Trusted Cloud

Kompetenzzentrum Trusted Cloud

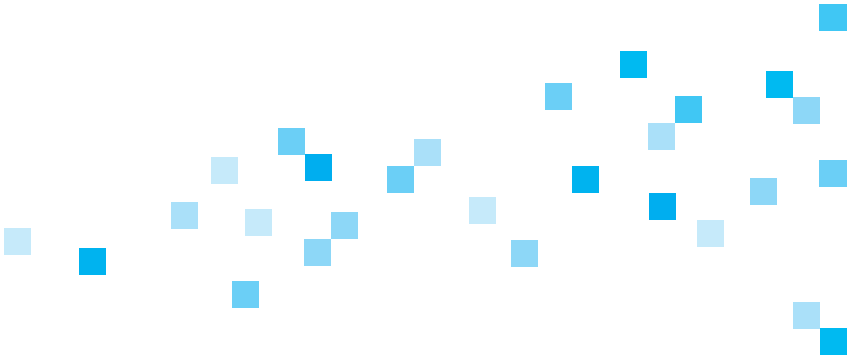
Arbeitspapier – Modulare Zertifizierung von Cloud-Diensten

Nr. 4

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“

Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das Bundesministerium für Wirtschaft und Energie (BMWi) daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen.

In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Sie wird geleitet von Prof. Dr. Georg Borges. Themenschwerpunkte sind u. a. Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten durchgeführt, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.

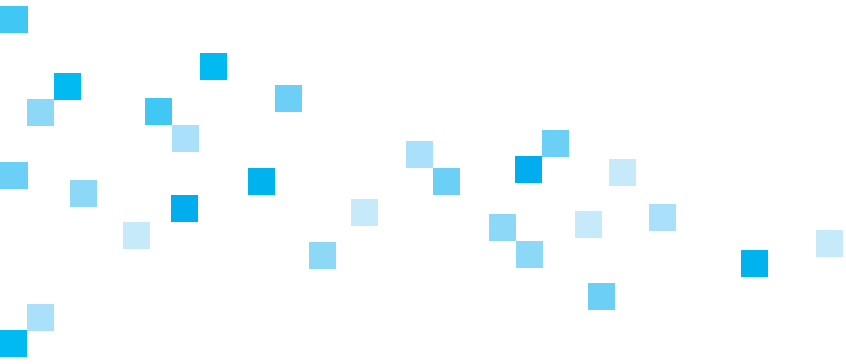


Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Herausforderung: Effizienter Datenschutz im Cloud Computing
Bei der Nutzung von Cloud-Computing-Diensten muss ein hinreichender Datenschutz gewährleistet sein, der sich im Rahmen der Auftragsdatenverarbeitung auch auf die Sicherheit der Datenverarbeitung beim Cloud-Anbieter erstreckt. Daher müssen die technischen und organisatorischen Maßnahmen des Cloud-Anbieters überprüft werden. Eine Überprüfung der technischen Systeme des Cloud-Anbieters durch jeden Cloud-Nutzer wäre jedoch kaum praktikabel und würde zu weit überhöhten Kosten führen. Viele Unternehmen, die Cloud-Dienste nutzen möchten, können diese nicht aus eigener Kraft durchführen.

Lösung: Datenschutz-Zertifizierung für Cloud-Dienste
Diese Schwierigkeiten können durch ein geeignetes Zertifizierungsverfahren überwunden werden, das alle datenschutzrechtlichen Anforderungen an den Auftragsdatenverarbeiter im Cloud Computing umfasst. Dabei werden die technischen Maßnahmen des Cloud-Anbieters von einer fachlich geeigneten und unabhängigen Zertifizierungsstelle überprüft. Das Ergebnis der Prüfung kommt allen Cloud-Nutzern zugute. Mit dieser Zertifizierung kann sowohl ein hohes Datenschutzniveau gewährleistet als auch eine effiziente Grundlage für die Nutzung von Cloud-Diensten geschaffen werden.

Ziel des Pilotprojekts
Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum Trusted Cloud hat im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) ein Konzept für ein solches Zertifizierungsverfahren ausgearbeitet. Dies ist in ihrem rechtspolitischen Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“ von Oktober 2012 dokumentiert. Im Rahmen des Pilotprojekts „Datenschutz-Zertifizierung für Cloud-Dienste“ werden auf der Grundlage dieses Konzepts die Einzelheiten einer datenschutzrechtlichen Zertifizierung von Cloud-Diensten erarbeitet und exemplarisch wird eine Zertifizierung einzelner geeigneter Cloud-Dienste durchgeführt werden.



