der Selbsteinschätzung wird dann im Internet im so genannten Security, Trust & Assurance Registry veröffentlicht, das CSA zusammen mit British Standards Institution (BSI) 2013 aufgesetzt hat. Stufe 2 bedeutet die Konformitätsbewertung durch eine dritte Partei. Hierfür wird die Prüfung, ob Unternehmen die CCM-Anforderungen erfüllen, entweder in die Zertifizierung nach ISO/IEC 27001 integriert oder in die „Wirtschaftsprüferwelt“ mit SOC 2 etc. Stufe 3 bedeutet ein kontinuierliches Monitoring und umfasst alle Maßnahmen der vorherigen Stufen.

3.2.5 EuroCloud StarAudit

Zweck des StarAudit-Kriterienkatalogs ist es, eine nachvollziehbare Qualitätsbewertung von Cloud-Diensten zu ermöglichen und so das Vertrauen von Kunden und Nutzern von Cloud-Diensten zu stärken.

StarAudit bewertet Cloud-Dienste anhand eines klar definierten Kriterienkatalogs und evaluiert sämtliche Teilnehmer an der spezifischen Lieferkette eines Cloud-Dienstes, so dass keine separaten, i.d.R. kostenintensiven, Audits aller an der Lieferkette beteiligten Teilnehmer erforderlich sind. Die Dienste werden nach ihrem Reife- und Compliancegrad verglichen und transparent gemacht. Im Ergebnis erhält ein Unternehmen eine Zertifizierung.

EuroCloud ist eine europäische Non-Profit-Vereinigung von IT-Unternehmen, Anwaltsfirmen und Wirtschaftsprüfungsorganisationen mit nationalen Verbänden. Die nationalen Verbände, wie die EuroCloud Deutschland_eco e.V.[33], überwachen die Zertifizierung. Das Zertifikat gilt dann für den gesamten europäischen Verband.

3.3 Datenschutzbezogene Konformität

Mit Inkrafttreten der DSGVO sind die bisher in Deutschland existierenden Schemata/Kriterienkataloge zum Nachweis der Datenschutzkonformität nicht mehr anwendbar, da sie auf dem alten BDSG basieren, so dass auch die entsprechenden Siegel und Zertifikate nicht mehr vergeben werden dürfen. Auch bei der DSGVO bleibt der Eigentümer der Daten, d.h. der Cloud-Kunde, Verantwortlicher (Art. 28 DSGVO) und muss daher sicherstellen, dass dem Schutzbedarf angemessene Schutzmechanismen bereitgestellt werden. Gleichzeitig wurde eine gemeinsame Verantwortung für jeden an der „Lieferkette“ Beteiligten geschaffen (Art. 26 DSGVO), wofür entsprechende Strukturen, aber auch vertragliche Vereinbarungen erforderlich sind. Dabei gilt, je höher der potenzielle Schaden durch einen Sicherheitsvorfall, desto genauer

31 GRC Stack = Governance, Risk Management and Compliance Stack soll Cloudkunden dabei unterstützen, zu bewerten, wie Cloud Service-Anbieter (CSP) den branchenüblichen Best Practices und Standards folgen und Complianceanforderungen erfüllen.

32 CSA o.J.

33 EuroCloud o.J.; StarAudit o.J.

müssen in einem Vertrag die Haftung und die geschuldete Sicherheitsleistung beschrieben sein.

Als Nachweis der Compliance ist in der DSGVO eine datenschutzspezifische Zertifizierung vorgesehen (Art. 42 DSGVO) Zertifikate dürfen gemäß Art. 42 Abs. 5 DSGVO nur von den Aufsichtsbehörden oder akkreditierten Zertifizierungsstellen ausgestellt werden. Derzeit liegen jedoch die Kriterien für die Zertifizierung, um den Anforderungen an Compliance zu genügen, noch nicht vor. Die Datenschutzaufsichtsbehörden arbeiten daran, diese festzulegen.[34] Als weitere Form der Konformitätsfeststellung dienen sogenannte genehmigte Verhaltensregeln (Code of Conducts) gemäß Art. 40 DSGVO, von denen zwei ausgewählte im Folgenden kurz beschrieben werden.

3.3.1 TCDP und Auditor der Stiftung Datenschutz

Das Trusted Cloud-Datenschutzprofil („TCDP") ist ein deutscher Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten. Durch Inkrafttreten der DSGVO wurde es notwendig, den Standard entsprechend den Anforderungen der DSGVO anzupassen. Er wird z.T. als DSGVO TCDP bezeichnet und ist noch nicht veröffentlicht.

Das Schema beschreibt datenschutzrechtliche Anforderungen der Cloud-Anbieter, nicht der Cloud-Nutzer. Adressiert werden vorrangig die Voraussetzungen der Auftragsdatenverarbeitung, die in der DSGVO und im neuen Bundesdatenschutzgesetz (BDSG neu) festgelegt sind. Geprüft wird zunächst der Inhalt der Verträge zwischen dem Betreiber des Cloud-Dienstes und dem Cloud-Nutzer. Den Schwerpunkt des Zertifizierungsprozesses bildet die Prüfung der technischen und organisatorischen Maßnahmen beim Cloud-Anbieter. Dabei wird etwa geprüft, ob die IT-Systeme des Cloud-Anbieters ausreichenden Schutz vor unberechtigtem Zugriff bieten und ob die Integrität und Wiederherstellbarkeit von Daten etwa bei Stromausfällen und Naturkatastrophen sichergestellt sind. Das Schema verweist häufig auf ISO-Standards. D.h. es verweisen fast alle TCDP-Nummern auf controls von ISO/IEC 27002, ISO/IEC 27017 oder ISO/IEC 27018.[35] Anders als die flexiblen ISO-Standards sind jedoch alle Verweise in den Anforderungen und den Umsetzungsempfehlungen des TCDP als zwingende Voraussetzungen zu betrachten.

Der TCDP wurde von der Bundesstiftung Datenschutz entwickelt und mit Mitteln des BMWI gefördert und steht kostenlos zur freien Verfügung[36]. Der Standard für die Datenschutz-Zertifizierung von Cloud-Diensten nach der DSGVO TCDP wird im Rahmen des derzeit laufenden Forschungsprojekt AUDITOR[37] bis Oktober 2019 entwickelt. Ziel des Forschungsprojekts ist die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten.

