Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

# Trusted Clouds für die digitale Transformation in der Wirtschaft

Teil 2: Regelwerk für die Nutzung des Labels „Trusted Cloud“

2

# Impressum

**Herausgeber**
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

**Text und Redaktion**
Kompetenzzentrum Trusted Cloud

**Gestaltung**
A&B One Kommunikationsagentur, Berlin

**Stand**
Februar 2015

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit vom Bundesministerium für Bildung und Forschung unentgeltlich abgegeben. Sie ist nicht zum gewerblichen Vertrieb bestimmt. Sie darf weder von Parteien noch von Wahlwerberinnen/Wahlwerbern oder Wahlhelferinnen/Wahlhelfern während eines Wahlkampfes zum Zweck der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament. Missbräuchlich sind insbesondere die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zweck der Wahlwerbung. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift der Empfängerin/dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Bundesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.

# Inhaltsverzeichnis

**Regelwerk für die Nutzung des Labels „Trusted Cloud“ – Leitfaden** 7

Trusted-Cloud-Referenzmodell 8

Das Label „Trusted Cloud“ 12

Funktionsanalyse 14

Spezifikation von Funktionalitäten 18

Transformation und Transformationsmanagement 20

**Cloud-Sicherheits-Leitfaden für Anbieter (CSLA)** **23**

**Zusammenfassung** **25**

**1 Einleitung zum Cloud-Sicherheits-Leitfaden für Anbieter (CSLA)** **26**
1.1 Bedeutung von Informationssicherheit im Zusammenhang mit Cloud Computing 26
1.2 Aufbau und Funktion des CSLA 27
1.3 Ein offenes Wort – Limitationen des CSLA 28

**2 Was steht eigentlich auf dem Spiel?** **29**
2.1 Identifizieren der Stakeholder 29
2.2 Analysieren der Werte 30

**3 Welche Bedrohungen sind zu beachten?** **32**
3.1 Bedrohungen durch die Cloud-Plattform 32
3.2 Allgemeine Bedrohungen von IKT-Systemen 34
3.3 Gefährdungen der Kommunikation und des Zusammenspiels 35
3.4 Rechtliche Gefahren 36

**4 Welche Risiken ergeben sich daraus?** **37**
4.1 Mögliche Auswirkungen der Bedrohungen auf die Werte analysieren 37
4.2 Welche Sicherheitsmaßnahmen sind erforderlich? 38

**5 Vertrauen schaffen** **39**
5.1 Schritte planen 39
5.2 Sicherheitsmaßnahmen implementieren 40
5.3 Prüfen und prüfen lassen 41
5.4 Kommunizieren 42

**6 Weiterführende Literatur** **44**
6.1 IT-Sicherheit 44
6.2 Risikoanalyse 44
6.3 Rechtliche Grundlagen 44
6.4 IT allgemein 44

**Cloud-Sicherheits-Leitfaden für Nutzer (CSLN) 45**

**Zusammenfassung 47**

**1 Einleitung zum Cloud-Sicherheits-Leitfaden für Nutzer CSLN 48**
1.1 Bedeutung von Informationssicherheit im Zusammenhang mit Cloud Computing 48
1.2 Aufbau und Funktion des CSLN 49
1.3 Ein offenes Wort – Limitationen des CSLN 50

**2 Was steht eigentlich auf dem Spiel? 51**
2.1 Identifizieren der Stakeholder 51
2.2 Analysieren der Werte 52

**3 Welche Bedrohungen sind zu beachten? 54**
3.1 Bedrohungen durch einen externen Cloud-Dienst und dessen Anbieter 54
3.2 Bedrohungen von IKT-Systemen 58
3.3 Gefährdungen der Kommunikation und des Zusammenspiels 59
3.4 Gefährdungen aufseiten der Nutzer 60

**4 Welche Risiken ergeben sich daraus? 61**
4.1 Mögliche Auswirkungen der Bedrohungen auf die Werte analysieren 61
4.2 Welche Sicherheitsmaßnahmen sind erforderlich? 62

**5 Cloud-Dienste bewerten, vergleichen, auswählen und nutzen 63**
5.1 Dienste evaluieren anhand der implementierten Sicherheitsmaßnahmen 63
5.2 Passendste Dienste finden 64
5.3 Nutzung der Cloud-Dienste 65

**6 Weiterführende Literatur 66**
6.1 IT-Sicherheit 66
6.2 Risikoanalyse 66
6.3 Rechtliche Grundlagen 66
6.4 IT allgemein 66

**Anhang A – Bedrohungen mit Konsequenzstufen und passenden Sicherheitsmaßnahmen 67**

**Anhang B – Sicherheitsmaßnahmen mit Schutzlevel 72**

**Anhang C – Definitionen und Erläuterungen 77**

**Anhang D – Bausteine für die Sicherheitsmaßnahmen 79**

**Datenschutz-Zertifizierung durch private Stellen** 87

**Die Bedeutung der datenschutzrechtlichen Compliance-Zertifizierung** 89
Bedarf an einer datenschutzrechtlichen Compliance-Zertifizierung 89
Gegenstand der datenschutzrechtlichen Compliance-Zertifizierung 89

**Zertifizierung durch Behörden oder private Stellen?** 90

**Rechtliche Grundlagen der datenschutzrechtlichen Compliance-Zertifizierung** 91

**Datenschutz-Zertifizierung im Entwurf der Datenschutz-Grundverordnung** 92

**Gründe für eine Zertifizierung durch Aufsichtsbehörden oder private Stellen** 93
Zertifizierung als Aufgabe der Aufsichtsbehörden 93
Zertifizierung als Aufgabe privater Stellen 94
Keine Beschränkung der Compliance-Zertifizierung auf Aufsichtsbehörden 95

**Schlussfolgerungen** 96

**Anhang** 97

**Schweigepflicht bei der Auslagerung von IT-Dienstleistungen** 105

**Einführung** 107

**1 Zunehmende Inanspruchnahme von externen IT-Dienstleistern durch Berufsgeheimnisträger** 108

**2 Datenschutzrechtliche Vorgaben bezüglich der Einschaltung von externen Dienstleistern** 109

**3 Strafbarkeitsrisiko bei der Einschaltung von externen Dienstleistern** 110

**4 Exemplarische Darstellung von Fallkonstellationen im Bereich von IT-Dienstleistungen** 111
Wartung durch externe Dienstleister 111
Cloud Storage-Dienste 112
Konfliktprüfungen 113
Cloud-Lösungen für medizinische Versorgung und Forschung 114

**5 De lege lata keine rechtssicheren Lösungen möglich** 116

**6 Große Bedeutung für die Praxis** 117

**7 Notwendigkeit einer Gesetzesänderung** 118

**8 Potenzielle Lösungsansätze im Rahmen einer Gesetzesänderung** 119
Gesetzliche Änderung des Gehilfenbegriffs 119
Bezugnahme zur datenschutzrechtlichen Auftragsdatenverarbeitung 120
Erlaubnis in Berufsgesetzen 121
Konkretisierung des Offenbarungsbegriffs 121

**Fazit** 122

# Regelwerk für die Nutzung des Labels „Trusted Cloud“

Leitfaden

# Trusted-Cloud-Referenzmodell

Der Begriff „Trust“ ist im Englischen genauso wie der Begriff „Vertrauen“ mit vielen Bedeutungen belegt und gibt demzufolge Anlass für unterschiedliche Deutungen. Für die Nutzung des Begriffs „Trust“ im Zusammenhang mit Cloud-Angeboten ist deshalb eine Festlegung der mit dem Begriff gemeinten Bedeutungen nötig. Diese Festlegung erfolgt zunächst durch die Einführung einer Reihe von Unterbegriffen zum Begriff „Trust“, mit denen unterschiedliche Dimensionen für seine Bedeutung festgelegt werden.

**Funktionalität**
Der Begriff „Funktionalität“ bezeichnet die Leistungen, die von einem Cloud-Angebot erbracht werden. Dies sind zuallererst die „Dienste“, die aus einer Cloud zum Abruf bereitgestellt werden. Dienste von Clouds sind grob kategorisiert als:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Für jede dieser Kategorien sind jeweils Klassen von Diensten angebbar, sodass mit der Kategorisierung und Klassifikation die Leistungen schrittweise in ihre Teilleistungen zerlegt dargestellt werden können und mit diesen Verfeinerungen auch die Verfeinerung der Bedeutung der Dienste angegeben werden kann.

Die Funktionalität eines Cloud-Angebots ist die erste und wichtigste Dimension zur Charakterisierung der Vertrauenswürdigkeit von Cloud-Angeboten, weil mit ihr die Leistung des Cloud-Angebots so beschrieben werden kann, dass ein potenzieller Nutzer Gewissheit darüber erlangen kann, dass die von ihm benötigte Leistung auch tatsächlich erbracht wird.