Inhaltsverzeichnis

1	Ziele und Herausforderungen der Zertifizierung von Cloud-Diensten	8
2	Lösungsvorschlag: Effiziente und kostengünstige Zertifizierung durch modulare Zertifizierung	11
3	Horizontal modulare Zertifizierung	12
4	Vertikal modulare Zertifizierung	13
5	Gleichwertigkeit der modularen Zertifizierung	14
6	Elemente und Herausforderungen eines Systems modularer Zertifizierung	15
7	Anwendungsbereiche modularer Zertifizierung und Cloud Computing	17
8	Ergebnis	18
Autoren		18

1 Ziele und Herausforderungen der Zertifizierung von Cloud-Diensten

Ziel der Zertifizierung und Stand der Diskussion

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 der Cloud-Nutzer (derjenige, für den der Cloud-Dienst erbracht wird) 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 ein geeignetes Zertifizierungsverfahren überwunden werden, das alle datenschutzrechtlichen Anforderungen an den Auftragsdatenverarbeiter im Cloud Computing umfasst. 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 kann sowohl ein hohes Datenschutzniveau gewährleistet als auch eine effiziente Grundlage für die Nutzung von Cloud-Diensten geschaffen werden.

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ hat ein Konzept für ein solches Zertifizierungsverfahren vorgelegt und eine gesetzliche Regelung der Zertifizierung im europäischen Datenschutzrecht gefordert, um gleiche Zertifizierungsstandards im europäischen Binnenmarkt zu erreichen (AG Rechtsrahmen des Cloud Computing: Datenschutzrechtliche Lösungen für Cloud Computing, Okt. 2012). Ein entsprechender Gesetzgebungsvorschlag wurde erarbeitet.

Auch andere Initiativen, etwa der Standard „Anforderungen an Auftragnehmer nach § 11 BDSG“ der Gesellschaft für Datenschutz und Datensicherheit e.V. und des Berufsverbands der Datenschutzbeauftragten Deutschlands e.V. beruhen, allerdings auf der Grundlage des BDSG, auf dem Grundgedanken der Zertifizierung als einer effizienten Lösung zur Gewährleistung des Überprüfungserfordernisses in der Auftragsdatenverarbeitung.

Der von der EU-Kommission vorgelegte Entwurf einer Datenschutz-Grundverordnung enthält in seinem Art. 39 eine normative Grundlage für eine solche datenschutzrechtliche Zertifizierung. Der Änderungsvorschlag des LIBE-Ausschusses des Europäischen Parlaments zu Art. 39 ist mit diesem Ziel vereinbar. Ein im Ministerrat erarbeiteter Entwurf zu Art. 39 und einem neuen Art. 39a enthält sogar wesentliche Elemente des von der AG Rechtsrahmen vorgelegten Konzepts.

Mit dem Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ des Kompetenzzentrums Trusted Cloud soll das Konzept der AG Rechtsrahmen des Cloud Computing zur Datenschutz-Zertifizierung weiter ausgearbeitet und prototypisch an ausgewählten Beispielen durchgeführt werden.

Das im Thesenpapier der AG Rechtsrahmen „Datenschutzrechtliche Lösungen für Cloud Computing“ entwickelte Konzept mit den dort beschriebenen Voraussetzungen und Wirkungen der Zertifizierung werden den nachfolgenden Überlegungen zugrunde gelegt.

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 ggf. künftig Art. 26 Datenschutz-Grundverordnung, Gegenstand der Prüfung durch den Cloud-Nutzer als Auftraggeber sind. Im Vordergrund stehen Maßnahmen zum Schutz gegen unbefugte Datenverarbeitung.

Effizienz als eine zentrale Herausforderung einer Zertifizierung

Ein Zertifizierungsverfahren, das das genannte Ziel – Entbehrlichkeit einer eigenen Überprüfung der Maßnahmen durch Vertrauen auf ein Zertifikat – erreichen soll, hat etliche Herausforderungen zu meistern. So müssen etwa Prüfanforderungen und das Verfahren der Zertifizierung festgelegt werden, Zuständigkeiten und Verantwortlichkeiten geklärt werden. Nach dem Konzept der AG Rechtsrahmen des Cloud Computing sollten diese Aspekte künftig gesetzlich geregelt werden, um eine rechtssichere Grundlage für die Zertifizierung und die Verlässlichkeit der Zertifikate zu schaffen.