(DSGVO) TCDP erfordert eine Prüfung und Bewertung der datenschutzrechtlichen Anforderungen durch unabhängige und zertifizierte Prüf- und Zertifizierungsstellen. Wie üblich erhebt dabei die Prüfstelle die zur Zertifizierung notwendigen Informationen selbst beim Anbieter oder anhand von dessen Dokumentation. Diese Informationen werden dann von der Zertifizierungsstelle ausgewertet. Sind die

34 Müller/Strick/Köhl 2018.

35 Die ISO-Normen gehören zur „27000-Familie" und spezifizieren einzelne Systeme im Bereich IT. So befasst sich bspw. die ISO/IEC 27018 mit Cloud-Technologien.

36 Trusted Cloud 2016b; https://tcdp.de/index.php/ueber-uns.

37 Auditor o.J.

Anforderungen erfüllt, erhält der Anbieter für den geprüften Cloud-Dienst das TCDP-Zertifikat, um dies auch gegenüber Dritten nachzuweisen. Eine Anerkennung eines DSGVO TCDP-Zertifikats nach Art. 42 Abs. 5 DSGVO ist angestrebt.

3.3.2 DSGVO Verhaltenskodex der Cloud Security Alliance

Der CSA-Verhaltenskodex (Code of Conduct for GDPR Compliance) für die Einhaltung der DSGVO gibt Cloud-Serviceprovidern (CSP), Cloud-Kunden und potenziellen Kunden Leitlinien an die Hand, damit sie den Verpflichtungen in Zusammenhang mit der europäischen Datenschutz-Grundverordnung (DSGVO) nachkommen können.

Der CSA-Verhaltenskodex für die Einhaltung der DSGVO spezifiziert die Anwendung der DSGVO in der Cloud-Umgebung, vor allem in Bezug auf die folgenden Kategorien:

- Faire und transparente Verarbeitung persönlicher Daten;
- Daten, die der Öffentlichkeit und den Datensubjekten zur Verfügung gestellt werden (gemäß Definition in Artikel 4 (1) der DSGVO);
- Ausübung der Rechte von Datensubjekten;
- Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 der DSGVO sowie Maßnahmen zur Gewährleistung der Verarbeitungssicherheit gemäß Artikel 32 der DSGVO;
- Meldung von Verstößen gegen personenbezogene Daten an die Aufsichtsbehörden (im Sinne des Artikels 4 (21) der DSGVO) und Mitteilung solcher Verstöße gegen personenbezogene Daten an die Datensubjekte und Transfer von persönlichen Daten in Drittländer.

Darüber hinaus enthält der CSA-Verhaltenskodex für die Einhaltung der DSGVO Mechanismen, die es der in Artikel 41 Absatz 1 der DSGVO genannten Stelle ermöglichen, eine obligatorische Überwachung der Einhaltung durch die für die Anwendung Verantwortlichen oder Verarbeiter durchzuführen, unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden gemäß den Artikeln 55 oder 56 der DSGVO.

Der DSGVO Verhaltenskodex steht online zur freien Verfügung.[38] Die CSA hat zwei Ansätze zur Einhaltung ihres Verhaltenskodex definiert: Ein Self Assessment (derzeit verfügbar) und eine auditbasierte Zertifizierung durch Dritte (derzeit in Bearbeitung). Bei Erfüllung aller Anforderungen kann die Konformität mit einer so genannten Trustmark bestätigt werden. Die Ergebnisse werden in der Public Registry der CSA veröffentlicht.

3.4 Zusammenfassende Betrachtung

Mit Ausnahme des C5 Standards des BSI wurden alle Standards und Prüfschemata aus der Industrie heraus entwickelt. Dabei hat der ISO-Standard, der unter Beteiligung von Marktteilnehmern entwickelt wurde, in der Wahrnehmung aufgrund des Normungsprozesses bzw. des dahinterliegenden Abstimmungsmechanismus gesetzesähnlichen Charakter. Die Standards beziehen sich in der Regel auf die gleichen Prüfbereiche; C5 bezieht sich ausdrücklich auf andere Industrie-Standards und hat diese einbezogen. Eine Verbindlichkeit dieser Branchenstandards und damit das Vertrauen in diese wird über eine „Prüf-/Zertifizierungskette“ erreicht, d.h. die Einbeziehung Dritter in

38 siehe https://gdpr.cloudsecurityalliance.org/resource/csa-code-of-conduct-for-gdpr-compliance/ (letzter Zugriff 15.03.2019)

Form einer Zertifizierung oder Testierung. Dabei werden Dritte selbst über Standards und Normen akkreditiert, um zertifizieren zu können. Zu betonen ist, auch mit Standards kann de facto keine absolute Sicherheit erreicht werden. Grundsätzlich werden Standards geschaffen, um Vertrauen für Marktteilnehmer herzustellen. Das bedeutet, die Abwägung für die öffentliche Verwaltung bleibt erhalten[39].

Folgende Tabelle stellt die wesentlichen Informationen der beschriebenen Standards bzw. Verhaltensregeln noch einmal zusammenfassend dar.

Tabelle 3: kriterienbasierte Übersicht der Standards und Verhaltensregeln

Standard	Akteur	Nachweisart	„Prüfstelle“	Laufzeit/ Gültigkeit
ISO 27001	Internationale Normungsorganisationen	Zertifikat	Zertifizierte Prüfstelle	3 Jahre, jedoch jährliches Überwachungsaudit
C5	BSI	Testat	Wirtschaftsprüfer	2 Jahre
Trusted Cloud	Kompetenznetzwerk Trusted Cloud e.V.	Label und öffentliche Anbieterliste	Trusted-Cloud-Beirat	
CCM	Cloud Security Alliance	• Selbsteinschätzung mit öffentlicher Listung • Testat • Zertifikat	• selbst • Wirtschaftsprüfer • Zertifizierte Prüfstelle	s.o., bzw. entsprechend der Prüfsysteme
EuroCloud	EuroCloud	Zertifikat	Von EuroCloud akkreditierte Partner	2 Jahre
TCDP/ Auditor	Bundesstiftung Datenschutz	Zertifikat	Zertifizierungsstelle	n.a.
DSGVO Verhaltenskodex	Cloud Security Alliance	• Selbsteinschätzung • Zertifikat	• selbst • Zertifizierungsstelle	n.a.

