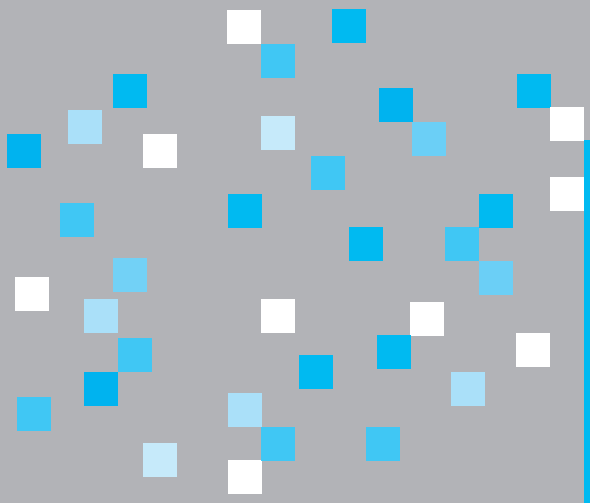
Trusted Cloud



Pilotprojekt Datenschutz-Zertifizierung für Cloud-Dienste

TCDP-Konzept der modularen Zertifizierung von Cloud-Diensten

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ wurde von November 2013 bis April 2015 (Phase 1) und von September 2015 bis September 2016 (Phase 2) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) durchgeführt.[1]

Am Pilotprojekt sind alle maßgeblichen Interessenvertreter beteiligt. Dazu gehören insbesondere Datenschutzbehörden und Privatwirtschaft, insbesondere Anbieter und Nutzer von Cloud-Diensten und Verbände, sowie Stellen mit Erfahrung in der Normung und Zertifizierung von IT-Diensten.

1 Informationen zum Pilotprojekt sind abrufbar unter www.tcdp.de.

Inhalt

1 Grundlagen der Datenschutz-Zertifizierung von Cloud-Diensten

1.1 Gegenstand und Ziel der Zertifizierung

Bei der Nutzung von Cloud Computing-Diensten muss ein hinreichender Datenschutz gewährleistet sein, der sich auch auf die Sicherheit der Datenverarbeitung beim Cloud-Anbieter erstreckt. Daher müssen die technischen und organisatorischen Maßnahmen des Cloud-Anbieters überprüft werden. Soweit der Cloud-Anbieter im Rahmen einer Auftragsdatenverarbeitung tätig wird, ist jeder Cloud-Nutzer (d.h. Cloud-Kunde, die Einheit, die den Dienst verwendet) als Auftraggeber gesetzlich verpflichtet, sich von der Ordnungsgemäßheit der technischen und organisatorischen Maßnahmen des Cloud-Anbieters zu überzeugen.

Eine Überprüfung der technischen Systeme des Cloud-Anbieters durch jeden Cloud-Nutzer ist jedoch nicht sinnvoll. Sie würde zu weit überhöhten Kosten für die – u.U. vielfache – Prüfung der Systeme des Cloud-Anbieters führen, könnte ihrerseits Sicherheitsrisiken bergen und von zahlreichen Cloud-Nutzern, insbesondere kleinen Unternehmen, nicht aus eigener Kraft durchgeführt werden.

Diese Schwierigkeiten können durch die Datenschutz-Zertifizierung nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) überwunden werden. Das TCDP umfasst die datenschutzrechtlichen Anforderungen des BDSG an den Auftragsdatenverarbeiter im Cloud Computing. Dabei werden die technischen Maßnahmen des Cloud-Anbieters von einer fachlich geeigneten und unabhängigen Stelle überprüft und bestätigt. Das Ergebnis der Prüfung kann allen Cloud-Nutzern zur Verfügung gestellt werden und ihnen die eigene Prüfung ersparen. Mit dieser Zertifizierung wird sowohl ein hohes Datenschutzniveau gewährleistet als auch eine effiziente Grundlage für die Nutzung von Cloud-Diensten geschaffen.

Das Konzept der Datenschutz-Zertifizierung wurde von der AG „Rechtsrahmen des Cloud-Computing“ im Technologieprogramm „Trusted Cloud“ des BMWi entwickelt.[2] Im Pilotprojekt Datenschutz-Zertifizierung für Cloud-Computing wurden die Grundlagen der Datenschutz-Zertifizierung, insbesondere das TCDP und die TCDP-Verfahrensordnung für Zertifizierung von Cloud-Diensten erarbeitet. Damit steht für den Geltungsbereich des BDSG die Datenschutz-Zertifizierung für Cloud-Dienste praktisch zur Verfügung und kann von allen Anbietern und Nutzern dieser Dienste genutzt werden.

Das TCDP und die TCDP-Verfahrensordnung für Cloud-Dienste werden ab Oktober 2016 von der Stiftung Datenschutz verwaltet. Die Stiftung Datenschutz führt auch ein Verzeichnis von Zertifizierungsstellen, die eine TCDP-Zertifizierung durchführen können.

1.2 Gesetzliche Grundlagen und künftige Entwicklung der Zertifizierung

Das TCDP beruht auf dem BDSG als maßgeblicher datenschutzrechtlicher Grundlage für den Bereich der Privatwirtschaft. Die im Mai 2016 in Kraft getretene Europäische Daten-

2 AG Rechtsrahmen des Cloud Computing, „Datenschutzrechtliche Lösungen für Cloud Computing. Ein rechtspolitisches Thesenpapier“, 2012, abrufbar unter www.tcdp.de.

schutz-Grundverordnung (DSGVO) wird ab dem 25. Mai 2018 in Deutschland anwendbar sein und nationale Gesetze verdrängen. Das BDSG wird voraussichtlich durch ein deutsches Ausführungsgesetz zur DSGVO ersetzt.

Die DSGVO enthält eine gesetzliche Grundlage für Datenschutz-Zertifizierungen, auf die die TCDP-Zertifizierung für Cloud-Dienste ausgerichtet ist. Die Zertifizierung nach TCDP muss mit Wirkung zum 25. Mai 2018 an die DSGVO angepasst werden. Das Bundesministerium für Wirtschaft und Energie (BMWi) sowie der Bundesminister des Innern (BMI) unterstützen die Weiterentwicklung der Datenschutz-Zertifizierung für Cloud-Dienste. Dabei wird angestrebt, die nach TCDP erteilten Zertifikate in ein Datenschutzzertifikat auf der Grundlage der DSGVO zu überführen, um eine lückenlose Zertifizierung für Cloud-Anbieter zu ermöglichen.

1.3 Gegenstand und Umfang der Zertifizierung

Der Gegenstand der Zertifizierung folgt aus ihrem Ziel. Da die Zertifizierung die eigene Prüfung der technischen und organisatorischen Maßnahmen des Auftragnehmers, beim Cloud-Computing also des Cloud-Anbieters, durch den Cloud-Nutzer als Auftraggeber ersetzen soll, muss Gegenstand der Zertifizierung der vom Cloud-Nutzer in Anspruch genommene Dienst sein, also die Leistung, die der Cloud-Anbieter für den Cloud-Nutzer erbringt.

Entsprechend muss die Zertifizierung aus deutscher Sicht ihrem Umfang nach alle Aspekte umfassen, die nach den gesetzlichen Anforderungen, derzeit § 11 BDSG i.V.m. § 9 BDSG und künftig Art. 28 DSGVO, Gegenstand der Prüfung durch den Cloud-Nutzer als Auftraggeber sind. Dies sind insbesondere die in § 9 BDSG genannten technischen und organisatorischen Maßnahmen, durch die die datenverarbeitende Stelle bzw. der Auftragnehmer die gesetzlichen Anforderungen erfüllt. Im Vordergrund stehen Maßnahmen zum Schutz gegen unbefugte Datenverarbeitung.