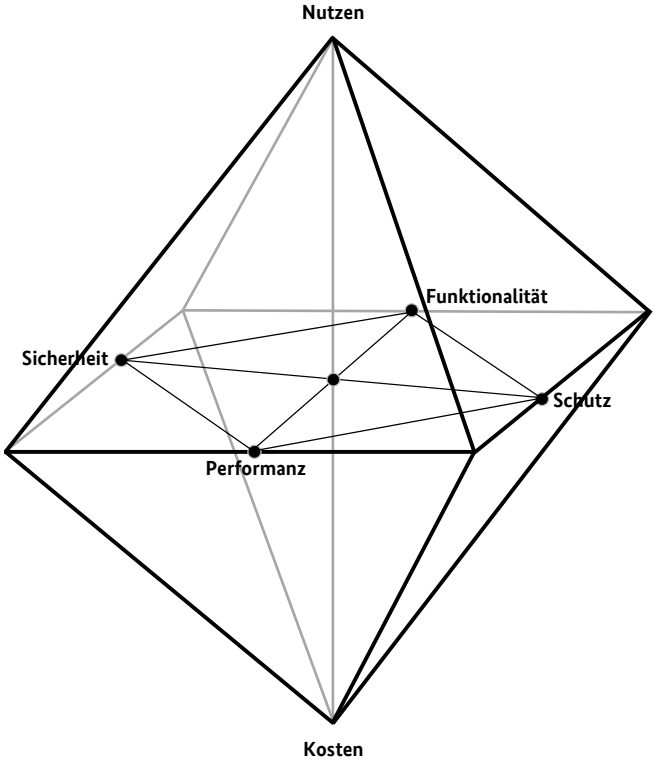
**Sicherheit**
Der Begriff „Sicherheit“ ist der mit den in den Informationstechnologien üblicherweise zugeordneten Bedeutungen. Er bezeichnet die Sicherheit aller Systeme und Infrastrukturen der Informationstechnologie sowohl im Hinblick auf alle von außen wirkenden Bedrohungen der gewünschten Funktionsweise der Systeme und der Infrastruktur als auch im Hinblick auf alle in den Systemen und in der Infrastruktur begründeten Fehlfunktionen. Vertrauen wird in ganz außerordentlicher Weise durch Sicherheit ermöglicht.

**Datenschutz**
Datenschutz bezeichnet alle gesetzlichen Regelungen, mit denen sichergestellt werden soll, dass mit personenbezogenen Daten keine unerlaubten Nutzungen möglich werden. Neben den aus gesetzlichen Regelungen ableitbaren Anforderungen an Cloud-Angebote sind auch solche von Bedeutung, die zwar nicht personenbezogen, aber dennoch von hoher Werthaltigkeit sind und deren Nutzung demzufolge nicht anderen als den dazu Autorisierten gestattet wird. Wie Sicherheit ist Datenschutz in hohem Maße für die Vertrauensbildung nötig.

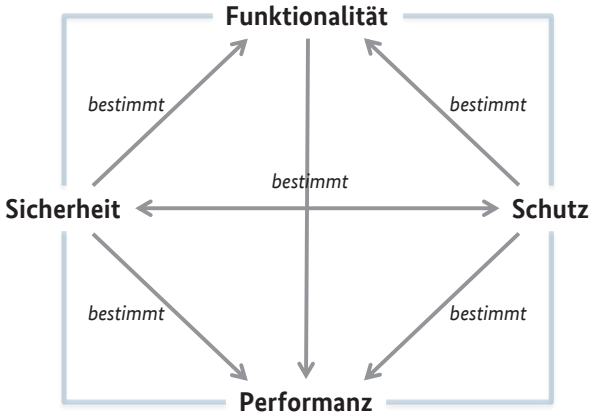
**Performanz**
Die mit Cloud-Angeboten verbundenen Leistungsangebote werden in aller Regel im Rahmen von Vorgaben für den Zeitpunkt oder Zeitraum, in dem die Leistung nach deren Anforderung erbracht werden muss, erwartet. Werden diese Zeitvorgaben nicht eingehalten, können nicht nur Verzögerungen allgemeiner Art, sondern auch „kritische", wie z. B. „geschäftskritische" oder „funktionskritische" Verzögerungen eintreten. Vertrauen entsteht in Cloud-Angeboten, wenn die zugesagten Vorgaben garantiert und eingehalten werden können.

**Kosten und Nutzen**
Die Belegung des Begriffs „Vertrauen" erfolgt in einem ökonomischen Sinn in der Regel durch die Begriffe „Kosten" und „Nutzen". Weder Kosten noch Nutzen sind immer leicht zu bestimmen, auch wenn sorgfältige Kostenplanungen und Nutzenplanungen der Nutzung von Cloud-Angeboten vorausgehen.

Kosten und Nutzen unterscheiden sich von den anderen Dimensionen auch noch insofern, als die anderen Dimensionen immer in Systemen und Infrastrukturen durch eine „System Analytics" oder „Program Analytics" auf ihre „Implementierung" in den jeweiligen Systemen hin überprüft werden können.



Die vorgenannten Dimensionen für die Beurteilung von Trusted Clouds sind – wie die Grafik zeigen soll – voneinander abhängig. Nicht nur macht die Grafik deutlich, dass Anforderungen an Sicherheit und Datenschutz sowie an Performanz die Funktionalität beeinflussen und bestimmen und dass die Funktionalität den Grad an Sicherheit, Datenschutz und die Performanz festlegt, sondern sie veranschaulicht auch, dass die Anforderungen an Datensicherheit und Datenschutz die Performanz beeinflussen und bestimmen, dass Datensicherheit und Datenschutz sich gegenseitig beeinflussen und bestimmen und dass letztlich Funktionalität, Sicherheit, Datenschutz und Performanz Kosten und Nutzen beeinflussen und bestimmen.



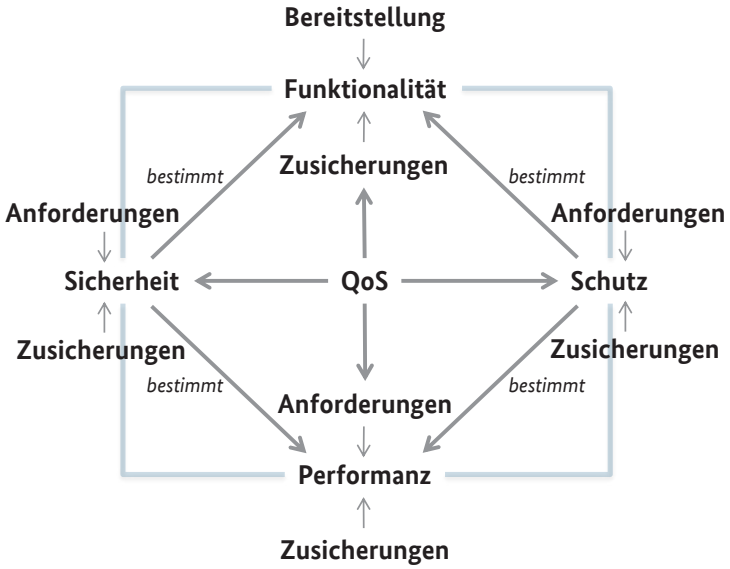

Für dieses Referenzmodell für „Trusted Clouds“ gilt zunächst nur, dass es eine qualitative Charakterisierung des Begriffs „Trust“ für das Label „Trusted Cloud“ darstellt. Eine quantitative Bewertung erfordert entsprechende Überprüfungen durch die „Vermessung“ der jeweiligen Systeme im Rahmen einer Code-Analyse.

Das Referenzmodell für Trusted Clouds legt also fest, welche Dimensionen der Beurteilung von essenzieller Bedeutung sind. Anhand von Angaben über Cloud-Angebote entlang dieser Dimensionen wird deutlich gemacht, welcher „Grad an Transparenz“ mit den Beurteilungen hergestellt wird. Vertrauen wird dann in Abhängigkeit von der Berücksichtigung dieser Dimensionen in der Beurteilung von Cloud-Angeboten und in Abhängigkeit von der Tiefe der jeweiligen Beurteilungen als „relatives“ Vertrauen in unterschiedlichen Vertrauensklassen darstellbar.