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. Zu Recht fordert das Europäische Parlament in seinen Änderungsvorschlägen (Art. 39 Abs. 1b neu) zum Entwurf der Datenschutz-Grundverordnung „erschwingliche“ Zertifizierungen.

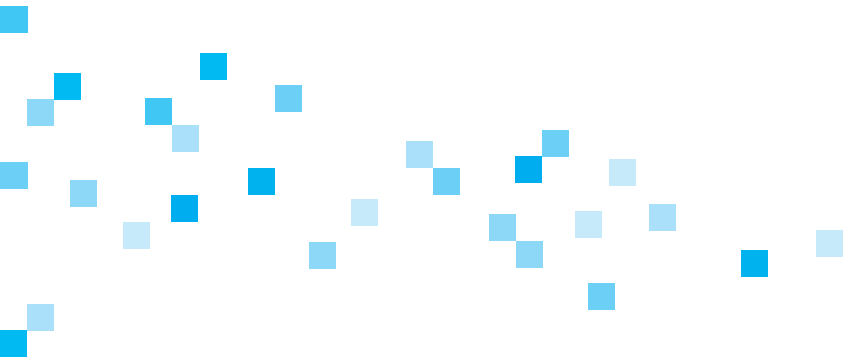
Ein wesentliches strukturelles Problem für kostengünstige Prüfung und Zertifizierung, nicht zuletzt beim Cloud Computing, ergibt sich aus dem Gegenstand der Zertifizierung, der sich auf die vom Cloud-Nutzer in Anspruch genommene Leistung beziehen muss.

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.

Für die Zertifizierung führt der Umstand, dass Cloud-Anbieter ihren Kunden zahlreiche unterschiedliche Varianten von Diensten anbieten, 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.

Sollte nun jedes einzelne dieser Dienstepakete einer separaten Prüfung bedürfen, müsste der Anbieter für jedes dieser Pakete die gesamten Kosten für Prüfung und Zertifizierung erneut aufbringen. Dies würde es Cloud-Anbietern wesentlich erschweren, neue Produkte anzubieten. Vor allem wäre dieses Vorgehen ineffizient, da die einzelnen Bestandteile der Dienstepakete 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 Lösungsvorschlag: 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 zugute kommen.

Entsprechendes muss innerhalb der Zertifizierung gelten: Die technischen und organisatorischen Maßnahmen sollten nur einmal geprüft werden, und diese Prüfung sollte allen Einsatzbereichen zugute kommen, 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 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.

3 Horizontal modulare Zertifizierung

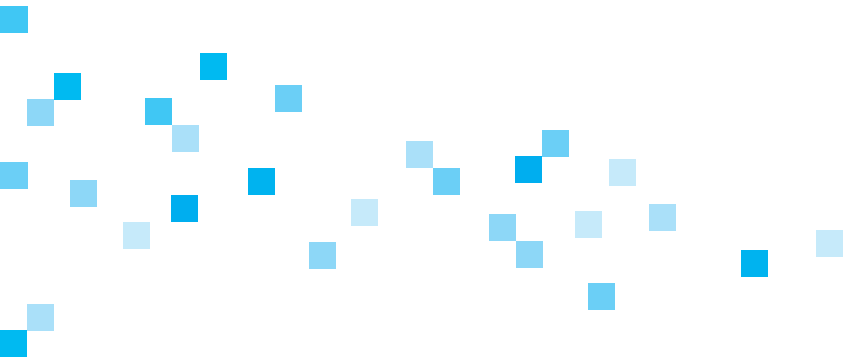
Horizontale Modularisierung von Datenverarbeitungsdiensten

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 Dienstepaketen 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.

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 kleine Unternehmen angeboten wird.



4 Vertikal modulare Zertifizierung

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.

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 auf einem physischen Server mehrere Anwendungen oder gar virtuelle Systeme betrieben werden.

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 verschiedener 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.

5 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.

6 Elemente und Herausforderungen eines Systems modularer Zertifizierung

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 können durch dieselbe Person erfolgen, können aber auch organisatorisch und rechtlich getrennt sein.

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 Dienstangebots 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.

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.