1.4 Effizienz als eine zentrale Herausforderung einer Zertifizierung

Ein Zertifizierungsverfahren, das es dem Cloud-Nutzer ermöglicht, auf die eigene Überprüfung der Maßnahmen des Cloud-Anbieters zu verzichten und auf das TCDP-Zertifikat zu vertrauen, hat etliche Herausforderungen zu meistern. So müssen etwa Prüfanforderungen und das Verfahren der Zertifizierung festgelegt werden, Zuständigkeiten und Verantwortlichkeiten geklärt werden. Daher wurden im Pilotprojekt Datenschutz-Zertifizierung die Prüfanforderungen durch das TCDP verbindlich festgelegt. Ebenso wurde festgelegt, dass das TCDP-Zertifikat nur unter Einhaltung der TCDP-Verfahrensordnung geführt werden darf.

Die für die Praxis wohl wichtigste Herausforderung dürfte sich aus den erheblichen Kosten ergeben, die mit der Prüfung und Zertifizierung von Datenverarbeitungssystemen verbunden sein können. Insbesondere besteht die Gefahr, dass bei überhöhten Anforderungen und entsprechend hohen Kosten für Prüfung und Zertifizierung die Zertifizierung für zahlreiche, insbesondere kleinere Anbieter von Cloud-Diensten unattraktiv wird.

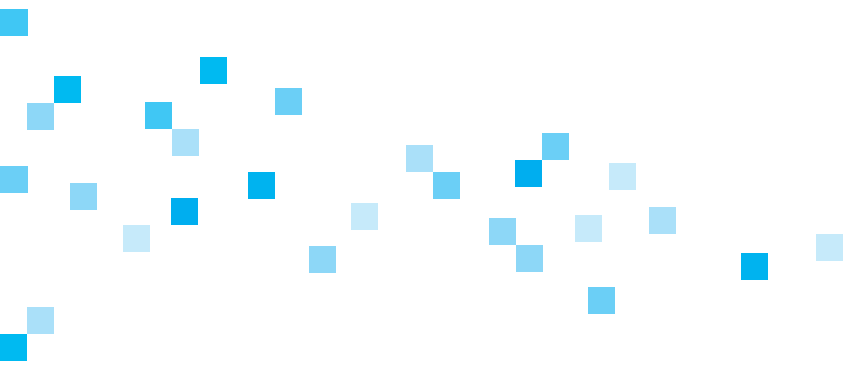
Ein wesentliches strukturelles Problem für kostengünstige Prüfung und Zertifizierung, nicht zuletzt beim Cloud Computing, ergibt sich aus dem Gegenstand der Zertifizierung, der sich auf die vom Cloud-Nutzer in Anspruch genommene Leistung beziehen muss.

Anbieter von Cloud-Diensten bieten zahlreiche unterschiedliche Pakete von Diensten (Funktionen) an, um ein für die Bedürfnisse ihrer Kunden maßgeschneidertes Angebot bereitzustellen. Es entspricht einem Grundanliegen des Cloud Computing, dem Nutzer diejenigen Datenverarbeitungsdienste anzubieten, die er tatsächlich benötigt. Aus dem individuellen Zuschnitt der Datenverarbeitungsdienste für die verschiedenen Nutzergruppen folgt ein Teil der mit Cloud Computing verbundenen Kostenvorteile. Außerdem werden Cloud-Dienste und ihre Bestandteile laufend fortentwickelt.

Für die Zertifizierung führt der Umstand, dass Cloud-Anbieter ihren Kunden zahlreiche unterschiedliche Varianten von Diensten anbieten und die Dienste sich ändern, zu einem entscheidenden Problem: Aus dem Grundsatz, dass die Zertifizierung den Dienst betreffen soll, den der Kunde in Anspruch nimmt, folgt, dass jede einzelne dieser Dienstevarianten der Zertifizierung bedarf. Weiterhin folgt daraus, dass bei Änderung eines Dienstebestandteils eine erneute Zertifizierung erforderlich sein kann.

Sollte nun jede einzelne dieser Dienstevarianten einer separaten Prüfung bedürfen oder bei jeder Änderung eines Bestandteils der gesamte Dienst neu zertifiziert werden müssen, müsste der Anbieter die gesamten Kosten für Prüfung und Zertifizierung häufig aufbringen. Dies würde es Cloud-Anbietern wesentlich erschweren, neue Produkte anzubieten oder Dienste fortzuentwickeln. Vor allem wäre dieses Vorgehen ineffizient, da die einzelnen Bestandteile der Dienste mehrfach, u.U. vielfach geprüft werden müssten, obwohl sie technisch identisch eingesetzt werden.

Damit ergibt sich, dass Voraussetzung eines erfolgreichen Einsatzes von Zertifizierungen die Gewährleistung eines kostengünstigen, effizienten Zertifizierungssystems ist, das Mehrfachprüfungen vermeidet.



2 Das TCDP-Konzept der modularen Zertifizierung

2.1 Effiziente und kostengünstige Zertifizierung durch modulare Zertifizierung

Wesentliches Element der Zertifizierung nach dem Konzept der AG „Rechtsrahmen des Cloud Computing“ ist es, dass ein Dienst möglichst nur einmal – von einer unabhängigen und kompetenten Stelle – geprüft werden muss. Diese Prüfung sollte allen Nutzern dieses Dienstes zugutekommen.

Entsprechendes muss innerhalb der Zertifizierung gelten: Die technischen und organisatorischen Maßnahmen sollten nur einmal geprüft werden, und diese Prüfung sollte allen Einsatzbereichen zugutekommen, soweit die Anforderungen des Einsatzbereiches von der Prüfung abgedeckt sind.

Dieses Ziel ließe sich teilweise durch eine Gesamt-Zertifizierung aller Dienste eines Anbieters erreichen. Wenn das größtmögliche Diensteangebot eines Cloud-Anbieters geprüft und zertifiziert wird, muss das Zertifikat auch das Anbieten von Teilen des Angebots abdecken. Beispiel: Wenn ein Cloud-Anbieter die Dienste A, B und C anbietet und das Diensteangebot aus diesen Diensten A, B, C einschließlich der Interaktion dieser Dienste geprüft und zertifiziert wurde, gilt dieses Zertifikat auch für ein Diensteangebot bestehend aus den Diensten A und B.

Allerdings hat die Gesamt-Zertifizierung Grenzen und Nachteile. Sie beantwortet nicht die Frage, wie zu verfahren ist, wenn der Cloud-Anbieter eine neue Komponente D hinzufügen möchte. Zudem wäre eine Gesamt-Zertifizierung oft unverhältnismäßig aufwendig, etwa wenn ein Cloud-Anbieter nur Teile seines Angebots zertifizieren lassen möchte, weil die Zertifizierung ausschließlich für diese von Bedeutung ist.

Daher ist die datenschutzrechtliche Zertifizierung im Hinblick auf eine effiziente Zertifizierung fortzuentwickeln: Bei Änderungen des Angebots sollte auf bestehende Zertifizierungen zurückgegriffen werden können, mit der Folge, dass ggf. nur Änderungen neu zu zertifizieren sind. Letztlich muss es möglich sein, die einzelnen Dienste, die nachfolgend als Module bezeichnet werden, jeweils separat zu prüfen und zu zertifizieren und bei der Zertifizierung der Kombinationen von Modulen (Diensten) hierauf zu verweisen.

Mit diesem Konzept, das man als modulare Zertifizierung bezeichnen kann, wird eine effiziente Zertifizierung ermöglicht und ein breites Anwendungsfeld für die Zertifizierung von Cloud-Diensten eröffnet. Im Rahmen dieser modularen Zertifizierung ist zwischen einer horizontalen und einer vertikalen Modularisierung zu unterscheiden.