39 Für den öffentlichen Sektor ist jedoch auch die Frage relevant, inwieweit ggf. Regierungen auf Daten zugreifen können (z.B. Cloud-Act), d.h. nicht nur Zertifikate/Testate sind ausschlaggebend, sondern auch rechtliche Regelungen.

Da Zertifizierungen auf Basis der oben beschriebenen Standards häufig nur nebeneinander stehen und zum Teil mit hohem Aufwand gleichzeitig aufrechterhalten werden, besteht für Cloud-Anwender die Herausforderung bei der Auswahl eines Anbieters, die Zertifizierungen und Testate der in der engeren Auswahl befindlichen Cloud-Anbieter belastbar miteinander zu vergleichen. Je nachdem, wie umfangreich die von den jeweiligen Cloud-Anbietern betriebenen Compliance-Programme sind, variieren auch die verfügbaren Zertifizierungen und Testate. Vor einer vergleichbaren Aufgabe stehen auch die Cloud-Anbieter: Da die Zertifizierungen und Testate nicht nur unterschiedliche Schwerpunkte setzen, sondern auch unterschiedliche Prüftiefen und -Verfahren erfordern sowie im internationalen Kontext oft ohne engeren Bezug nebeneinander stehen, lassen sie sich nur schwer miteinander vergleichen.

Daher müssen sich sowohl Anwender als auch Anbieter mit allen Prüfschemen vertraut machen, um diese in Beziehung zu einander setzen und abwägen zu können. Daher wird aktuell das Projekt „European Security Certification Framework“ (EU-SEC)[40] von der Europäischen Kommission gefördert. Dieses Projekt hat zum Ziel, einen innovativen Multi-Party-Recognition-Ansatz zu entwickeln, der den Compliance-Aufwand sowohl für Anbieter als auch Anwender reduziert. Es zielt darauf ab, einen europäischen Rahmen für Zertifizierungssysteme und Bewertungskonzepte zur Sicherung von Cloud-Infrastrukturen zu schaffen. In diesem Rahmen können bestehende nationale und internationale Zertifizierungen nebeneinander bestehen. Dennoch sollen die gemeinsamen Komponenten gegenseitig anerkannt und nur entsprechende Lücken durch Zertifizierungsmodule geschlossen werden.

40 EU SEC o.J.

4 NUTZUNG DER STANDARDS ZUR ANFORDERUNGSBESCHREIBUNG UND ÜBERPRÜFUNG BEI CLOUD-DIENSTEN IM ÖFFENTLICHEN BEREICH

Nachdem wesentliche Standards beschrieben wurden, stellt sich die Frage: Wie kann ein Cloud-Anwender erstens definieren, welche Anforderungen an einen Cloud-Dienst zu stellen sind und wie kann er vor allem fest- und sicherstellen, dass diese Anforderungen auch entsprechend erfüllt werden?

Als Orientierung für die Sicherheit bei Cloud-Dienstleistungen[41] hat das BSI Mindestanforderungen herausgegeben. Für das Informationssicherheitsmanagement gehören dazu:

- Definiertes Vorgehensmodell für alle IT-Prozesse (z.B. nach ITIL[42], COBIT)
- Implementation eines anerkannten Informationssicherheits-Managementsystems (z.B. nach ISO 27001)
- Nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud
- Nachweis einer ausreichenden Informationssicherheit
- Angemessene Organisationsstruktur für Informationssicherheit beim CSP (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)

Da in der Cloud i.d.R. personenbezogene Daten erhoben, verarbeitet oder genutzt werden, muss der Schutz personenbezogener Daten gemäß den datenschutzrechtlichen Bestimmungen, d.h. der DSGVO, dem BDSG neu und ggf. der Landesdatenschutzgesetze, gewährleistet sein. Meist handelt es sich im öffentlichen Bereich um eine Auftragsverarbeitung, bei der die datenschutzrechtliche Verantwortlichkeit uneingeschränkt beim Cloud-Nutzer als Auftraggeber verbleibt. Die Mindestanforderungen nach BSI lauten[43]

- Gewährleistung des Datenschutzes
- Datenschutzrichtlinien und -gesetze, denen der Cloud-Nutzer unterliegt, müssen eingehalten werden
- Bei Datenübermittlung: Rechtsgrundlage für die Übermittlung und Einwilligung
- Bei Auftragsverarbeitung: Schriftliche Vereinbarung zwischen Cloud-Nutzer und Cloud-Anbieter

41 vgl. BSI 2012, S. 26.

42 Die Information Technology Infrastructure Library (ITIL) ist eine Sammlung vordefinierter Prozesse, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur mittlerer und großer Unternehmen vorkommen.

43 vgl. BSI 2012, S. 74ff.

- Sitz des Cloud-Computing-Anbieters innerhalb der EU oder den Staaten des Europäischen Wirtschaftsraums (EWR) und Verarbeitung der Daten auch dort

Diese Mindestanforderungen des BSI lenken den Blick auf wichtige Aspekte bei Sicherheit in der Cloud, sind allerdings für eine Leistungs- und Anforderungsbeschreibung zu vage und abstrakt, da sie auf einer oberen Ebene bleiben und nicht spezifiziert werden. Beispielsweise ist die Anforderung „Der Datenschutz muss gewährleistet sein" viel zu generell; der „Teufel steckt hier im Detail". Vielmehr müssen sie für eine Anforderungsdefinition bei Cloud-Diensten konkretisiert werden, um entsprechende Nachweise zu erhalten und eine angemessene Entscheidung treffen zu können. Da es bisher an einem europaweit einheitlichen Standard fehlt[44], können die in Kapitel 2 beschriebenen Kriterienkataloge dazu dienen, die Anforderungen an IT-Sicherheit und Datenschutz definieren, da sie sie sehr dezidiert und genau die in den Mindestanforderungen des BSI operationalisieren.