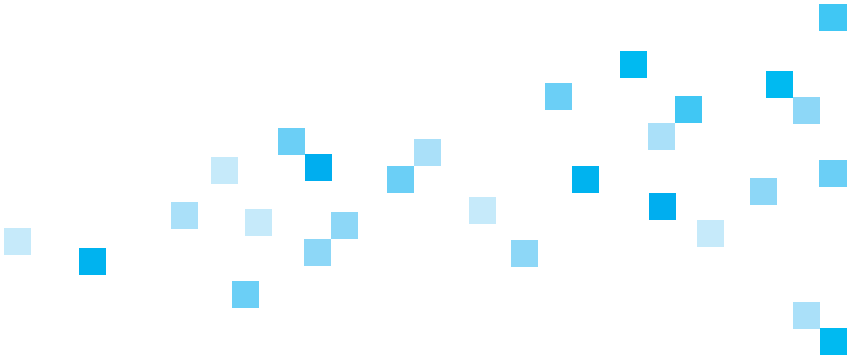
Wesentliche Grundlage eines Systems modularer Zertifizierung ist damit, dass hinsichtlich der Prüfanforderungen und der Gleichwertigkeit von Prüfungen Transparenz und Rechtssicherheit bestehen.

7 Anwendungsbereiche 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.



8 Ergebnis

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.

Autoren

Oliver Berthold, Berliner Beauftragter für Datenschutz und Informationsfreiheit

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud

Mathias Cellarius, SAP AG

Susanne Dehmel, BITKOM

Thomas Doms, TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria

Impressum

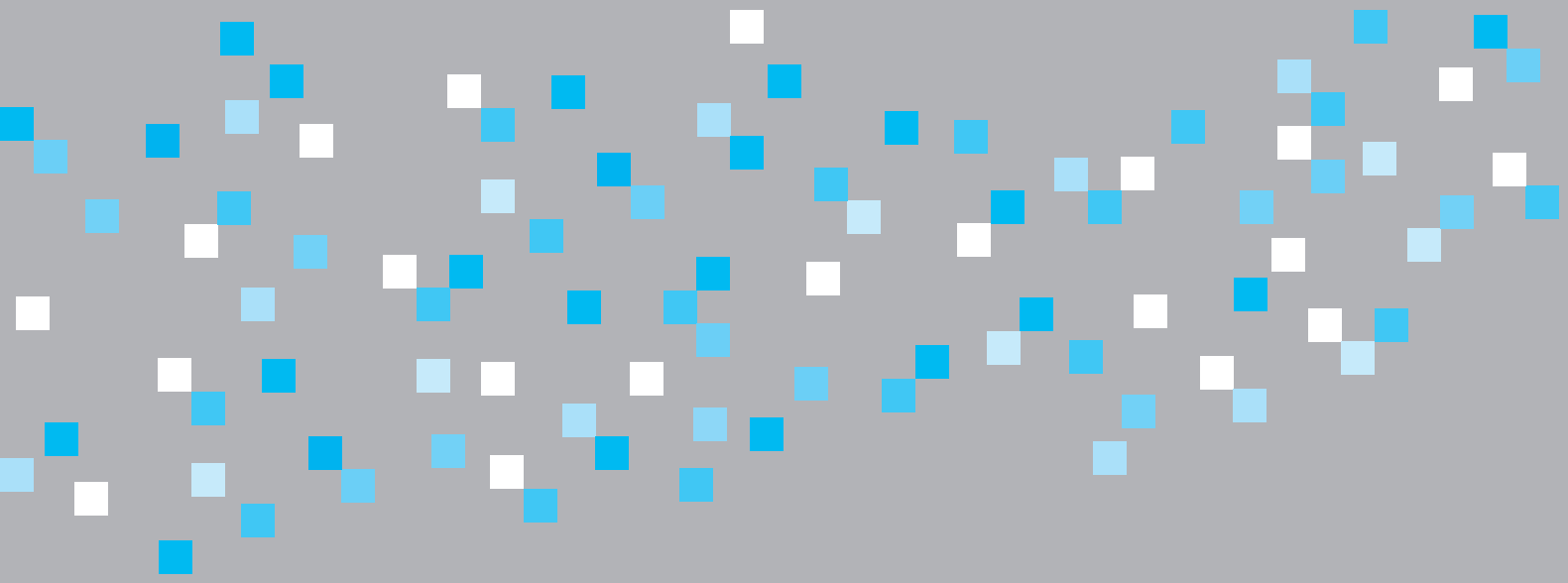
Herausgeber
Kompetenzzentrum Trusted Cloud
Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: März 2014



www.trusted-cloud.de