2.2 Horizontal modulare Zertifizierung

2.2.1 Horizontale Modularisierung von Datenverarbeitungsdiensten

Die modulare Zertifizierung entspricht dem Umstand, dass Angebote von Datenverarbeitungsdiensten häufig modular aufgebaut sind. So kann etwa Datenspeicherung als separater Dienst angeboten werden, ist aber zugleich Bestandteil fast aller komplexeren Dienste. E-Mail kann als einzelner Dienst angeboten werden, ist aber oft in Dienstepake-

ten als Modul (Funktion, Element) enthalten. Die einzelnen Module werden häufig mehrfach genutzt. So wird ein Modul technisch identisch als Bestandteil unterschiedlicher Dienste oder Dienstepakete für unterschiedliche Kundenkreise angeboten und genutzt. Dies ist notwendig, denn nur dadurch können die Angebote für die einzelnen Nutzer effizient gestaltet werden.

Insoweit kann, da die Zusammensetzung auf der Anwendungsebene erfolgt, von einer horizontalen Modularisierung der Datenverarbeitungsdienste (oder Anwendungen) gesprochen werden.

2.2.2 Horizontale Modularisierung der Prüfung und Zertifizierung

Aus der horizontal modularen Struktur der Dienste folgt der Bedarf nach einer horizontal modularisierten Prüfung und Zertifizierung. Der Dienst „E-Mail“ beispielsweise sollte nicht deswegen anhand derselben Prüfanforderungen mehrfach geprüft werden müssen, weil er einmal als Dienst für Verbraucher, und ein anderes Mal – technisch identisch – als Bestandteil eines Dienstepaketes für Unternehmen angeboten wird.

2.3 Vertikal modulare Zertifizierung

2.3.1 Vertikale Struktur von Datenverarbeitungsdiensten

Eine modulare Struktur lässt sich auch hinsichtlich der Zusammensetzung der einzelnen Dienste feststellen. Ein Datenverarbeitungsdienst beruht jeweils auf mehreren technischen und organisatorischen Komponenten (Bestandteile, Elemente). So sind Geräte und Programme zu unterscheiden. Technische Geräte, z.B. Server, die für den Dienst benötigt werden, sind in einem Serverraum untergebracht. Sowohl für diesen als auch für die technische Infrastruktur gelten entsprechende technische und organisatorische Anforderungen.

Diese technischen Grundlagen, angefangen vom Serverraum über Stromversorgung etc. bis zu Programmen, lassen sich systematisch in Schichten oder Funktionen aufspalten. In aller Regel beruht eine Anwendung auf mehreren Schichten, die durch unterschiedliche technische Maßnahmen ausgeübt werden können (siehe unten 3).

Diese technischen Komponenten werden oft von mehreren Anwendungen gleichermaßen genutzt. So kann ein Serverraum für eine Mehrzahl oder gar Vielzahl von Systemen genutzt werden, die unterschiedlichen Anwendungen dienen, oder es können auf einem physischen Server mehrere Anwendungen oder virtuelle Systeme betrieben werden.

2.3.2 Effiziente Prüfung und Zertifizierung einzelner Dienstebestandteile

Ähnlich wie bei der unterschiedlichen Kombination von Anwendungen in verschiedene Dienstepakete, stellt sich in Bezug auf Zertifizierung von Diensten die Frage, ob einzelne Bestandteile des Dienstes jeweils neu geprüft werden müssen, wenn sie für einen anderen Dienst eingesetzt werden. Muss beispielsweise die Sicherheit eines Serverraums mehrfach geprüft werden, wenn neben einem E-Mail-Dienst von dort aus auch ein Speicherdienst angeboten wird? Oder – unterstellt, es gelten dieselben Anforderungen – muss es nicht ausreichen, wenn der Serverraum einmal geprüft wird? Es ist offensichtlich, dass eine mehrfache Prüfung derselben technischen und organisatorischen Grundlagen verschiede-

ner Dienste anhand derselben Prüfanforderungen, beispielsweise der Sicherheit von Serverräumen, ineffizient wäre.

Daher ist anzustreben, dass eine Prüfung einer einzelnen technischen und organisatorischen Komponente für alle Dienste gilt, in denen diese Komponente eingesetzt wird, soweit die für die jeweiligen Dienste maßgeblichen Prüfanforderungen von der Prüfung umfasst sind. Entsprechend muss ein Zertifikat für einen einzelnen Dienst auf eine solche Prüfung zurückgreifen können. Insoweit ist von einer vertikal modularen Prüfung und Zertifizierung zu sprechen.

2.4 Gleichwertigkeit der modularen Zertifizierung

Die modulare Prüfung und Zertifizierung kann der einheitlichen, separaten Zertifizierung eines Diensteangebots gleichwertig sein, soweit die modulare Zertifizierung alle Merkmale der gebotenen Prüfung und Zertifizierung umfasst und hinsichtlich der Elemente der Prüfung und Zertifizierung denselben Anforderungen genügt, wie die einheitliche, separate Prüfung und Zertifizierung.

Dazu müssen anspruchsvolle Voraussetzungen erfüllt werden. So ist sicherzustellen, dass eine modulare Prüfung im Ergebnis alle Prüfanforderungen an den jeweiligen Dienst abdeckt. Weiterhin müssen alle Prüfungen, auf die sich das Zertifikat des Dienstes bezieht, auch verfahrensmäßig nach einem einheitlichen Standard durchgeführt werden, der den Anforderungen an eine ordnungsgemäße Prüfung für den jeweiligen Dienst genügt. In Bezug auf Verantwortlichkeit und Haftung für Prüfung und Zertifizierung dürfen sich für Dritte keine Nachteile gegenüber einer einheitlichen Prüfung und Zertifizierung ergeben.

Sind diese Voraussetzungen gegeben, ist ein auf modularer Prüfung beruhendes Zertifikat einem auf einheitlicher Prüfung beruhenden Zertifikat gleichwertig und muss dieselbe tatsächliche und rechtliche Bedeutung haben.

2.5 Elemente und Herausforderungen eines Systems modularer Zertifizierung

2.5.1 Das Verhältnis von Prüfung und Zertifizierung

Für ein System modularer Zertifizierung ist das Verhältnis von Prüfung und Zertifizierung zu klären. Prüfung und Zertifizierung sind jedenfalls systematisch, nicht notwendig organisatorisch, getrennte Vorgänge. Prüfung ist die von einer Person, dem Prüfer oder der Prüfstelle, durchgeführte Untersuchung, ob der Prüfgegenstand die erforderlichen normativen Merkmale (Prüfanforderungen) aufweist. Die Zertifizierung ist die Bestätigung einer Person der Zertifizierungsstelle, dass die Prüfung durch den Prüfer (ordnungsgemäß) erfolgte. Prüfung und Zertifizierung sind im System der Zertifizierung nach TCDP organisatorisch und rechtlich getrennt.

2.5.2 Modulare Zertifizierung durch Verweis auf Zertifikate

Bei einer modularen Zertifizierung bestehen in Bezug auf die Prüfung keine grundsätzlichen Besonderheiten. Für die technischen und organisatorischen Anforderungen eines Moduls oder einer Komponente ist eine Prüfung durchzuführen. Für jede Prüfung sollte ein Zertifikat ausgestellt werden können. Wesentlich für die modulare Zertifizierung ist,

dass auf (vorangegangene) Prüfungen von Modulen oder Komponenten verwiesen werden kann. Dies kann insbesondere dann erfolgen, wenn die Prüfung durch ein Zertifikat dokumentiert ist. Es wird dann also auf ein Zertifikat verwiesen.

Auch im Rahmen einer modularen Zertifizierung benötigt jeder Dienst i.S. eines Dienstesangebots für einen Nutzer ein Zertifikat. Dieses kann aber ganz oder teilweise zusammengesetzt sein aus dem Verweis auf verschiedene Zertifikate, die für die einzelnen Komponenten und Module ausgestellt sind.