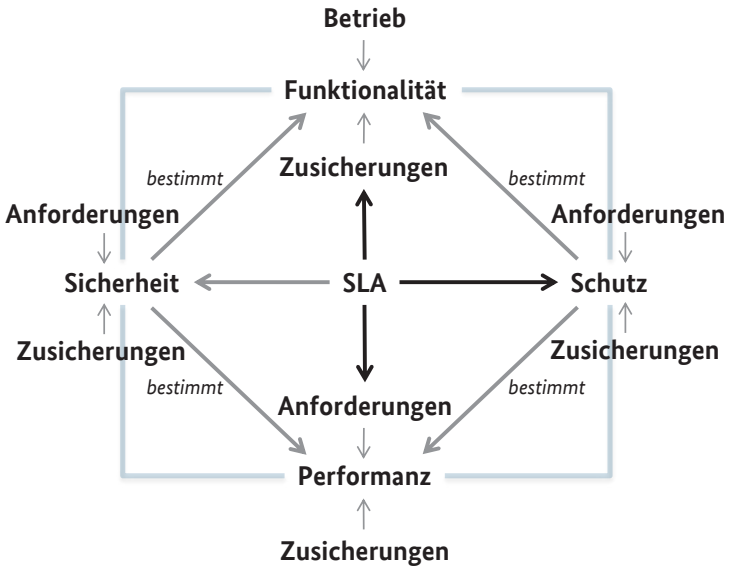
Da die Beurteilung der Vertrauenswürdigkeit von Cloud-Angeboten entlang aller Dimensionen anhand von Analysen der Funktionalität erfolgt, wird dies späterhin als „Function Analytics“ weiter definiert werden.

Die Beurteilung von Cloud-Angeboten wird dann als ein Abgleich zwischen Anforderungen der potenziellen Nutzer von Trusted Clouds und den Angeboten erfolgen, indem die Anforderungen für alle Dimensionen als „funktionale Anforderungen“ und „funktionale Zusicherungen“ betrachtet werden.

Auf der Basis der Ergebnisse dieser Abgleiche wird dann jeweils die „Quality of Services“ bestimmt




und werden Anleitungen für das Abfassen von „Service Level Agreements“ abgeleitet.



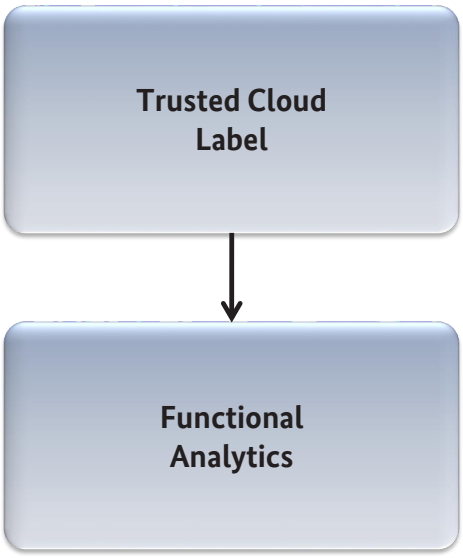
# Das Label „Trusted Cloud“

Die Nutzung des Labels „Trusted Cloud“ setzt voraus, dass eine Ende-zu-Ende-Analyse der zur Cloud-Nutzung in Anspruch genommenen Diensteinfrastruktur erfolgt ist und dass dabei der Abgleich zwischen Anforderungen und Zusicherungen entlang der Dimensionen des „Trusted-Cloud-Referenzmodells“ sichergestellt worden ist. Das bedeutet, dass nicht ein „universelles“ Label „Trusted Cloud“, sondern ein auf die jeweiligen Anforderungen und Zusicherungen hin „speziell“ zugeschnittenes Label für die jeweilige Cloud-Nutzung gilt. Dies trägt der Tatsache Rechnung, dass in der Praxis, in den verschiedenen Anwendungen, in den verschiedenen Branchen und in den verschiedenen Jurisdiktionen verschiedener Standorte unterschiedliche Anforderungen existieren und demzufolge auch unterschiedliche Zusicherungen nötig werden.

Mit der Ende-zu-Ende-Analyse wird zudem sichergestellt, dass nicht nur eine „partielle“ Vertrauenswürdigkeit zugesichert wird, sondern dass jeweils alle an der Cloud-Nutzung beteiligten Komponenten einer Diensteinfrastruktur, von den jeweiligen Endgeräten über die Kommunikationsverbindungen bis zum Cloud-Angebot, der Analyse unterworfen werden und dass die Vertrauenswürdigkeit der gesamten Infrastruktur immer durch das „schwächste Glied“ in der Kette der genutzten Systeme den Grad der Vertrauenswürdigkeit bestimmt.

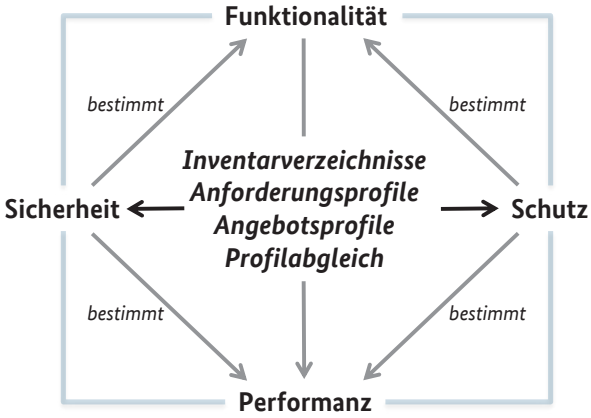
Das bedeutet, dass zur Durchführung der Ende-zu-Ende-Analyse Informationen über die Gesamtheit der in einer Cloud-Nutzung in Anspruch genommenen Systeme verfügbar sein müssen. In der Praxis werden dazu häufig Demonstrationen und Erprobungen der in Anspruch genommenen Diensteinfrastruktur als ausreichende Überprüfungen angeboten. Mit Demonstrationen und Erprobungen allein sind die zur Nutzung des Labels „Trusted Cloud“ zu erfüllenden Anforderungen nicht zu erbringen, weil mit ihnen in aller Regel nicht die Überprüfung aller Zusicherungen im Hinblick auf alle Anforderungen möglich sein wird. Eine vollständige Überprüfung von Zusicherungen andererseits würde aber letztlich eine Code-Analyse für alle beteiligten Softwaresysteme und eine Funktionsanalyse für alle beteiligten Hardwaresysteme erfordern. Dies kann aus den folgenden praktischen Gründen nicht gefordert werden: Die zur Nutzung kommenden Systeme einer Diensteinfrastruktur sind in aller Regel proprietär, und die Offenlegung von Programmen und Hardwarefunktionen kann nicht erwartet oder verlangt werden. Der für die Erlangung der Berechtigung zur Nutzung des Labels „Trusted Cloud“ zu erbringende Nachweis verlangt dagegen eine „Funktionsanalyse“, mit der die Funktionalitäten der genutzten Diensteinfrastruktur durch deren Anbieter ermittelt und beschrieben werden. Damit wird Vertrauenswürdigkeit, die mit dem Label „Trusted Cloud“ zugesichert wird, als eine nicht nur technische Eigenschaft, sondern auch als eine von der Reputation aller Beteiligten abhängige Eigenschaft betrachtet.

Dies mag für eine „puristische“ Definition des Begriffs „Trusted Cloud“ nicht ausreichend sein, ist aber für eine „praktikable“ Definition ausreichend. Der durch die Reputation der Beteiligten bestimmten „Unschärfe“ des Labels „Trusted Cloud“ wird späterhin dadurch begegnet, dass auch für alle Beteiligten im Rahmen der Funktionsanalyse Informationen angefordert, erfasst und vorgehalten werden. Mit diesen Erläuterungen wird deutlich gemacht, dass die Berechtigung zur Nutzung des Labels „Trusted Cloud“ nur im Rahmen dieser Funktionsanalyse erworben werden kann.



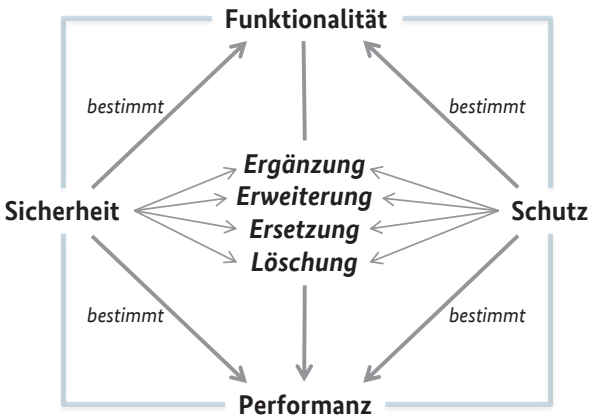
# Funktionsanalyse

Die Funktionsanalyse dient zunächst der Erfassung aller Systeme einer Diensteinfrastruktur, deren Verfügbarkeit die Voraussetzung für die Nutzung eines Cloud-Angebotes ist. Sie alle stellen zunächst mögliche Risiken im Hinblick auf die Vertrauenswürdigkeit einer Trusted Cloud dar. Dazu wird gefordert, dass im Rahmen der Funktionsanalyse ein Inventarverzeichnis mit allen Systemen der Infrastruktur und den zwischen den Systemen existierenden „Abhängigkeiten“ dargestellt wird. Abhängigkeiten sind z. B. dadurch gegeben, dass die Systeme der Diensteinfrastruktur bei der Cloud-Nutzung in einer bestimmten Reihenfolge in Anspruch genommen werden. Andere Abhängigkeiten existieren z. B. dadurch, dass zwischen einzelnen Systemen ein Datenaustausch stattfinden muss.