Pointiert formuliert: Die meist frei verfügbaren Kriterienkataloge können als Informationsquelle genutzt werden, um die Sicherheits- und weitere Anforderungen an einen Cloud-Dienste-Anbieter zu beschreiben. Ob eine Kommune oder öffentliche Verwaltung dabei nur einen ausgewählten oder gleich mehrere Kriterienkataloge für Cloud-Sicherheit und Datenschutz in der Cloud nutzt, ist unerheblich. Wichtig ist, dass die wesentlichen Aspekte genauestens formuliert sind und einen Nachweis der Erfüllung seitens des Cloud-Anbieters ermöglichen. Sollten mehrere Kriterienkataloge herangezogen werden, besteht die Schwierigkeit darin, die einzelnen Anforderungen bzw. Kriterien voneinander abzugrenzen bzw. zu matchen. Denn die meisten Kataloge decken zum größten Teil identische Aspekte ab, sind aber unter Umständen anders formuliert und/oder benannt. Das macht es für Nicht-Experten schwerer, gleichartige Anforderungen zu erkennen. Hier kann es sinnvoll sein, die Unterstützung des IT-Dienstleisters zu nutzen oder sich selbst etwas einzulesen, um ein besseres Gefühl für die Materie zu bekommen. Sind die Anforderungen formuliert und liegen entsprechende Angebote von möglichen Anbietern vor, besteht die Herausforderung darin, die Angebote miteinander zu vergleichen und vor allem zu überprüfen, ob und wie die definierten Anforderungen, insbesondere bzgl. der Sicherheit, jeweils erfüllt werden. Der vermeintlich einfache Weg ist, auf die vom Anbieter ausgewiesenen Zertifizierungen und Testate, wie im Kapitel 2 beschrieben, zu vertrauen. Zertifikate und Testate dienen dazu, Vertrauen aufzubauen, denn der Cloud-Anbieter macht einem Externen die eigenen Sicherheitsmaßnahmen transparent und veröffentlicht das Ergebnis, oder zumindest Teile davon.

Bei den IT-Sicherheitsbezogenen Standards handelt es sich mehrheitlich um sogenannte Branchenstandards. Die Herkunft aus der Industrie könnte für den öffentlichen Sektor eher unbekannt sein und daher ist ggf. die Glaubwürdigkeit schwer einzuschätzen und weniger Vertrauen vorhanden. Zwar werden diese meist von unabhängigen und akkreditierten Dritten (meist Wirtschaftsprüfern) ausgestellt und sind somit grundsätzlich vertrauenswürdig. In aller Regel kann man sich als Anwender darauf verlassen, sollte sich aber nicht nur mit einem Zertifikat oder Siegel zufriedengeben, sondern auch den Prüfbericht lesen und zumindest den genauen Gegenstand und Umfang der Zertifizierung feststellen und mit den eigenen Anforderungen abgleichen. Ebenfalls ist zu verifizieren, ob eine solche Zertifizierung auch in Zukunft aufrechterhalten wird. Hinzukommt, dass Selbsterklärungen auf Basis von anerkannten Verhaltenskodizes, durch Protokolle, Reports und Statistiken

44 siehe Bernnat et al. o.J.

oder interne Auditberichte zunehmend an Bedeutung gewinnen. Dies bildet die Einstiegsstufe des Nachweises, den man häufig bei kleineren Anbietern findet, da Zertifizierungen teuer und aufwändig sind. Das ist nicht gleichbedeutend damit, dass das Sicherheitsniveau nicht ausreichend ist und sollte nicht per se Misstrauen wecken.

Im Ergebnis bleibt festzuhalten: Ein Cloud-Anwender muss die Aussagekraft des Zertifikats/Testats einschätzen können, um zu beurteilen, ob dadurch die eigenen Sicherheitsvorgaben eingehalten werden. Dabei besteht die Herausforderung, dass in der Tiefe meist nicht ganz klar ist, welche Anforderungen von welchen Zertifizierungsstandards abgedeckt werden. Der sicherste Weg ist eine so genannte vergleichende Synopse, d.h. eine Auflistung, welcher Standard welche Anforderung abdeckt. Das setzt allerdings erhebliches Fachwissen und ein tiefes Durchdringen der Materie voraussetzt. Nicht nur deswegen, sondern auch wegen des erheblichen zeitlichen Aufwands wird dies für eine Kommune kaum möglich sein. Ein angemessener Abgleich mit den aufgestellten Anforderungen kann aber auch dadurch erreicht werden, indem die Prüfberichte gelesen und mit den eigenen Anforderungen in Beziehung gesetzt werden. Anbieter werden damit mehr und mehr in die Verantwortlichkeit genommen, die entsprechende Auszüge aus Prüfberichten je Anforderung bereitzustellen und so auf eine vorhandene (Selbst-)Zertifizierung dieses Teilbereichs zu verweisen.

Kommunen und öffentlichen Verwaltungen wird geraten, nicht blind auf solche Nachweise zu vertrauen, sondern Unterlagen auf ihre Aussage- und Beweiskraft dahingehend zu überprüfen, ob ihre Anforderungen an die Cloud tatsächlich mit denen der favorisierten Lösungen übereinstimmen und vor allem wie diese Anforderungen erfüllt werden.

5 FAZIT UND AUSBLICK

Die Kurzstudie verdeutlichte, dass die Vorteile des Cloud-Computings eindeutig sind (siehe auch Anhang): große Datenmengen können günstig gespeichert, Informationen orts- und geräteunabhängig genutzt und IT-Ressourcen aller Art bedarfsgerecht und flexibel bereitgestellt werden, ohne dass damit eigene Anschaffungs- und Betriebskosten einhergehen, denn die Abrechnung erfolgt verbrauchsorientiert. Jedoch muss man sich eines bewusst sein: Die Daten und Ressourcen liegen auf fremden Servern an ggf. unterschiedlichen Standorten, die durch Netze untereinander verbunden sind, was bspw. erhöhte Anforderungen an die Sicherheit stellt. Beim Auswählen eines Cloud-Anbieters gilt es, Informationen zu verschiedensten Themengebieten zusammenzuführen, zu konsolidieren und zu verarbeiten. Insbesondere gehören auch Informationen dazu, die Auskunft darüber geben, inwiefern der Anbieter sowie der Cloud-Dienst selbst die jeweiligen Anforderungen an die Informationssicherheit und den Datenschutz erfüllen.