Beispiel: Ein Zertifikat für ein Dienstepaket bestehend aus den Modulen A, B und C könnte auf bestehende Zertifikate für die Module A und B verweisen und für das Modul C sowie für das Zusammenwirken der drei Module auf einer im Rahmen der Zertifizierung erfolgten zusätzlichen Prüfung beruhen. Es könnte alternativ auf bestehende Zertifikate für alle drei Module und für das Zusammenwirken der Module verweisen. Ebenso kann ein Zertifikat für ein Modul A zusammengesetzt werden aus bestehenden Zertifikaten für die Komponenten 1, 2 und 3 sowie einer im Rahmen der Zertifizierung erfolgten zusätzlichen Prüfung des Zusammenwirkens der Komponenten.

2.5.3 Verhältnis von Prüfung und Zertifizierung und Verantwortlichkeiten

In einem System modularer Zertifizierung können Zertifikate auf Prüfungen und Zertifizierungen unterschiedlicher Zertifizierungsstellen beruhen. So kann es sein, dass etwa ein Rechenzentrum durch die Zertifizierungsstelle A, der unter Nutzung dieses Rechenzentrums angebotene Dienst aber von der Zertifizierungsstelle B zertifiziert werden soll.

Voraussetzung einer Kombination von Zertifikaten unterschiedlicher Zertifizierungsstellen ist, dass die Prüfung durch die Zertifizierungsstelle, auf deren Zertifikat verwiesen wird, einer eigenen Prüfung gleichwertig ist. Dies ist der Fall, wenn die Prüfung anhand mindestens gleichwertiger Prüfanforderungen erfolgt und das Zertifizierungsverfahren, in dem das Zertifikat erstellt wurde, ebenfalls den Anforderungen des Zertifizierungsverfahrens genügt, in dem auf das vorangegangene Zertifikat verwiesen werden soll. Dies setzt eine vollständige Transparenz hinsichtlich der Prüfanforderungen und die Möglichkeit voraus, die Gleichwertigkeit von Zertifizierungsverfahren festzustellen.

Bei einer derartigen Kombination von Zertifikaten unterschiedlicher Zertifizierungsstellen ergeben sich Fragen hinsichtlich der Verantwortlichkeit und Haftung, die weiterer Erörterung bedürfen. Dies ändert aber nichts daran, dass der Verweis auf Zertifikate anderer Zertifizierungsstellen möglich ist, soweit die dort erfolgte Prüfung einer eigenen Prüfung der Zertifizierungsstelle gleichwertig ist.

Wesentliche Grundlage eines Systems modularer Zertifizierung ist damit, dass hinsichtlich der Prüfanforderungen und der Gleichwertigkeit von Prüfungen Transparenz und Rechtssicherheit bestehen.

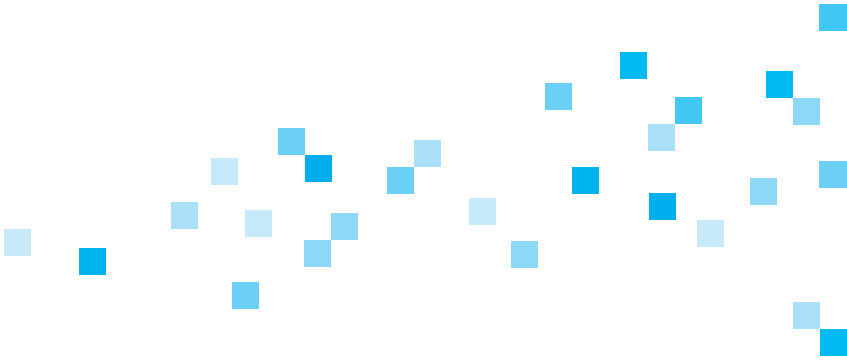
Im der TCDP-Verfahrensordnung ist die Anerkennung von Zertifikaten ausdrücklich geregelt. TCDP-Zertifikate werden danach innerhalb ihres Geltungsbereichs anerkannt. Andere Zertifikate können anerkannt werden, soweit die Gleichwertigkeit der Zertifikate nach Maßgabe der TCDP-Verfahrensordnung festgestellt ist.

2.6 Anwendungsbereich modularer Zertifizierung und Cloud Computing

Die Überlegungen zur modularen Zertifizierung im Datenschutz sind nicht auf Cloud Computing beschränkt, sondern gelten grundsätzlich für alle Datenverarbeitungsdienste.

Die Zertifizierung als solche und ebenso die modulare Zertifizierung ist nicht nur für die Auftragsdatenverarbeitung von Bedeutung. Zwar ist sie hier von besonderem Nutzen, da sie es dem Auftraggeber (Cloud-Nutzer) ermöglicht, auf das Zertifikat zu vertrauen und von einer eigenen Prüfung der technischen und organisatorischen Maßnahmen des Auftragnehmers abzusehen. Die Bedeutung von Zertifizierungen geht aber darüber hinaus. So kann eine Zertifizierung auch für die Zulässigkeit einer Übermittlung von Daten von Bedeutung sein, die etwa bei der Funktionsübertragung vorliegt. Außerdem kann die Zertifizierung für die Haftung des Geschäftsleitungsorgans eines datenverarbeitenden Unternehmens relevant sein, das eine Zertifizierung zur Erfüllung seiner Pflicht zur Überwachung der Rechtmäßigkeit der Datenverarbeitung (Compliance) einsetzt.

Das Konzept einer modularen Zertifizierung ist aber für Cloud Computing besonders relevant, da die Modularisierung des Angebots von Datenverarbeitungsdiensten ein Wesensmerkmal des Cloud Computing als eines auf die Bedürfnisse des Cloud-Nutzers zugeschnittenen, dynamischen Dienstes, der typischerweise gleichwohl aus Standardelementen besteht, ist. Daher wird Cloud Computing zu Recht als primärer Anwendungsfall für die Entwicklung der modularen Zertifizierung angesehen.



3 Der modulare Aufbau von Cloud-Diensten

Die modulare Zertifizierung setzt voraus, dass sich alle Komponenten eines Cloud-Dienstes durch Module beschreiben lassen. Im Folgenden werden die Anforderungen an eine modulare Struktur der sich vertikal, als Bestandteile aufeinander beziehenden Dienste formuliert und eine Abgrenzung zu bestehenden Referenzarchitekturen vorgenommen. Darauf basierend wird ein Vorschlag für eine modulare Struktur der Pilot-Zertifizierung ausgewählter Beispiel-Dienste abgeleitet. Schließlich wird der Vorschlag auf seine Anwendbarkeit hin grob vorgeprüft und betrachtet. Am Ende wird das Fazit formuliert.

3.1 Anforderungen an die vertikale modulare Struktur

Jeder Cloud-Dienst beruht auf mehreren technischen und organisatorischen Bestandteilen, d.h. auf verschiedenen Hard- und Softwarekomponenten sowie verschiedenen Prozessen in verschiedenen Organisationen. Diese lassen sich systematisch in Schichten oder Funktionen aufspalten. Jede Anwendung beruht auf mehreren solcher Funktionsblöcke. Das Zusammenspiel dieser unterschiedlichen Funktionen wird als Architektur bezeichnet, die aus vier verschiedenen Perspektiven betrachtet werden kann:

1. **Die Sicht der Nutzer des Cloud-Dienstes (User-View)**
   Hier stellt sich die Frage, welche Akteure in welchen Rollen wie aktiv sind.
2. **Die funktionale Sicht (Functional View)**
   Hier ist relevant, welche Funktionen zur Bedienung der Aktionen der Nutzer notwendig sind.
3. **Die Implementierungs-Sicht (Implementation View)**
   Hier ist die konkrete technische und organisatorische Umsetzung dieser Funktionen von Interesse.
4. **Die Einsatz-Sicht (Deployment View)**
   Hier ist entscheidend, ob diese Funktionen sich tatsächlich so, wie sie konzeptionell vorgesehen wurden, im Einsatz befinden.