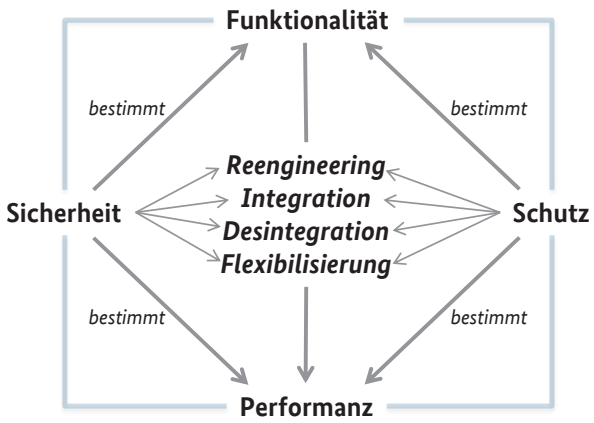



Neben der Erstellung eines Inventarverzeichnisses für eine Cloud-Nutzung sind für diese auch „Anforderungsprofile“ im Hinblick auf die die Vertrauenswürdigkeit festlegenden Dimensionen „Funktionalität“, „Sicherheit“, „Datenschutz“, „Performanz“ und „Kosten/Nutzen“ zu erstellen. Die Nutzung eines „bestimmten“ Cloud-Angebots sollte immer an die Bedingung geknüpft sein, dass das Cloud-Angebot durch ein Angebotsprofil charakterisiert ist. Nur dann ist der Abgleich zwischen Nachfrage und Angebot möglich.

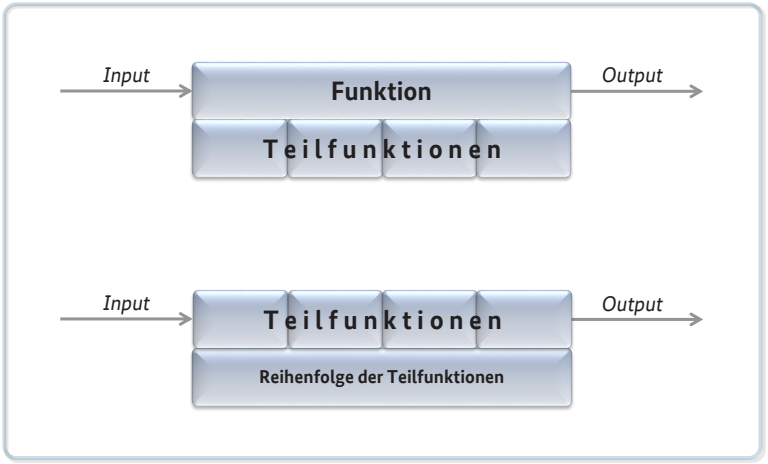
Um sicherzustellen, dass die Nutzung eines Cloud-Angebots in einer schon existierenden Unternehmens-IT in diese Unternehmens-IT eingebettet werden kann und dann mit dieser schon existierenden Unternehmens-IT kompatibel ist, sollte im Rahmen der Funktionsanalyse bestimmt werden, wie die neue Cloud-Nutzung in die existierende Unternehmens-IT einbezogen werden soll.



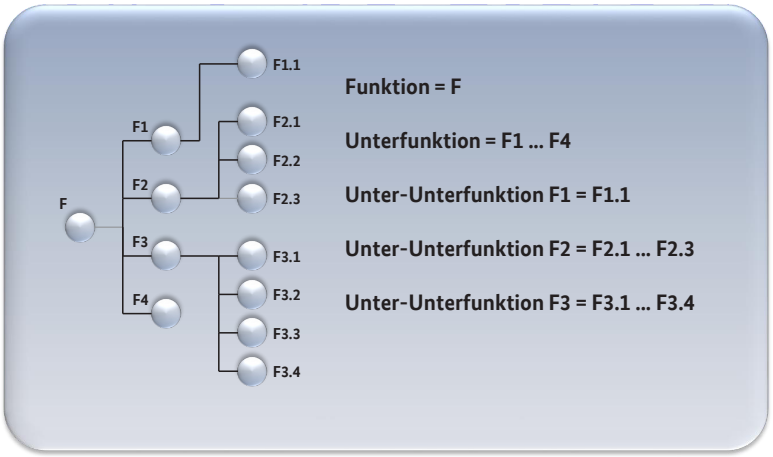

Von gleicher Bedeutung sind an dieser Stelle Festlegungen dafür, welche Verfahren zur Einbettung existieren bzw. entwickelt werden müssen.




Die Funktionsanalyse einer Diensteinfrastruktur zur Nutzung von Cloud-Angeboten charakterisiert alle Systeme der Diensteinfrastruktur durch ihre „Funktionalität". Die Funktionalität eines Systems ist zunächst nur eine Bezeichnung für eine oder mehrere Funktionen. Bezeichner sind zum Verständnis der von einem System zu erbringenden Leistung „sinngebende" Namen für die jeweilige Funktionalität. Darüber hinaus wird eine Funktionalität durch das zur Nutzung der Funktionalität erforderliche „Input" und das mit der Nutzung der Funktionalität erzeugte „Output" unterschiedlichster Art festgelegt.

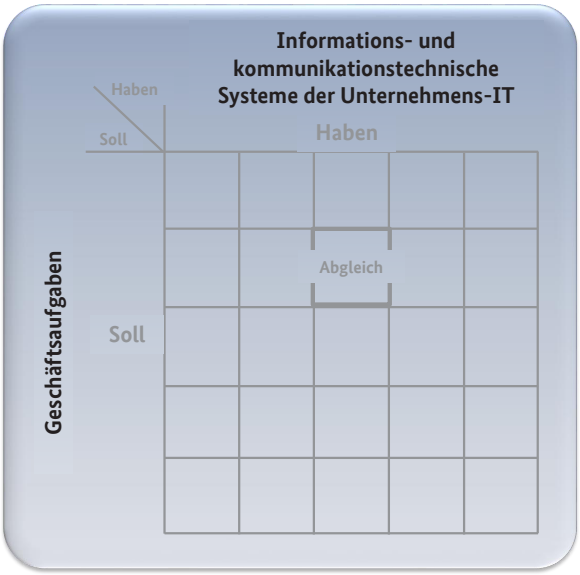



Diese zunächst sehr grobe Analyse der Funktionalität reicht möglicherweise aus, wenn die angestrebte Cloud-Nutzung eher niedrige Anforderungen an ihre Vertrauenswürdigkeit stellt. Sind höhere Anforderungen zu erfüllen, kann die Funktionsanalyse erweitert werden, sodass die zunächst grob bestimmten Funktionalitäten schrittweise verfeinert werden. Die Verfeinerung erfolgt so, dass die identifizierte Zerlegung der Funktionalität dadurch beschrieben wird, dass auch für die durch die Zerlegung identifizierten „Komponenten-Funktionalitäten“ wiederum durch entsprechende sinngebende Bezeichner deren Benennung erfolgt.

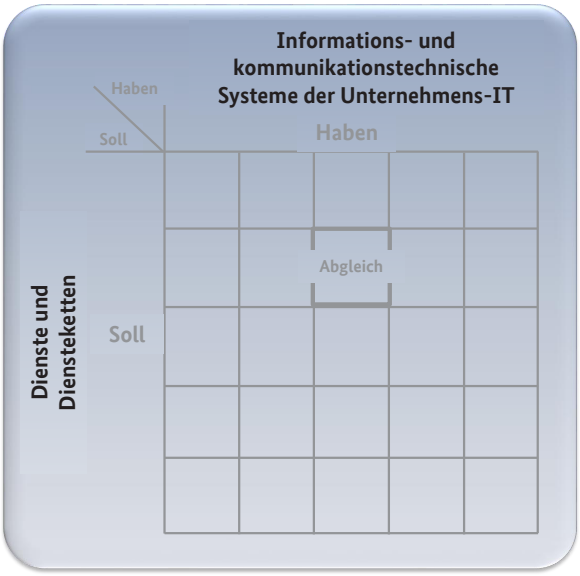



Diese Verfeinerung kann dann auch als eine Präzisierung der Bedeutung einer durch eine Hierarchie von Unterfunktionalitäten beschriebenen Funktionalität gelten. Dies entspricht dem auch umgangssprachlichen Brauch, einen Begriff durch weitere „untergeordnete“ erklärende Begriffe zu präzisieren, und es entspricht insbesondere auch dem Vorgehen, den Aufbau der in der physikalischen Welt existierenden Artefakte durch deren „Stückliste“ zu erläutern.