Die in der Kurzstudie dargestellten Standards bzw. die dahinter liegenden Kriterienkataloge im Bereich IT-Sicherheit und Datenschutz in der Cloud können als Formulierungshilfe für die Leistungs- und Anforderungsbeschreibung genutzt werden. Als Gradmesser für die Sicherheit in der Cloud dienen entsprechende Nachweise in Form von Zertifizierungen auf Basis existierender (de facto) Standards der Anbieter. Dabei kann zwar allen Nachweisformen generell vertraut werden, zur Überprüfung, ob und wie das Maß an Sicherheit tatsächlich ausreichend erfüllt ist, ist es jedoch empfehlenswert, die Nachweise und Prüfberichte genau zu prüfen. Das setzt wiederum ein gewisses Maß an Kompetenz voraus, das nicht ohne Weiteres vorhanden ist, gerade in kleinen Kommunen. Sofern man nicht auf die Kompetenz Dritter, bspw. des IT-Dienstleisters, zurückgreifen kann oder möchte, ist der eigene Kompetenzaufbau unerlässlich, um fundierte Entscheidungen für oder gegen eine Cloud-Lösung zu treffen. Der entsprechende Weg zu einer Auftraggeberkompetenz führt über die Auseinandersetzung mit entsprechenden Anforderungen an IT-Sicherheit und Datenschutz in der Cloud, welche nicht nur für die Auftragsvergabe, sondern auch für die spätere Steuerung des Dienstleisters notwendig ist. Die Kriterienkataloge der in der Kurzstudie ausgewählten Standards bieten dazu eine gute Übersicht und Strukturierung. Um diesen Kompetenzaufbau zu unterstützen und zu erleichtern, sollten in einem nächsten Schritt die zahlreichen Anforderungen konsolidiert und anwendergerecht operationalisiert werden. Auf diesem Weg werden öffentliche Verwaltungen und Kommunen besser als bisher in die Lage versetzt, die Prüfung der Sicherheitsanforderungen möglichst selbstständig vorzunehmen. Dabei geht es nicht nur um reine „Usability-Fragen“. Vielmehr sollen die Inhalte so aufbereitet werden, dass auch „Nicht“-Experten ein Verständnis davon bekommen, was die Anforderungen bedeuten, wie sie umzusetzen sind und welche Auswirkungen es haben kann, wenn diese nicht erfüllt werden.

QUELLENVERZEICHNIS

Arbeitsgemeinschaft der Leiter der Landesrechenzentren 2014: Cloud-Services der Landesrechenzentren. Eine Handlungsempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud (Entwurfspapier), https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/16_Sitzung/08_Cloud-Handlungsempfehlungen.pdf;jsessionid=FB5648A24907E523F-2B692D0AB42C390.1_cid322?__blob=publicationFile&v=2 (letzter Zugriff: 15.03.2019)

Auditor o.J.: European Cloud Service Data Protection Certification, https://www.auditor-cert.de (letzter Zugriff: 15.03.2019)

Beeck, V., o.J.: Bestätigungsvermerk, Definition, https://wirtschaftslexikon.gabler.de/definition/bestaetigungsvermerk-30733 (letzter Zugriff: 15.03.2019)

Bernnat, R./Zink, W./Bieber, N./Strach, J./Fischer, R./Tai, S. o.J.: Das Normungs- und Standardisierungsumfeld von Cloud Computing – Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud". Eine Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, https://www.trusted-cloud.de/sites/default/files/studie_normung_standards_lang.pdf (letzter Zugriff: 15.03.2019)

Bundesamt für Sicherheit in der Informationstechnik BSI 2012: Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit – (Eckpunktepapier), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-Cloud-Computing-Anbieter.pdf?__blob=publicationFile&v=8 (letzter Zugriff: 15.03.2019)

Bundesamt für Sicherheit in der Informationstechnik BSI 2017: Anforderungskatalog Cloud Computing (C5). Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3 (letzter Zugriff: 15.03.2019)

Bundesamt für Sicherheit in der Informationstechnik BSI, o.J.: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (letzter Zugriff: 15.03.2019)

Cloud Security Alliance CSA 2013: Cloud Controls Matrix v3.0 Info Sheet, https://downloads.cloudsecurityalliance.org/initiatives/ccm/CCM_v3_Info_Sheet.pdf (letzter Zugriff: 15.03.2019)

Cloud Security Alliance CSA o.J.: Cloud Controls Matrix Working Group, https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview (letzter Zugriff: 15.03.2019)

Deussen, P.H./Eckert, K.P./Hoepner, P./Hoffmann, C./Strick, L. 2014: Cloud-Fahrplan für die öffentliche Verwaltung, Paper des Kompetenzzentrum Öffentliche IT, https://www.oeffentliche-it.de/documents/10181/14412/Cloud-Fahrplan+öffentliche+Verwaltung (letzter Zugriff: 15.03.2019)

Deussen, P.H./Strick, L./Peters, J. 2010: Cloud-Computing für die öffentliche Verwaltung; ISPRAT-Studie, November 2010.

Deutscher Rat für Konformitätsbewertung im DIN, DIN KonRat 2013: Festlegungen zur Konformitätsbewertung in Normen, https://www.din.de/blob/66274/d599cc2763fdaef078caa5b4ef361e82/din-merkblatt-zur-konformitaetsbewertung-data.pdf (letzter Zugriff: 15.03.2019)

DIN/ISO o.J., Zertifizierung, https://www.din-iso-zertifizierung-qms-handbuch.de/zertifizierung/ (letzter Zugriff: 15.03.2019)

Dosch, S./Karlstetter, F. 2017: Cloud-Zertifikate: Stochern im Nebel. Wie man einen zuverlässigen Cloud-Anbieter erkennt, https://www.cloudcomputing-insider.de/wie-man-einen-zuverlaessigen-cloud-anbieter-erkennt-a-638966/ (letzter Zugriff: 15.03.2019)

EU SEC The European Security Certification Framework o.J.: https://www.sec-cert.eu (letzter Zugriff: 15.03.2019)

EuroCloud o.J.: StarAudit, https://www.eco.de/eurocloud/staraudit/ und https://www.eco.de/wp-content/blogs.dir/5/files/staraudit_folder-de1.pdf (letzter Zugriff: 15.03.2019)

Glancy, D.J. (1979): The Invention of the Right tp Privacy; in: Arizona Law Review (21) 1, pp. 1-39.