Die Sicht der Nutzer und die funktionale Sicht sind für die Strukturierung des vertikalen Aufbaus der Cloud-Dienste bestimmend. Allerdings ist für die technische und organisatorische Datensicherheit, die zentraler Bestandteil einer Datenschutz-Zertifizierung sein muss, auch und gerade die Implementierungs- und Einsatz-Sicht von zentraler Bedeutung.

→ **Anforderung I**

Für die gesuchte vertikale Struktur ist es nicht hinreichend, die Sicht der Nutzer und die funktionale Sicht zu beschreiben. Für die Zwecke der Zertifizierung ist es erforderlich, insbesondere die Implementierungs- und Einsatz-Sicht zu berücksichtigen.

Nun können Cloud-Dienste, allgemeiner gesprochen, zentral organisierte Datenverarbeitungsdienste, ganz unterschiedlich konzipiert und implementiert sein. Die gesuchte vertikale Struktur muss deshalb so generisch formuliert werden, dass praktisch alle am Markt verfügbaren und heute denkbaren Dienste damit abgebildet werden können. Insbesondere sollen marktübliche

- „Software as a Service"-Dienste (SaaS)
- „Platform as a Service"-Dienste (PaaS)
- „Infrastructure as a Service"-Dienste (IaaS)
- „Hosting"-Dienste und
- „Housing"-Dienste

abgebildet werden können. Außerdem ist damit zu rechnen, dass sich eine Vielzahl von SaaS auch auf andere SaaS beziehen wird. Es ist also des Weiteren zwischen

- SaaS, die sich direkt auf Plattform- und Infrastruktur-Dienste beziehen, und
- SaaS, die auf anderen SaaS-Diensten aufbauen,

zu unterscheiden.

→ **Anforderung II**

Um Allgemeingültigkeit für die gesuchte Struktur zu erlangen, müssen die vertikalen Module zumindest die Gliederung der Funktionen in die marktüblichen Cloud-Dienst-Angebote der Kategorie SaaS, aufeinander aufbauende SaaS, PaaS, IaaS, Hosting und Housing als Bestandteile eines Dienstes zulassen, wie auch beliebige Kombinationen aus diesen Angeboten.

Damit ein Cloud-Dienst als Ganzes aufgrund einer modularen Zertifizierung ein Datenschutz-Zertifikat erhalten kann, ist es erforderlich, dass alle Bestandteile zertifiziert sind. Übertragen auf die vertikale Struktur bedeutet dies, dass alle vertikalen Module geprüft und zertifiziert sein müssen. Daraus ergibt sich schließlich die dritte Anforderung, dass nicht, wie so oft in Architekturen, Schichten mit spezifischen Funktionen neben Blöcken mit übergreifenden Funktionen abgebildet werden, sondern eine vertikale Schichtung mit konjunktiv zu verknüpfenden Funktionseinheiten vorzusehen ist.

→ **Anforderung III**

Für die gesuchte vertikale Struktur soll ein einfacher Stapel an Funktionsblöcken (Modulen) gebildet werden. Funktionen und Anforderungen, die sich in allen Modulen wiederfinden, werden nicht extra ausgewiesen, sondern in den Kriterien, die einer Zertifizierung zu Grunde gelegt werden, gefasst. Daraus resultiert die Anforderung an Cloud-Dienste, dass – ausgehend von einer Funktionsschicht – alle beinhaltenden Funktionen, d.h. alle darunter liegende Module, ebenfalls zertifiziert sein müssen.

Um die gesuchte vertikale Struktur zu bilden, wird auf bekannte Strukturen aus verschiedenen Referenzarchitekturen (NIST und BSI, sowie ISO in Arbeit) für Cloud-Dienste zurückgegriffen.

3.2 Vergleich der Anforderungen mit den Anforderungen an bekannte Referenzarchitekturen

Mit dem Standard ISO/IEC 17789:2014 wurde eine „Cloud Computing Reference Architecture“ (CCRA) für die User- und Funktional-View geschaffen. Sie stellt eine Generalisierung der schon länger verfügbaren NIST- und BSI-Referenzarchitekturen dar, die in den Abbildungen 1a und 1b wiedergegeben sind:

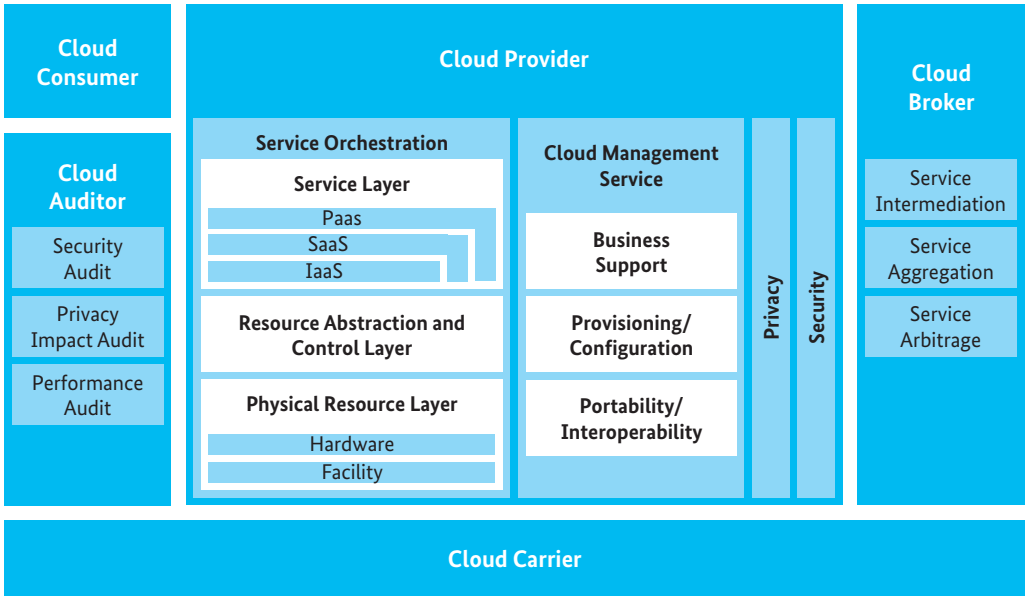


Abbildung 1a: NIST Referenzarchitektur für Cloud-Dienste

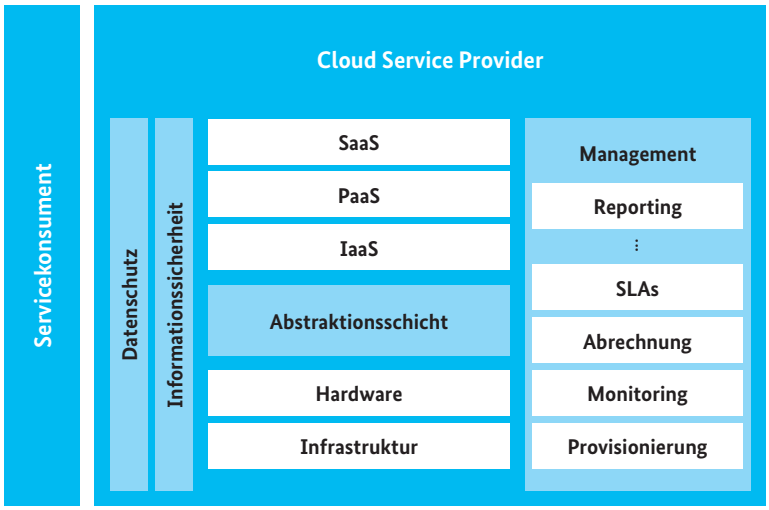


Abbildung 1b: BSI Referenzarchitektur für Cloud-Dienste

Bei beiden Referenzarchitekturen sind neben den vertikal geschichteten Funktionsblöcken, die im Wesentlichen die Rechenzentrum-Infrastruktur, die Hardware, eine Abstraktionsschicht und die bekannten Dienste-Kategorien IaaS, PaaS und SaaS umfassen, übergreifende Funktionen wie Datenschutz und Sicherheit dargestellt. Beide Referenzarchitekturen beschränken sich nicht nur auf die Funktions-Sicht, sondern beinhalten in den Blöcken „Cloud-Consumer“ bzw. Servicekonsument Aspekte der Nutzer-Sicht sowie in den Blöcken Auditor, Management, Broker und Carrier Aspekte der Implementierung und des Einsatzes.