Nachdem die Vorgehensweise zu Funktionalitäten und die Verfeinerungen der Funktionalitäten für die Beschreibung von Dienste-Infrastrukturen zur Nutzung von Cloud-Angeboten erläutert sind, werden für die Dokumentation der Ergebnisse der Funktionsanalyse die folgenden Vorschläge unterbreitet: Um für die Dokumentation existierende und erprobte Werkzeuge nutzen zu können, werden Funktionalitäten und Verfeinerungen von Funktionalitäten von Angeboten und Nachfrage in Tabellen dargestellt. Sinnvolle und notwendige Tabellen sind in den folgenden Bildern dargestellt.



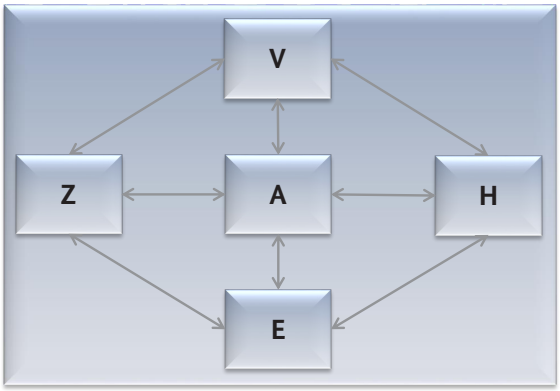

Die Nachfrage in Form einer „Geschäftsaufgabe“ oder einer „Geschäftsfunktion“ kann dem Angebot für Leistungen, die eine Unternehmens-IT bereitstellen kann, gegenübergestellt werden.




Die Nachfrage in Form von gewünschten „Diensten“ kann dem Angebot für Leistungen, die ein Cloud-Angebot bereitstellen kann, gegenübergestellt werden.

# Spezifikation von Funktionalitäten

Die bis dahin erläuterten Möglichkeiten für eine Beschreibung der Funktionalitäten einer Diensteinfrastruktur, über die Cloud-Angebote genutzt werden können, sind noch immer nicht notwendigerweise hinreichend, um eine Entscheidung über deren Inanspruchnahme als vertrauenswürdige Angebote treffen zu können. Dafür werden Spezifikationen der identifizierten Funktionalitäten und von deren Verfeinerungen vorgesehen. Spezifikationen umfassen Informationen, die heute häufig als Metainformationen bezeichnet werden und die beteiligten Personen, Instanzen, Anbieter, Nutzer etc. umfassen und hier summarisch als „Verantwortliche" bezeichnet werden. Daneben umfassen Spezifikationen vor allen Dingen die Beschreibung der Abläufe bei der Nutzung der Funktionalitäten und die bei der Nutzung einzuhaltenden Reihenfolgen für die Nutzung der „Komponenten-Funktionalitäten". Darüber hinaus werden in Spezifikationen auch wieder „Input" und „Output" der jeweiligen Funktionalitäten, aber auch die Hilfsmittel für die Nutzung der Funktionalitäten bestimmt. Letztlich umfassen Spezifikationen auch eine Beschreibung des mit den jeweiligen Funktionalitäten verfolgten Ziels.

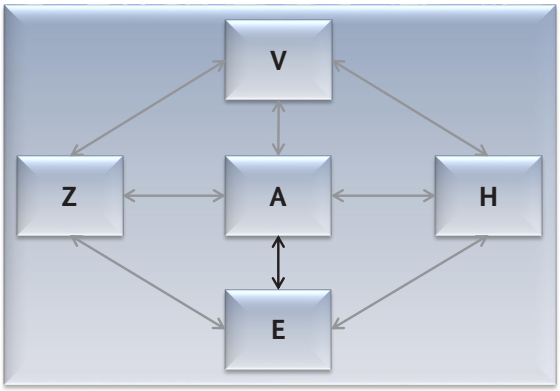



**A = Ablauf**
**Z = Ziel**
**V = Verantwortliche**
**H = Hilfsmittel**
**E = Ergebnis**

Dieses Schema für die Spezifikation von Funktionalitäten kann dann für die Beschreibung der Funktionalität unterschiedlicher Artefakte genutzt werden.

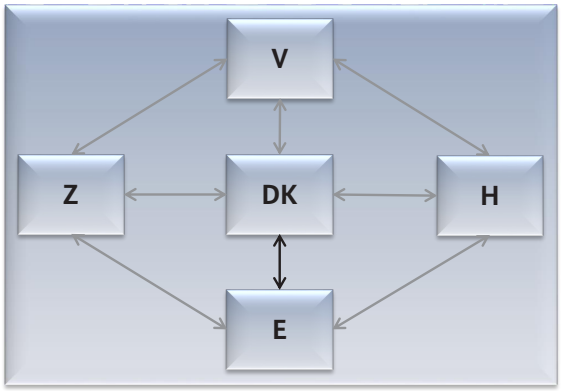
Mithilfe von Spezifikationen können dann sowohl „Geschäftsaufgaben" als auch „Dienste", aber auch „IT-Funktionen" so weit charakterisiert werden, dass hinreichend viele Informationen für die Entscheidungsfindung verfügbar werden.

**Aufgabe**



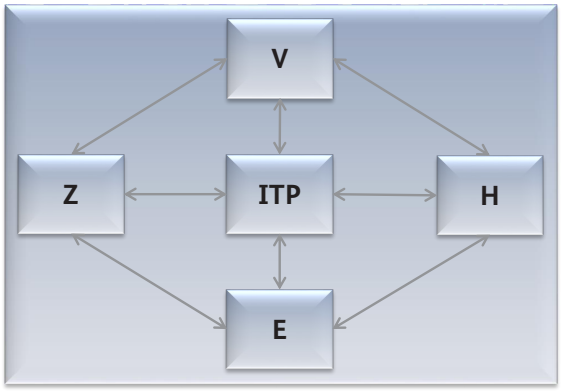

**A = Ablauf**
**Z = Ziel**
**V = Verantwortliche**
**H = Hilfsmittel**
**E = Ergebnis**

**Dienst**




DK = Dienstekette
Z = Ziel
V = Verantwortliche
H = Hilfsmittel
E = Ergebnis

**IT-Funktion**



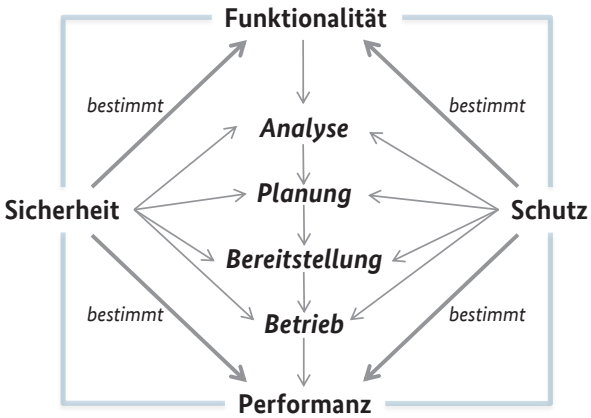

ITP = IT-Prozesse
Z = Ziel
V = Verantwortliche
H = Hilfsmittel
E = Ergebnis

Das Label Trusted Cloud muss, wie die sich ändernden Anforderungen wegen sich verändernder Bedrohungen der Vertrauenswürdigkeit, in regelmäßigen Abständen erneuert werden. Dieser Dynamik der Anforderungen muss mit einer Dynamik der Zusicherungen entgegnet werden. Um diese Dynamik zu ermöglichen, entsteht die Notwendigkeit, die Weiterentwicklung des Labels sicherzustellen, und das wiederum erfordert die Existenz einer unabhängigen und vertrauenswürdigen Institution zur Übernahme der Verantwortung für diese Weiterentwicklung.