Haberich, F./Karlstetter, F. 2018: Microsoft stellt die deutsche Cloud ein. Warum?, https://www.cloudcomputing-insider.de/microsoft-stellt-die-deutsche-cloud-ein-warum-a-750263/ (letzter Zugriff: 15.03.2019)

ISO/IEC o.J.: ISO/IEC 27017:2015/ITU-T X.1631 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, http://www.iso27001security.com/html/27017.html (letzter Zugriff: 15.03.2019)

ITZ Bund 2018: Geschäftsbericht 2017, https://www.itzbund.de/DE/UeberUns/Imagematerial/Geschaeftsbericht_2017.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 15.03.2019)

Kersten, H., Klett, G., Reuter, J., Schröder, K.-W. 2016: IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls, Wiesbaden.

KGSt 2018: Cloud Computing verstehen und wirkungsvoll einsetzen; KGSt-Bericht 2/2018.

Klein, M. 2018: Digitalisierung mit der Bundescloud. Bundesbehörden können IaaS-Dienste nutzen, https://www.egovernment-computing.de/bundesbehoerden-koennen-iaas-dienste-nutzen-a-690803/ (letzter Zugriff: 15.03.2019)

Meints, M. 2014: Möglichkeiten der Nutzung von Cloud Services in der öffentlichen Verwaltung, Vortrag im November 2014.

Müller, D./ Karlstetter, F. 2018: Microsoft beerdigt seine Deutschland-Cloud. Treuhandmodell am Ende – die Deutsche Cloud lebt aber, https://www.cloudcomputing-insider.de/treuhandmodell-am-ende-die-deutsche-cloud-lebt-aber-a-750129/ (letzter Zugriff: 15.03.2019)

Müller, H./Strick, L./Köhl, S. 2018: Cloud-Dienste und DSGVO. Compliance-Anforderungen für öffent-liche Verwaltungen, in: Behörden Spiegel, November 2018, S. 26.

NIST 2011: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, (letzter Zugriff: 15.03.2019)

Saidah, A.S./Adelbaki, N. 2014: New Governance Framework to Secure Cloud Computing, in: Helfert, M./Desprez, F./Ferguson, D./Leymann, F./Munoz, V.M. (Hrsg.): Cloud Computing and Services Sciences. International Conference in Cloud Computing and Services Sciences, CLOSER 2014, Revised Selected Papers, April 3-5, 2014, Barcelona, Heidelberg.

StarAudit o.J.: https://staraudit.org/de/ (letzter Zugriff: 15.03.2019)

Trusted Cloud e.V. 2016: Cloud-Standards und Zertifizierungen im Überblick. Was cloud-spezifisch beachtet werden sollte, https://www.trusted-cloud.de/sites/default/files/beitrag-cloud-standards_und_zertifizierungen_im_ueberblick.pdf (letzter Zugriff: 15.03.2019)

Trusted Cloud e.V. 2016a: Kriterienkatalog für Cloud Services, https://www.trusted-cloud.de/sites/default/files/media/article/downloads/trusted_cloud_kriterienkatalog_v1.0_0.pdf, (letzter Zugriff: 15.03.2019)

Trusted Cloud e.V. 2016b: Trusted Cloud-Datenschutzpro l für Cloud-Dienste (TCDP), Version 1.0, https://tcdp.de/data/pdf/TCDP-1-0.pdf (letzter Zugriff: 15.03.2019)

Trusted Cloud e.V. 2017: Trusted Cloud Directory für Dienstleister Kriterien für kompetente Cloud-Beratung, Vortrag auf der CeBIT 2017 Hannover, https://www.trusted-cloud.de/sites/default/files/2017_tc_cebit_listung_dienstleister_v1.0.pdf (letzter Zugriff: 15.03.2019)

Trusted Cloud e.V. o.J.: Das Kompetenznetzwerk Trusted Cloud, https://www.trusted-cloud.de/de/ueber-trusted-cloud (letzter Zugriff: 20.08.2019)

ABBILDUNGS- UND TABELLENVERZEICHNIS

ANHANG: ENTWICKLUNGEN/ UMSETZUNG VON CLOUD IN DER DEUTSCHEN ÖFFENTLICHEN VERWALTUNG

In der jüngeren Vergangenheit gab es mehrere Anstrengungen, Cloud-Systeme auch für die öffentliche Verwaltung nutzbar zu machen. Auf Bundesebene wurde für die Bundesverwaltung die Bundescloud eingeführt, die öffentlichen IT-Dienstleister in den Bundesländern bieten zunehmend Cloud-Lösungen an und auch ein breites privatwirtschaftliches Angebot existiert, das öffentliche Einrichtungen nutzen können.

Ebenenübergreifender Rahmen für die Cloud-Nutzung

Auf Initiative mehrerer öffentlicher IT-Dienstleister hat der IT-Planungsrat einen Rahmen für die Ausschreibung von Cloud-Diensten 2014 beschlossen, der in der Anlage auch Kriterien für die Entscheidung enthält[45]. Im Kontext der Landesrechenzentren werden erweiterte Kombinationen der grundsätzlichen Betriebsmodelle betrachtet und Empfehlungen gegeben, wann diese verwendet werden sollten.