Mit dem im Folgenden dargestellten Vorschlag für die vertikale Struktur wird auf die funktionalen Blöcke dieser Referenzarchitekturen zurückgegriffen, und er werden Anpassungen für die der avisierten Datenschutz-Zertifizierung spezifischen entsprechenden Anforderungen vorgenommen.

3.3 Vorschlag für eine modulare Struktur der Pilot-Zertifizierung ausgewählter Dienste

Um den Anforderungen I bis III gerecht zu werden, wird, wie in Abbildung 2 gezeigt, vorgeschlagen, eine vertikale Schichtung der funktionalen Kernmodule aus den bekannten Referenzarchitekturen zu übernehmen. Allerdings wird jedes dieser Module so interpretiert, dass es als eigenständiger Dienst gemeinsam mit den darunter liegenden Modulen als dessen Bestandteil angeboten werden kann.

Abbildung 2: Einfache vertikale Struktur von Cloud-Diensten

Dazu gehört, dass in jedem dieser Module neben den wiederum vertikal organisierten Grundfunktionen, die übergreifenden Funktionen wie Sicherheit, Datenschutz, Betriebs- und Geschäfts-Unterstützung, die Unterstützung bei Bereitstellung, Entwicklung und Einsatz sowie die organisatorischen Grundlagen enthalten sind.

Diese sind in Anlehnung an ISO/IEC 17789:2014 für eine „Cloud Computing Reference Architecture“ in Abbildung 3 durch vertikal ausgerichtete Felder illustriert. Dabei handelt es sich zwar um übergreifende Funktionen, d.h. Funktionen wie Integration, Datensicherheit, Datenschutz, Betriebs-, Geschäfts-, Entwicklungs- und Einsatz-Unterstützung, die in jedem Modul wiederkehren, aber durchaus in jedem dieser Module unterschiedlich implementiert sein können. Beispielsweise erfordert die Datensicherheit in jedem dieser Module ganz unterschiedliche technische und organisatorische Maßnahmen. Abbildung 3 enthält weiterhin die Differenzierung zwischen für jedes Modul grundsätzlich notwendigen Nutzer-, Zugriffs-, Dienste- und Ressourcen-Schichten.

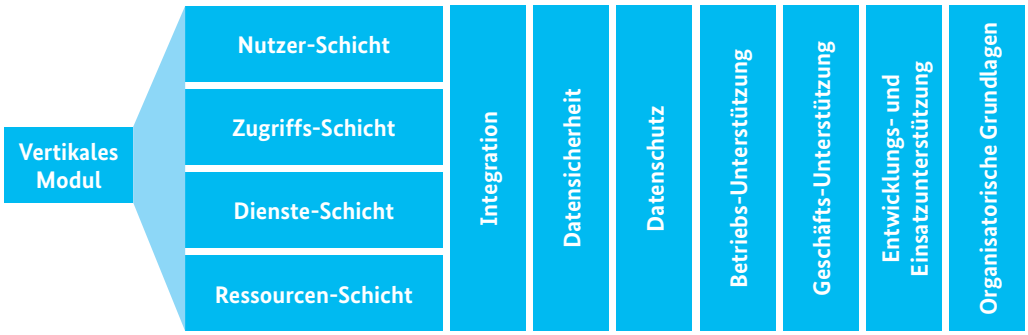


Abbildung 3: Interne Struktur der vertikalen Module

In der in Abbildung 3 detailliert dargestellten inneren Struktur der Module erstrecken sich die datenschutzrechtlichen Anforderungen auf mehrere Säulen, etwa die Datensicherheit und die organisatorischen Grundlagen.

In Abbildung 4 ist eine Erweiterung der Struktur aus Abbildung 2 durch Aufspaltung der obersten und untersten Schicht dargestellt. Je feiner die Module gegliedert werden und umso weniger Funktionen in einem Modul zusammengefasst werden, desto eher können für die Gesamtzertifizierung bestehende Zertifikate wieder- und weiterverwendet werden.

Zum einen ist in Abbildung 4 das Modul „Rechenzentrum- und Netzinfrastruktur“ in ein Modul „Rechenz-Infrastruktur“ und ein Modul „Netz-Infrastruktur“ aufgeteilt, um bestehende Zertifikate betreffend des Informations-Sicherheits-Managements der Rechenzentrums-Infrastruktur, die oft die Netz-Infrastruktur nicht beinhalten, für die Datenschutz-Zertifizierung wiederverwenden zu können.

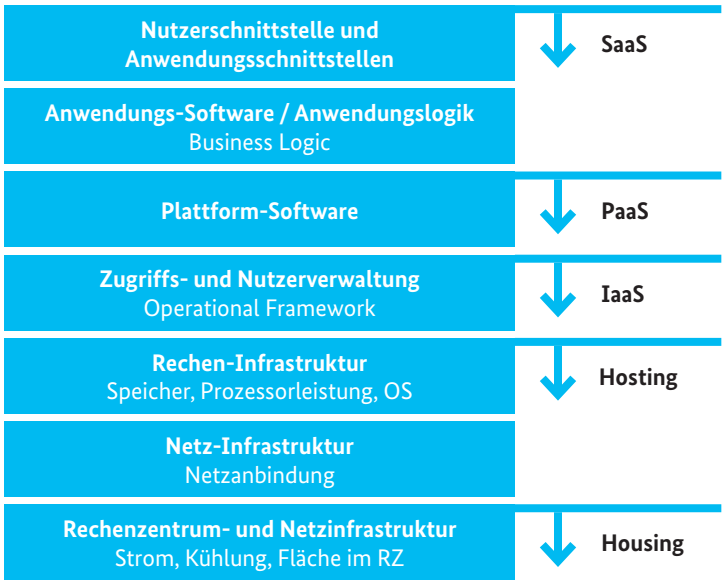


Abbildung 4: Erweiterung der vertikalen Struktur

Zum anderen ist in Abbildung 4 das Modul Anwendungs-Software aus Abbildung 2 in ein Modul Anwendungs-Software/Anwendungslogik (Business Logik) und ein Modul Nutzerschnittstelle und Anwendungsschnittstellen aufgeteilt. In der Praxis beziehen sich sehr häufig SaaS Cloud-Dienste direkt an der Nutzerschnittstelle („graphical user interface“, GUI) auf andere SaaS Cloud-Dienste. Da jedes modulare Zertifizierungsverfahren nicht nur die Einzelmodule separat prüfen darf, sondern auch deren Zusammenspiel bei der Prüfung berücksichtigen muss, ist es sinnvoll die Anwendungslogik als separates Modul

abzuspalten, damit dieses aufwendig zu prüfende Modul nicht bei jeder Kombination eines SaaS mit anderen SaaS erneut in die Prüfung des Zusammenspiels einzubeziehen ist. Die vorgeschlagenen Module insgesamt sind in Abbildung 5 dargestellt.

Abbildung 5: Vollständige vertikale Struktur von Cloud-Diensten

Im Folgenden sei eine Kurzdefinition der Module gegeben.