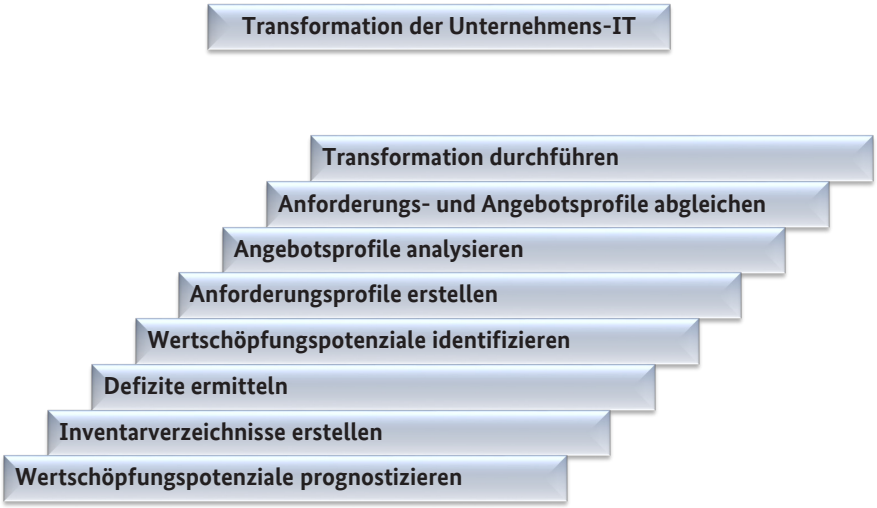
Im Rahmen des Trusted-Cloud-Programms des Bundesministeriums für Wirtschaft und Energie (BMWi) ist deshalb der Vorschlag für die Etablierung eines Kompetenznetzwerks und eines Kompetenzzentrums Trusted Cloud erarbeitet worden. Die nötigen regelmäßigen Überprüfungen werden nach diesem Vorschlag vertrauenswürdigen Prüfunternehmen überlassen werden.

# Transformation und Transformationsmanagement

Die Nutzung von Cloud-Angeboten in der Wirtschaft erfordert stets – wie schon angedeutet – die Einbettung der Cloud-Angebote in eine existierende Unternehmens-IT. Es ist auch schon verdeutlicht worden, dass deren Integration zur Ermöglichung von „Kollaborationen“ zwischen Anwendungen von „Interoperation“ zwischen Systemen und zur „Vernetzung“ von unterschiedlichen Hardware-/Softwaresystemen zu einer engen „Verzahnung“ mit dem Rest der Unternehmens-IT werden kann. Letztlich kann auch der Ersatz existierender Teile der Unternehmens-IT durch „bessere“ Cloud-Angebote angezeigt sein, was eine besonders enge „Kopplung“ zwischen existierender Unternehmens-IT und Cloud-Angeboten nach sich zieht. All dies ist in aller Regel mit erheblichen Aufwänden verbunden und erfordert das systematische Management dieser Transformationen.




Dazu würden in aller Regel die Erfahrungen aus anderen IT-Vorhaben und Projekten eine ausreichende Basis darstellen. Hier soll nur angedeutet werden, dass klassische Techniken des Softwareengineering mit der Definition von Vorgehensmodellen oder durch die Nutzung „agiler“ Vorgehensweisen nötig sind, und falls sie nicht vorhanden sind, wird die Inanspruchnahme von Expertenhilfe unabdingbar sein. Einen ersten Überblick über die zu bewältigenden Aufgaben in der Transformation gibt die folgende Skizze:



Mit der Skizze wird verdeutlicht, dass schon in der Vorbereitung der Nutzung von Trusted Clouds logische Reihenfolgen zu beachten sind. Das Orientierungswissen und einige Leitfäden sollen helfen, die Komplexität der Aufgabe zu bewältigen. Das hier vorgeschlagene Vorgehen sieht die folgenden Stufen vor:

1. Wertschöpfungspotenziale, die mit dem Einsatz von Trusted-Cloud-Angeboten verbunden sind, prognostizieren auf der Basis von Potenzialbeschreibungen (wie im Teil 1 „Modernisierung der Unternehmens-IT für die digitale Transformation in der Wirtschaft“, S. 33 ff., vorgeschlagen).

2. Inventarverzeichnisse (soweit sie nicht schon existieren) der genutzten Unternehmens-IT anlegen und Durchführung von Stärken-Schwächen-Analysen (wie im Leitfaden „Der Weg in die Trusted Cloud“ vorgeschlagen).

3. Ermittlung der Defizite und Maßnahmenvorschläge entwickeln. Priorisierung der vorgeschlagenen Maßnahmen.

4. Für die mit Priorität belegten Maßnahmen Wertschöpfungspotenziale aus der Nutzung von Cloud-Angeboten identifizieren und abschätzen.

5. Erstellen von Anforderungsprofilen (wie in den Leitfäden „Der Weg in die Trusted Cloud“, „Cloud-Sicherheits-Leitfaden für Anbieter [CSLA]“ und „Cloud-Sicherheits-Leitfaden für Nutzer [CSLN]“ vorgeschlagen).

6. Angebotsprofile analysieren (wie in den Leitfäden „Der Weg in die Trusted Cloud“, „Cloud-Sicherheits-Leitfaden für Anbieter [CSLA]“ und „Cloud-Sicherheits-Leitfaden für Nutzer [CSLN]“ vorgeschlagen).

7. Den Abgleich zwischen Anforderungs- und Angebotsprofilen durchführen (wie in den Leitfäden „Der Weg in die Trusted Cloud“, „Cloud-Sicherheits-Leitfaden für Anbieter [CSLA]“ und „Cloud-Sicherheits-Leitfaden für Nutzer [CSLN]“ vorgeschlagen).

8. Transformation und Transformationsmanagement planen.

Die zentrale Entscheidung zur Transformation besteht darin, eine Festlegung darüber zu treffen, wie die Nutzung von Cloud-Angeboten in die existierende Unternehmens-IT eingebunden werden soll:

1. Sollten die Cloud-Angebote als „Stand-alone"-Leistungen neben den übrigen Leistungen der Unternehmens-IT genutzt werden, ist der Integrationsaufwand und damit der Transformationsaufwand gering.

2. Soll die Nutzung der Cloud-Angebote mit dem Rest der Unternehmens-IT lose gekoppelt sein, muss die syntaktische Interoperabilität zwischen den Cloud-Angeboten und dem Rest der Unternehmens-IT sichergestellt werden und der dazu nötige Integrationsaufwand sowie der Transformationsaufwand werden erheblich höher sein.

3. Soll die Nutzung der Cloud-Angebote mit dem Rest der Unternehmens-IT eng gekoppelt sein, muss die semantische Interoperabilität zwischen Cloud-Angeboten und dem Rest der Unternehmens-IT sichergestellt werden, und der dazu nötige Integrationsaufwand sowie der Transformationsaufwand sind erwartungsgemäß groß und können nicht nur von dem für den Betrieb der Unternehmens-IT Zuständigen allein bewältigt werden, sondern erfordern die enge Absprache zwischen diesen und den Fachbereichen des Unternehmens.

Insbesondere kleine und mittlere Unternehmen werden für die Transformation nicht immer die notwendige Expertise zur Verfügung haben und sollten abwägen zwischen notwendigen Transformationen und dem „Umstieg" auf erprobte Cloud-Lösungen.

# Cloud-Sicherheits-Leitfaden für Anbieter (CSLA)

# Zusammenfassung

Der vorliegende Cloud-Sicherheits-Leitfaden für Anbieter von Cloud-Diensten (CSLA) bietet Hilfestellungen bei der Analyse von Sicherheitsrisiken, bei der Planung und Durchführung von Sicherheitsmaßnahmen und insbesondere bei der Kommunikation der Sicherheitsleistungen. Durch die Verwendung des CSLA können Entwickler und Betreiber von Cloud-Diensten ihr Angebot gegenüber der Konkurrenz positionieren. Potenzielle Kunden können mit dem CSLA gestaltete Angebote mithilfe des Cloud-Sicherheits-Leitfadens für Nutzer von Cloud-Diensten (CSLN) gemäß ihren persönlichen Sicherheitsanforderungen beurteilen und so eine passende Lösung finden, der sie vertrauen können.

Zum einen beinhaltet der CSLA eine Methode zur Risikoanalyse, die auch für kleine und mittelständische Unternehmen zu bewältigen ist. Zum anderen werden standardisierte Sicherheitsmaßnahmen mit verschiedenen Schutzlevels vorgestellt, die nicht nur die Konzeption und die Realisierung adäquater Sicherheitskonzepte zur Reduktion der identifizierten Sicherheitsrisiken unterstützen, sondern die im Zusammenspiel mit dem CSLN auch den potenziellen Nutzern die Einschätzung des gebotenen Sicherheitsniveaus und letztlich das Schöpfen von Vertrauen in den angebotenen Cloud-Dienst erleichtern.

Hinweis zur Version 0.1:
Dieser Leitfaden befindet sich noch in der Entwicklung. Anregungen zur Verbesserung sind willkommen. Die bisher nur vorläufigen BSI-Grundschutz-Bausteine zum Thema Cloud sind noch nicht vollständig integriert.