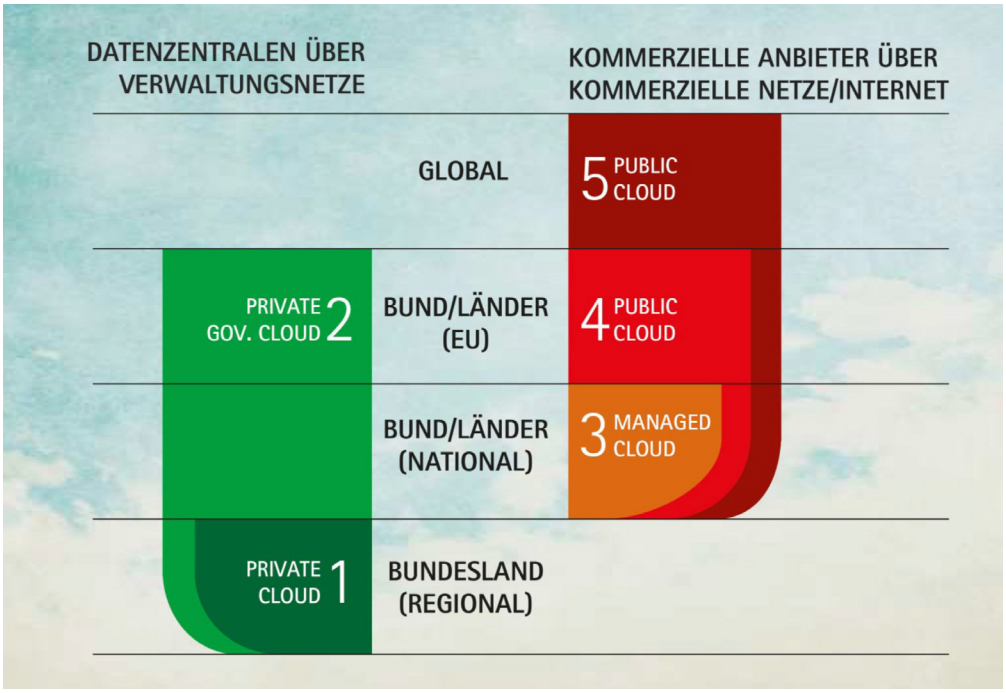

Abbildung 3: Cloud-Kategorien im Kontext der Landesrechenzentren (Quelle: Arbeitsgemeinschaft der Leiter der Landesrechenzentren 2014, S. 8)

45 Arbeitsgemeinschaft der Leiter der Landesrechenzentren 2014.

1. Private Cloud: Bei der Private Cloud handelt es sich um einen individuell und exklusiv für einen Kunden eingerichteten Service, der genaugenommen als Managed Private Cloud anzusehen ist.

2. Private Government Cloud (PGC): Im Rahmen der Private Government Cloud (PGC) können Skalen-Effekte realisiert werden, die dem einzelnen Land nicht möglich wären. Somit können bundesweit einheitliche Service kostengünstiger als ein einzelnes Rechenzentrum angeboten werden (Stichwort: Community Cloud). Die Netzanbindung ist durch die verschiedenen Ebenen der Verwaltungsnetze gewährleistet. Ob die Cloud Infrastruktur rechenzentrums- oder sogar bundesländerübergreifend bzw. national von öffentlichen oder geeigneten kommerziellen Anbietern bereitgestellt werden, ist zu entscheiden.

3. Managed Cloud kommerzieller deutscher Anbieter: Dieses Modell entspricht im Wesentlichen der Privaten Cloud mit dem Unterschied, dass es sich bei dem Anbieter um einen kommerziellen Anbieter ohne die in den Landesrechenzentren besondere Spezialisierung für die öffentliche Verwaltung handelt und die Netzanbindung nicht über ein Verwaltungsnetz erfolgt.

4. Public Cloud kommerzieller europäischer Anbieter: Public Clouds werden von kommerziellen Unternehmen betrieben, wobei in den meisten Fällen unbekannt ist, von welchem Rechenzentrum die eigentlichen Cloud-Infrastrukturen bereitgestellt und betrieben werden, wo sich diese Standorte befinden und welchen Sicherheitskriterien sie unterliegen. Die Netzanbindung erfolgt nicht über ein Verwaltungsnetz.

5. Sonstige Public Clouds: Die Rechenzentren dieser Anbieter stehen häufig an Orten, die durch das Datenschutzrecht (DSGVO und BDSG neu) als bedenklich einzustufen sind, oder deren Orte unbekannt sind und sind daher als unsicher einzuschätzen. Die Services werden ohne individuellen Vertrag bereitgestellt. Sie sind vergleichbar mit öffentlichen Plätzen und fallen unter die Rubrik „Nutzung auf eigene Gefahr“ und sollten für die öffentliche Verwaltung nicht in Betracht gezogen werden.

Da der Rahmen jedoch vor Inkrafttreten der neuen europäischen Datenschutzgrundverordnung (DSGVO) beschlossen wurde, sind die Hinweise auf die jeweiligen Landesdatenschutzgesetze hinfällig bzw. sind entsprechend zu überprüfen. In den Bewertungen über die Geeignetheit für eines der Modelle wird auf Sicherheitsstandards und Rechtssicherheit verwiesen, die die jeweiligen Anbieter und Modelle erfüllen. Immer wieder wird auch darauf verwiesen, dass die Cloud-Systeme der öffentlichen Dienstleister den Anforderungen der öffentlichen Verwaltungen besser abdecken als private Anbieter.

Bundescloud

Zum 30.06.2017 wurde mit der Bundescloud-Box (BC-Box) der erste Dienst mittels der Bundescloud produktiv gesetzt. Es ist vorgesehen, die BC-Box sukzessive für alle Bundesbediensteten zur Verfügung zu stellen. Mit der BC-Box können Daten sicher in der Cloud gespeichert und selbstbestimmt auch ressortübergreifend geteilt oder gemeinsam bearbeitet werden. Der Zugang zur Bundescloud ist nur aus den sicheren Verwaltungsnetzen möglich. Betreiber der Bundescloud ist aktuell das Informationstechnikzentrum Bund (ITZBund). Die BWI GmbH wird als zweiter bundeseigener IT-Dienstleister eine wichtige Rolle beim weiteren Ausbau der Bundescloud spielen. Die Bundescloud wird im Rahmen des ressortübergreifenden Projekts „IT-Konsolidierung Bund" realisiert.[46][47] Mit Bereitstellung der Infrastruktur-Angebote (IaaS) unterstützt die Bundescloud seit März 2018 die Betriebskonsolidierung der Bundesbehörden. Zudem sollen mit der Bundescloud IT-Services für Behörden des Bundes automatisiert und standardisiert bereitgestellt werden. Die Dienste sind damit behördenübergreifend und schnell nutzbar. Mitarbeiter der Bundesverwaltung sollen Daten und Dokumente über die Bundescloud sicher behördenübergreifend austauschen können. Außerdem wird ein Self-Service-Portal angeboten, über das Cloud-Services bestellt und künftig auch überwacht und abgerechnet werden sollen. Die Bestellprozesse für IT-Services sollen dadurch vereinheitlicht und verschlankt werden.