1. Nutzerschnittstelle und Anwendungsschnittstellen

- Dieses Modul umfasst die Teile der Anwendungssoftware, die die Anwendungsschnittstellen zu den Nutzern (User) oder zu anderen technischen Systemen abbilden.
- Wird als eigenes Modul vorgeschlagen, da eine Fokussierung auf die Kriterien der Zugangskontrolle eine effiziente Zertifizierung nur dieses Moduls und eine Integration verschiedener Dienste modular ermöglicht.

2. Anwendungs-Software/Anwendungslogik (Business Logic)

- Die Teile der Anwendungssoftware, die die Logik der Anwendungsfunktion abbilden.

3. Plattform-Software

- Systeme, die das Betreiben einer Anwendung von der Rechen-Infrastruktur isolieren, indem standardisierte Routinen der Anwendung einheitlich zur Verfügung gestellt werden.
- Wird als eigenes Modul vorgeschlagen, da diese Systeme die Dienste konstituieren, die als PaaS charakterisiert werden.
- Kann in Einzelfällen, in denen keine solche Plattform-Software verwendet wird, trivial sein.

4. Zugriffs- bzw. Nutzerverwaltung (Operational Framework)

- Systeme, die den Zugriff zu Prozessorleistung und Speicher steuern.
- Wird vorgeschlagen, getrennt von der Rechen-Infrastruktur zu führen, da Kriterien deutlich andere Schutzziele betreffen als bei der Rechen-Infrastruktur und da diese Systeme die Dienste konstituieren, die als IaaS charakterisiert werden.

5. Rechen-Infrastruktur

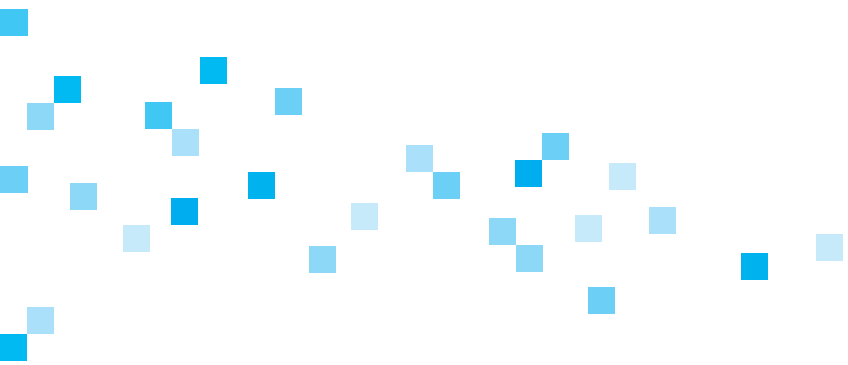
- Die Speicher und Server mit installierten Betriebssystemen

6. Netz-Infrastruktur

- Die Anbindung an das Internet
- Wird als eigenes Modul vorgeschlagen, da in der Praxis Housing sowohl mit als auch ohne Netz-Infrastruktur als Dienst angeboten und zertifiziert wird.

7. Rechenzentrum-Infrastruktur

- Die Fläche, sowie deren Energieversorgung im Rechenzentrum
- Fläche und Stromversorgung sowie Kühlung werden gemeinsam als ein Modul vorgeschlagen, obwohl sie verschiedene Anforderungen betreffen, da in der Praxis diese Leistungen fast immer gemeinsam angeboten werden und um die Zahl der Module klein zu halten. Im Folgenden wird dargestellt, wie sich bekannte Cloud-Dienste in die hier vorgeschlagene vertikale Struktur einfügen lassen.



3.4 Abbildung von Cloud-Diensten in der modularen Struktur

Die Anwendbarkeit der modularen Struktur von Cloud-Diensten ist dann am besten gegeben, wenn die praxisrelevanten Cloud-Dienste-Kategorien auf der Grundlage der modularen Struktur dargestellt werden können.

In Abbildung 6 ist eine Reihe von exemplarischen Cloud-Dienste-Kategorien als Spalten der tabellarischen Darstellung aufgeführt. In den Zeilen sind diejenigen Module dunkelblau markiert, deren Funktionen die Anbieter des Dienstes selber erbringen. Die Module, deren Funktionen von den darunterliegenden Diensten erbracht werden, sind hellblau markiert.

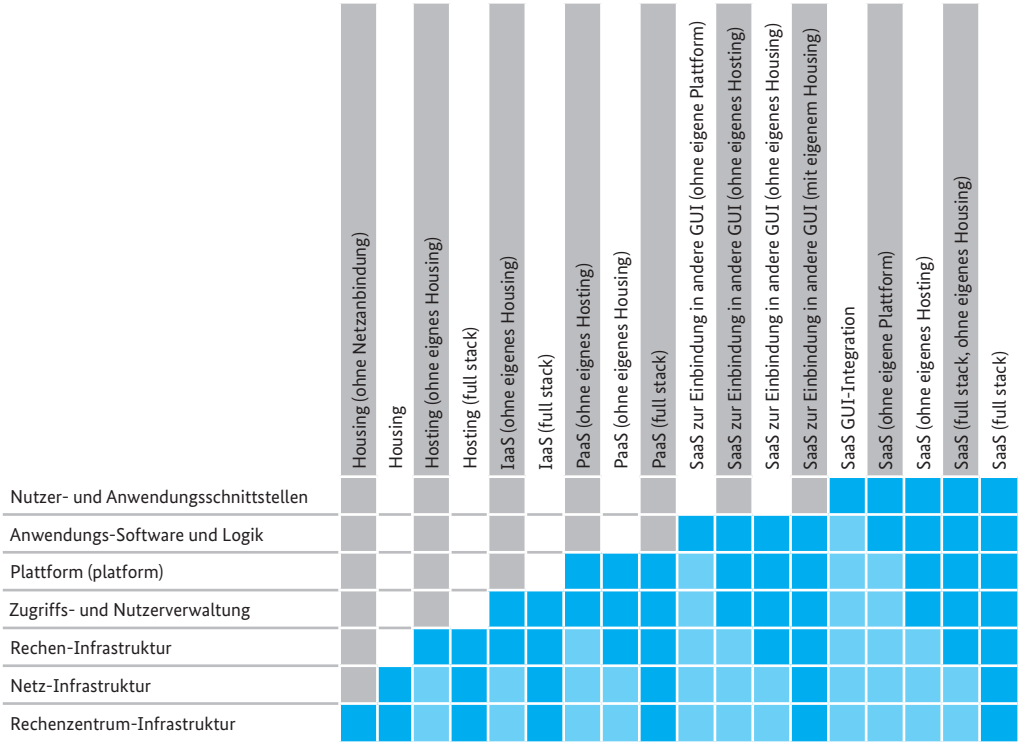


Abbildung 6: Darstellung verschiedener Cloud-Dienste-Kategorien durch vertikale Module.

Die Reihe der Cloud-Dienste-Kategorien ist nicht vollständig und wurde aus Gründen der Übersichtlichkeit auf die praktisch am meisten relevanten Fälle beschränkt. Es ist jedoch ersichtlich, dass mit dieser vertikalen Modularisierung die wesentlichen Kategorien abgebildet werden können. Insbesondere wird deutlich, dass auch Dienste, die auf Vorleistungen anderer Dienste zurückgreifen, durch die modulare Struktur dargestellt werden können.

Bei der Kombination von Diensten kann es vorkommen, dass einzelne Schichten (Module) doppelt vorliegen. Dies ist beispielsweise der Fall, wenn ein „SaaS ohne eigenes Hosting“ auf einem Dienst „IaaS full stack“ aufsetzt. In diesem Fall enthalten beide Dienste die Funktion (Modul) „Zugriffs- und Nutzerverwaltung“.

4 Zusammenfassung

Das Ziel, eine kostengünstige und effiziente datenschutzrechtliche Zertifizierung für Cloud-Dienste zu ermöglichen, kann durch ein System einer modularen Zertifizierung erreicht werden, das sowohl eine horizontale wie eine vertikale Einbeziehung vorangegangener Zertifizierungen erlaubt. Durch die Einbeziehung wird eine erneute Prüfung der bereits zertifizierten Elemente grundsätzlich entbehrlich.