# 1 Einleitung zum Cloud-Sicherheits-Leitfaden für Anbieter (CSLA)

## 1.1 Bedeutung von Informationssicherheit im Zusammenhang mit Cloud Computing

Cloud Computing ist eine Bezeichnung für verschiedene Formen von serviceorientierten Virtualisierungen in verteilten Computersystemen. Externe Cloud-Lösungen, bei denen die Cloud-Dienste von fremden Anbietern genutzt werden, haben einen besonders schweren Stand, was Vertrauen und Sicherheit angeht. Der Grund liegt in dem externen Anbieter – diesem müssen Nutzer in der Regel vertrauen. Es bestehen Abhängigkeiten von den Leistungen des Anbieters, über die Anwender keine vollständige Kontrolle haben. Außerdem existieren je nach Rechtsraum verschiedene rechtliche Schranken bezüglich der Zulässigkeit von Outsourcing.

Anbieter von Cloud-Diensten müssen sich das Vertrauen ihrer potenziellen Nutzer und Kunden verdienen. Ihre Angebote können gegenüber lokalen IKT-Lösungen auf Systemen in der Verwaltung der Anwender sogar Sicherheitsvorteile bieten, denn viele kleine und mittelständische Unternehmen, Selbstständige sowie Privatpersonen, die keine IT-Experten sind, können kaum ein so hohes Sicherheitsniveau gewährleisten, wie es die professionellen Betreiber von Cloud-Diensten können. Die Themen Vertrauenswürdigkeit und Sicherheit können auch eine große Stärke des Cloud-Angebots sein.

Es genügt nicht, ausgefeilte technische Sicherheitsmaßnahmen zu ergreifen und vertragliche Garantien anzubieten. Vertrauensbildende Maßnahmen müssen auch kommuniziert werden und die potenziellen Nutzer müssen sie objektiv prüfen können. Der vorliegende Cloud-Sicherheits-Leitfaden für Anbieter von Cloud-Diensten (CSLA) soll genau bei diesem Kommunikationsproblem helfen. Mit diesem CSLA können Angebote erstellt werden, die darauf optimiert sind, dass sie mit dem Cloud-Sicherheits-Leitfaden für Nutzer von Cloud-Diensten auf Sicherheit und Vertrauenswürdigkeit geprüft werden können.

## 1.2 Aufbau und Funktion des CSLA

Der Cloud-Sicherheits-Leitfaden für Anbieter besteht aus einer dreistufigen Methode zur Risikoanalyse sowie aus einem Vertrauensbildungs- und Kommunikationsverfahren für Angebote von Cloud-Diensten. Abbildung 1 visualisiert die Konzepte.

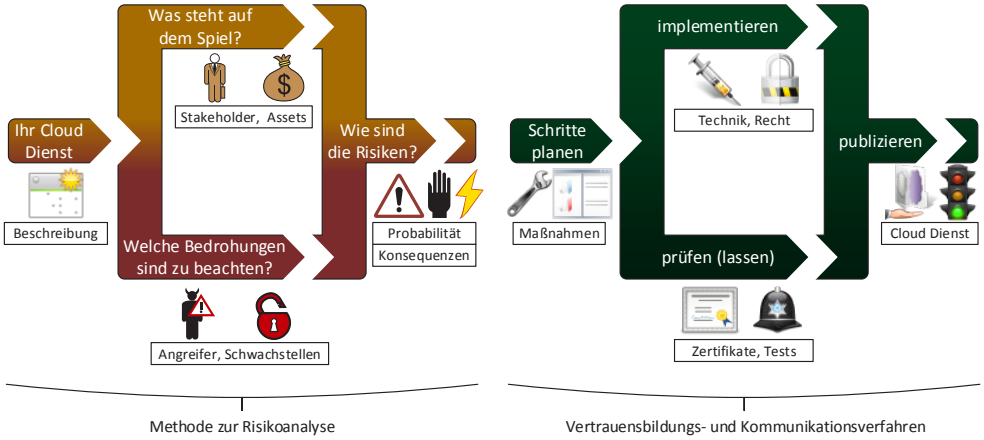



Abbildung 1: Konzeptuelle Übersicht zum Cloud-Sicherheits-Leitfaden für Anbieter (CSLA)

## 1.3 Ein offenes Wort – Limitationen des CSLA

**Einsatzgebiet und Voraussetzungen des CSLA**

Der Cloud-Sicherheits-Leitfaden für Anbieter (CSLA) bietet sicherheitstechnische Hilfestellungen für die Anbieter von Cloud-Diensten sowohl zur Risikoanalyse als auch zur Risikominimierung und insbesondere zur Kommunikation der ergriffenen Sicherheitsmaßnahmen. Der CSLA bietet keine Unterstützung zur Entwicklung und Kommunikation der funktionalen Aspekte.

**IKT-Sicherheit ist und bleibt eine Herausforderung**

Der CSLA ist als Orientierungshilfe konzipiert, um eine systematische Auseinandersetzung mit den Themen Sicherheits- und Risikomanagement im Zusammenhang mit Cloud-Technologien zu ermöglichen. Die korrekte und hinreichend gründliche Anwendung der hier vorgestellten Verfahren zur Analyse sowie zur Vertrauensbildung ist eine anspruchsvolle, interdisziplinäre Aufgabe.

**Sicherheit ist kostspielig**

Maßnahmen, die Sicherheit schaffen und Risiken reduzieren sollen, sind oftmals mit erheblichen Aufwendungen verbunden. Auch die Benutzerfreundlichkeit kann durch starke Sicherheitskonzepte beeinträchtigt werden. Wenn andererseits aufgrund von mangelhaften Sicherheitsmaßnahmen Schäden entstehen, kann dies ebenfalls sehr teuer werden und die Benutzer abschrecken. Verspieltes Vertrauen kann ein irreparabler Schaden sein. In der Praxis gilt es, vernünftige Kompromisse zu finden.

**Sicherheit ist nie vollkommen**

Auch eine korrekte Befolgung dieses CSLA kann keine hundertprozentige Sicherheit garantieren. Es wird kein Anspruch auf Vollständigkeit erhoben. Der Gebrauch des CSLA entbindet nicht von der Sorgfaltspflicht. Auch hier nicht erwähnte potenzielle Bedrohungen sowie Risiken müssen beachtet werden und es gilt, angemessen darauf zu reagieren. Die aufgeführten Sicherheitsmaßnahmen werden nicht immer genügen und es sind eventuell weitere, hier nicht beschriebene Maßnahmen zu ergreifen. Im Zweifelsfall sollte zusätzlich Rat bei unabhängigen Security-Experten und Juristen eingeholt werden.

# 2 Was steht eigentlich auf dem Spiel?

Eine mögliche Annäherung an das Thema Sicherheit besteht darin, sich zunächst mit dem zu beschäftigen, was gefährdet werden könnte – also mit den Dingen, die passieren können, wenn Sicherheit nicht gegeben wäre. Um zu erfassen, welche Gefahren bestehen, sollte zunächst geklärt werden, wer überhaupt betroffen sein könnte, wenn etwas schiefläuft. Dies wird mit der Identifizierung der Stakeholder geleistet. In einem zweiten Schritt sollte dann identifiziert werden, welche Werte der potenziell Betroffenen beeinträchtigt werden könnten. Hierzu dient die Wertanalyse.

## 2.1 Identifizieren der Stakeholder

Hier werden eine Reihe von generischen Stakeholdern vorgestellt, die typischerweise zu beachten sind. In der Analyse kann je nach Bedarf auch eine präzisere Gliederung mit feiner unterteilten Stakeholder-Typen vorgenommen werden.

### 2.1.1 Anbieter

Anbieter sind im Sinne des CSLA Unternehmen, Organisationseinheiten oder juristische Personen, die selbst die zu analysierenden Cloud-Dienste entwickeln und die diese Dienste externen Nutzern zur Verwendung bereitstellen.

### 2.1.2 Eigner des Anbieters

Sofern der Anbieter ein Unternehmen ist, sind eventuell auch die Eigner, welche Anteile an diesen Unternehmen besitzen, als Stakeholder zu berücksichtigen.

### 2.1.3 Mitarbeiter

Wenn der Anbieter ein Unternehmen oder eine Organisationseinheit ist, so sind die Mitarbeiter des Anbieters als Stakeholder zu beachten.

### 2.1.4 Nutzer

Nutzer sind im Sinne des CSLA diejenigen natürlichen Personen oder Organisationseinheiten, die selbst Cloud-Dienste des Anbieters verwenden. Die Nutzer sind Kunden des Anbieters.

Sofern Unternehmen zu den Nutzern zählen, sind auch diejenigen, die Anteile an diesen Unternehmen besitzen, die Mitarbeiter und die Kunden dieser Unternehmen als Stakeholder zu berücksichtigen, unabhängig davon, ob diese die Cloud-Dienste selbst in Anspruch nehmen.