Deutschland-Cloud von Microsoft und T-Systems

Die Besonderheit der Deutschland-Cloud ist, dass Microsoft die Daten seiner Kunden bei diesem Dienst in Deutschland speichern wollte, statt – wie sonst üblich – in den USA. Als Treuhänder kam die Telekom-Tochter T-Systems International zum Einsatz, die den Zugang zu den Kundendaten kontrolliert und überwacht hat. Für diese Sicherheit mussten die Kunden einen Aufpreis zahlen. Der Softwarekonzern hatte Ende 2015 vor allem auf die NSA-Affäre reagiert und den Service einer „deutschen Cloud" aufgebaut. Dabei fungiert die Telekom als Treuhänder, so dass Microsoft selbst in der Regel keinerlei Zugriff auf die Daten der Kunden hat. Somit hätte das Unternehmen bei Forderungen amerikanischer Behörden keine Daten aushändigen können. Der Ende März in den USA in Kraft getretene Gesetz CLOUD Act sieht vor, dass amerikanische Onlinefirmen US-Ermittlungsbehörden grundsätzlich Zugang zu den Daten von US-Bürgern gewähren müssen, auch wenn diese außerhalb der USA gespeichert sind. Zugleich können sich die Firmen dagegen wehren, wenn es um Bürger anderer Länder geht oder dadurch Gesetze anderer Staaten verletzt würden.[48]

Es gibt so gut wie keine Nachfrage zur Deutschen Cloud. Dies hat zwei Gründe: zum einen ist die Deutsche Cloud kostenintensiver als die „normale" Europäische Cloud und zum anderen ist der Aufwand, um in die Deutsche Cloud von Microsoft zu kommen, auf Kunden- und Microsoft-Seite höher.[49]

Initiative Cloud-Services „Made in Germany"

Die Initiative wurde 2010 vom deutschen Cloud-Anbieter AppShere AG gegründet. Ziel ist es, Vertrauen in Cloud-Ressourcen zu erhöhen und Anwender bei der Auswahl von rechtssicheren Cloud-Lösungen

46 Klein 2018.

47 ITZ Bund 2018, S. 24.

48 siehe http://www.spiegel.de/netzwelt/web/deutsche-cloud-microsoft-stellt-vertrieb-seines-datendienstes-ein-a-1226307.html (letzter Zugriff 15.03.2019)

49 vgl. Haberich/Karlstetter 2018 und Müller/Karlstetter 2018.

zu unterstützen. Zudem sollen die Lösungen deutscher Anbieter bekannt gemacht werden. Cloud-Unternehmen können Mitglied werden, wenn sie folgende Kriterien erfüllen:

- Das Unternehmen des Cloud Service-Betreibers wurde in Deutschland gegründet und hat dort seinen Hauptsitz.
- Das Unternehmen schließt mit seinen Cloud Service-Kunden Verträge mit Service Level Agreements (SLA) nach deutschem Recht.
- Der Gerichtsstand für alle vertraglichen und juristischen Angelegenheiten liegt in Deutschland.
- Das Unternehmen stellt für Kundenanfragen einen lokal ansässigen, deutschsprachigen Service und Support zur Verfügung.
- Die Mitglieder bieten SaaS-, PaaS- und IaaS-Lösungen an, die auf der Webseite der Initiative in einem Katalog gelistet sind.[50]

Die Initiative wirbt damit, dass Kundendaten ausschließlich in Deutschland liegen, so dass eine der häufigen Grundanforderungen der öffentlichen Verwaltung erfüllt ist. Zudem präferiert die öffentliche Verwaltung in der Regel einen örtlichen und deutschsprachigen Support.

50 https://www.cloud-services-made-in-germany.de/loesungskatalog.

IMPRESSUM

Die Kurzstudie basiert auf einer Initiative des Nationalen E-Government Kompetenzzentrums e. V.

Ansprechpartner

Stefanie Köhl
koehl@shi-institut.de

Heidrun Müller
heidrun.mueller@egovcd.de

SHI Stein-Hardenberg Institut GmbH
in Kooperation mit eGov Consulting and Development GmbH (eGovCD)

Nationales E-Government Kompetenzzentrum e. V.

Pressehaus / 4102
Schiffbauerdamm 40
10117 Berlin

+49 (0)30 80494747
info@negz.org
negz.org

Gestalterische Umsetzung
made in – Design & Strategieberatung
www.madein.io

Druckproduktion
DRUCKPUNKT Digital Offset GmbH
www.druckpunkt-digital-offset.de

BERICHTE DES NEGZ

Folgende Kurzstudien sind in der Reihe „Berichte des NEGZ“ bereits erschienen:

Nr. 1 Schuppan, T., Köhl, S., Off, T. (2018). Vollzugsorientierte Gesetzgebung durch eine Vollzugssimulationsmaschine, Berlin. » DOI

Nr. 2 Ogonek, N., Distel B., Ben Rehouma, M., Hofmann, S., Räckers, M. (2018). Digitalisierungsverständnis von Führungskräften, Berlin. » DOI

Nr. 3 Djeffal, C. (2018). Künstliche Intelligenz in der öffentlichen Verwaltung, Berlin. » DOI

Nr. 4 Fadavian, B., Franzen-Paustenbach, D., Rehfeld, D., Schmitt, M., Schweikart, D., Djeffal, C. (2019). Data Driven Government, Berlin. » DOI

Nr. 5 Balta, D., Hofmann, S., Rehfeld, D., Kuhn, P., Krcmar, H., (2019). Sharing Economy: Potential im öffentlichen Sektor, Berlin. » DOI

Nr. 6 Hoepner, P., Welzel, C., Wulff, M. (2019). Identifizierung und Authentifizierung leicht gemacht – die Nutzer ins Zentrum stellen, Berlin. » DOI

Nationales E-Government Kompetenzzentrum e. V.
Pressehaus / 4102
Schiffbauerdamm 40
10117 Berlin

+49 (0)30 80494747
info@negz.org
negz.org

ISSN (online) 2626-6032
DOI 10.30418/2626-6032.2019.07