Die horizontale Modularisierung der Zertifizierung ermöglicht es, auf der Anwendungsebene ein Zertifikat für eine Mehrheit von Modulen (Anwendungen) in der Weise zu erstellen, dass bestehende Zertifikate für einzelne Module durch Bezugnahme in die Zertifizierung einbezogen werden. Die vertikale Modularisierung der Zertifizierung ermöglicht es, bei der Zertifizierung einer einzelnen Anwendung auf bestehende Zertifikate für die verschiedenen technischen und organisatorischen Komponenten zu verweisen und diese in die Zertifizierung einzubeziehen.

Die modulare Prüfung und Zertifizierung kann der einheitlichen, separaten Zertifizierung eines Diensteangebots gleichwertig sein, soweit die modulare Zertifizierung alle Merkmale der erforderlichen Prüfung und Zertifizierung umfasst und die Prüfung und Zertifizierung auch qualitativ gleichwertig ist.

Die modulare Zertifizierung setzt insbesondere in Bezug auf die vertikale Modularisierung eine Beschreibung des modularen Aufbaus von Cloud-Diensten voraus. Die vorgestellte vertikale modulare Struktur zur Beschreibung von Cloud-Diensten orientiert sich an bestehenden und sich in Vorbereitung befindlichen Standards und ist allgemein anwendbar, das heißt sie kann mindestens auf die Mehrzahl, wahrscheinlich auf alle Cloud-Dienste angewendet werden. Der linear geschichtete Aufbau verdeutlicht, dass alle Cloud-Angebote sich jeweils auf alle „darunter liegenden“ Module beziehen.

Die vertikale, modulare Struktur ermöglicht es, unterschiedliche Anforderungen an die verschiedenen Funktionen (Module) von Cloud-Diensten unterschiedlichen Modulen zuzuordnen. Auf dieser Grundlage kann die modulare Zertifizierung auch bei komplexen, aus mehreren Modulen mit unterschiedlichen Anforderungen zusammengesetzten Diensten durchgeführt werden. Weiterhin wird die modulare Zertifizierung auch dann möglich, wenn der Anbieter des Cloud-Dienstes einen zugrunde liegenden Dienst eines anderen Anbieters in seinen Dienst einbezieht.

Die TCDP-Zertifizierung beruht auf dem Konzept der modularen Zertifizierung. Die Voraussetzungen der modularen Zertifizierung, insbesondere die Anerkennung zugrunde liegender Zertifikate, erfolgt nach Maßgabe der TCDP-Verfahrensordnung unter den dort geregelten Voraussetzungen.

Beteiligte des Pilotprojekts

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Bird & Bird LLP

Bitkom Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Prof. Dr. Georg Borges

Deutsche Telekom AG

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg

DIN Deutsches Institut für Normung e. V.

ecsec GmbH

EuroCloud Deutschland_eco e.V.

Europäische EDV-Akademie des Rechts gGmbH

Landesbeauftragte für Datenschutz und
Informationsfreiheit Nordrhein-Westfalen

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft

regio iT gesellschaft für informationstechnologie mbh

SAP SE

Stiftung Datenschutz

TÜV Informationstechnik GmbH

TÜV SÜD Sec-IT GmbH

Unabhängiges Datenschutzzentrum Saarland

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Uniscon GmbH

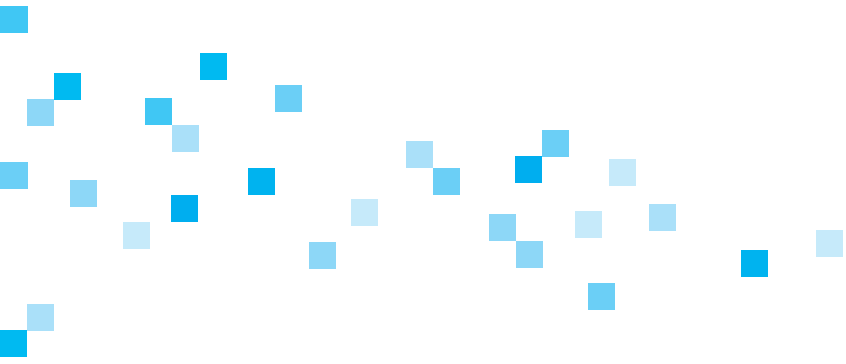
VOICE Bundesverband der IT-Anwender e.V.

Beobachtende Teilnehmer

Bayerisches Landesamt für Datenschutzaufsicht

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesministerium des Innern



Impressum

Herausgeber
Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
E-Mail: info@tcdp.de
www.tcdp.de

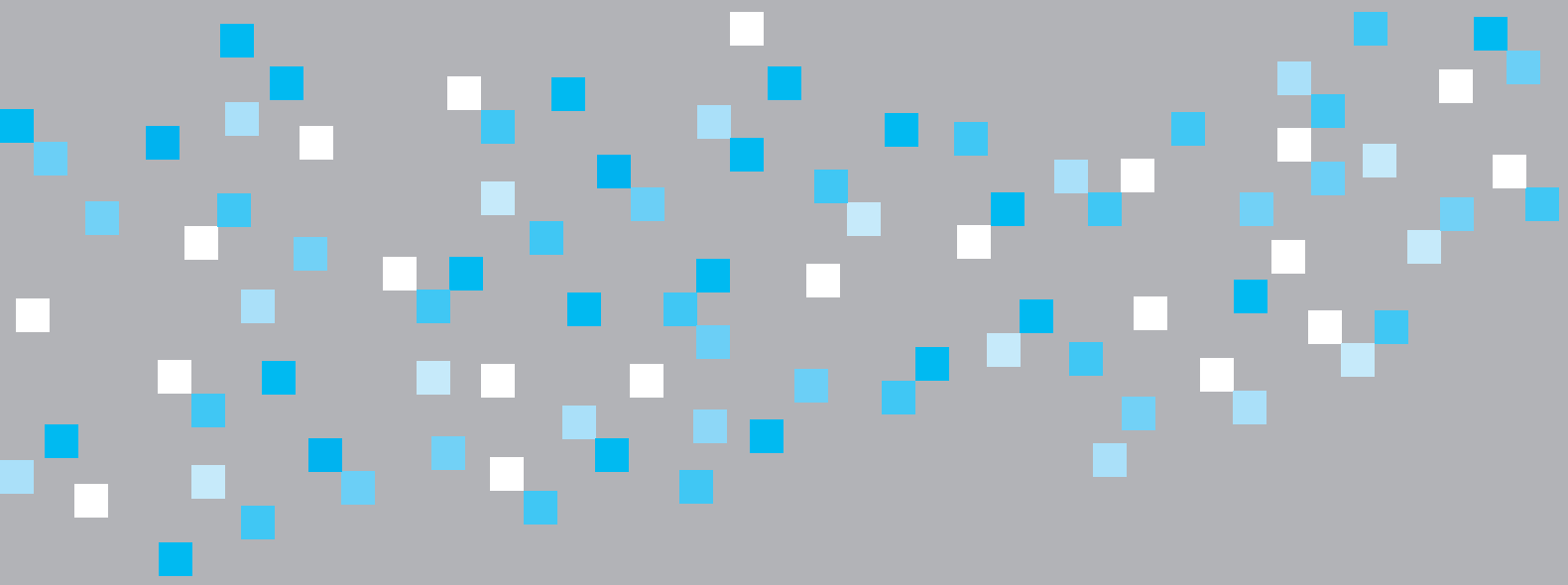
Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Satz
Christoph Engling

Druck
Ortmeier Medien GmbH, Saerbeck

Stand: September 2016



www.tcdp.de