### 2.1.5 Geschäftspartner des Anbieters

Geschäftspartner des Anbieters können durch die Cloud-Dienste des Anbieters eventuell beeinflusst werden, auch wenn die Geschäftspartner selbst keine Nutzer der Cloud-Dienste sind.

### 2.1.6 Öffentlich-rechtliche Institutionen

Als öffentlich-rechtliche Stakeholder sind politische Unionen, Staaten und Behörden zu berücksichtigen.

### 2.1.7 Dritte

Personen, Unternehmen und Organisationseinheiten, die nicht in eine der genannten Kategorien von Stakeholdern passen, aber trotzdem betroffen sein könnten, werden hier als Dritte bezeichnet. Dies können beispielsweise externe Personen sein, über die Daten gesammelt werden, obwohl sie weder Nutzer der Cloud-Dienste des Anbieters noch Geschäftspartner des Anbieters sind.

## 2.2 Analysieren der Werte

In diesem Schritt wird analysiert, was für die identifizierten Stakeholder im Zusammenhang mit dem Cloud-Dienst von Wert ist bzw. von Wert sein könnte und gefährdet werden könnte. Es ist zweckdienlich, für jeden erfassten Typ von Stakeholder eine eigene Analyse der möglicherweise betroffenen Werte durchzuführen. Jeder einzelne identifizierte Wert sollte mit einer eindeutigen ID versehen werden.

### 2.2.1 Käufliche Werte

Diese Assets sind dadurch gekennzeichnet, dass sie sich auf dem Markt handeln lassen. Mithin ist es relativ einfach möglich, hierfür einen Preis zu ermitteln. Verluste dieser Werte lassen sich oftmals mit Geld wieder ausgleichen.
Hierzu gehören:

- Finanzvermögen
  - Bargeld
  - Aktien
  - Bankguthaben

- materielle Sachwerte
  - Immobilien
  - Grundstücke
  - Fahrzeuge
  - Computer und Maschinen

- (informationstechnische) Dienstleistungen

### 2.2.2 Unveräußerliche Werte

Unveräußerliche Assets können prinzipiell nicht durch Kauf erlangt werden. Werden unveräußerliche Assets verletzt, so kann dies trotzdem zu erheblichen, auch direkt finanziellen Verlusten führen. Eventuell drohen zusätzlich juristische Sanktionen. Einmal entstandene Verluste lassen sich mit Geld in der Regel nicht ohne weiteres kompensieren. Beispiele sind:

- Vertrauenswürdigkeit
- Reputation
- Persönlichkeitsrecht

### 2.2.3 Immaterielle Werte

Immaterielle Assets lassen sich durchaus auf einem freien Markt kaufen und verkaufen, zumindest solange sie geheim sind. Für sie lässt sich also prinzipiell ein Verkaufspreis ermitteln. Umgekehrt lassen sich einmal preisgegebene und eventuell publik gewordene Informationen jedoch nicht wieder geheim machen. Ein Rückkauf im Verlustfall ist allgemein nicht möglich. An immateriellen Werten sind zu beachten:

- private Daten, vertrauliche Kundendaten, Unternehmensdaten, Geschäftsgeheimnisse
  - Authentizität, Integrität, Verfügbarkeit, Geheimhaltung
- urheberrechtlich geschützte Daten
- Für Cloud-Anbieter insbesondere:
  - Source-Code der Cloud-Dienste
  - Datenbanken, auf deren Informationen die Cloud-Dienste zugreifen

### 2.2.4 Detailgrad der Wertanalyse

Für einzelne Güter wie beispielsweise für Kreditkartendaten von Kunden kann es Sinn ergeben, bereits bei der Wertanalyse genau das, was an dem Gut gefährdet werden könnte, was verloren gehen könnte, als eigenständige Werte zu erfassen. Im Beispiel mit dem Gut Kreditkartendaten würde das bedeuten, statt einfach nur die Kreditkartendaten als Wert zu identifizieren, die Geheimhaltung, die Authentizität, die Integrität, die Verfügbarkeit und die Gültigkeit (Aktualität) der Kreditkartendaten jeweils als eigene Werte aufzunehmen. Dies erleichtert die Identifikation von relevanten Bedrohungsszenarien sowie Gefährdungen und die anschließende Beurteilung der potenziellen Konsequenzen.

# 3 Welche Bedrohungen sind zu beachten?

Dieses Kapitel besteht im Wesentlichen aus einer Auflistung von Bedrohungsszenarien, denen IKT-Systeme und speziell cloudbasierte Systeme typischerweise ausgesetzt sind. Die Aufgabe für den Analysten ist, jene Bedrohungen herauszufiltern und zu verstehen, die Auswirkungen auf die identifizierten Werte haben könnten. Dazu können die entsprechenden Werte-IDs aus der Wertanalyse in den nachfolgenden Tabellen in die Zeile des jeweiligen Bedrohungsszenarios geschrieben werden.

Die folgende Aufstellung der potenziellen Bedrohungsszenarien orientiert sich an den (teils vorläufigen) BSI-Grundschutz-Katalog-Bausteinen B 1.1.1 Outsourcing, B 5.23 Cloud-Management und B 5.24 Web-Services. Die einzelnen Bedrohungen werden mithilfe von Gefahren-IDs aus dem BSI-Grundschutz-Katalog identifiziert. Ausführliche Beschreibungen der einzelnen Gefahren und Bedrohungsszenarien finden sich im BSI-Grundschutz-Katalog.

## 3.1 Bedrohungen durch die Cloud-Plattform

Technische Angriffe gegen Cloud-Plattformen bedrohen prinzipiell alle Cloud-Lösungen. Grundlage der Cloud ist die Virtualisierung. Die Virtualisierung an sich schafft mindestens eine zusätzliche Ebene, die angegriffen werden kann. Die Virtualisierungsumgebung selbst (G 5.150) und die von ihr bereitgestellten Funktionen (G 5.148) können missbraucht werden, beispielsweise die Erzeugung von Snapshots (G 3.100). Auch die Verwaltung (G 3.102, G 4.76) und die Vernetzung (G 4.75, G 5.147) der Virtualisierung bieten eventuell Angriffspunkte. Schließlich können auch die Tools (G 2.150, G 3.101, G 4.77, G 5.147) und Anwendungen (G 2.151), die in der Virtualisierung betrieben werden, Probleme bereiten.

Eine Klasse von Gefahren bilden unzureichende physische IT-Systeme, auf denen die Virtualisierung betrieben wird (G 2.32, G 2.149, G 3.99, G 4.74, G 4.75, G 4.76, G 4.77). Ursachen können etwa eine zu geringe Redundanz oder mangelhafte Leistungsreserven für den gleichzeitigen Zugriff durch viele Nutzer sein. Es handelt sich oftmals um Planungsfehler (G 2.148), aufgrund des Kostendrucks sind Anbieter von Cloud-Diensten versucht, die technische Basis knapp zu halten.

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.32 | Unzureichende Leitungskapazitäten | | |
| G 2.148 | Fehlerhafte Planung der Virtualisierung | | |
| G 2.149 | Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme | | |
| G 2.150 | Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen | | |
| G 2.151 | Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen | | |
| G 3.99 | Fehlerhafte Netzanbindungen eines Virtualisierungsservers | | |
| G 3.100 | Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme | | |
| G 3.101 | Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen | | |
| G 3.102 | Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen | | |
| G 4.74 | Ausfall von IT-Komponenten in einer virtualisierten Umgebung | | |
| G 4.75 | Störung der Netzinfrastruktur von Virtualisierungsumgebungen | | |
| G 4.76 | Ausfall von Verwaltungsservern für Virtualisierungssysteme | | |
| G 4.77 | Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen | | |
| G 5.147 | Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes | | |
| G 5.148 | Missbrauch von Virtualisierungsfunktionen | | |
| G 5.149 | Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen | | |
| G 5.150 | Kompromittierung des Hypervisors virtueller IT-Systeme | | |

## 3.2 Allgemeine Bedrohungen von IKT-Systemen

Die bei IKT-Systemen allgemein zu beachtenden Angriffsszenarien sind auch bei Cloud-Lösungen zu berücksichtigen – und zwar für alle beteiligten Systeme nicht nur in der Cloud, sondern auch außerhalb, etwa für Zugangssysteme der Nutzer. Zu diesen Bedrohungen zählen insbesondere gezielter Diebstahl (G 4.33, G 4.35, G 5.4, G 5.71), Manipulationen (G 5.1, G 5.3, G 5.85) und die Ausführung von schädlichen Programmen (G 4.22, G 5.2, G 5.173) durch externe Angreifer.

Zu den Werkzeugen von externen Angreifern gehören insbesondere Schadprogramme (G 5.23) wie Computerviren und Spähprogramme (Spyware). Als informationstechnische Türöffner dienen neben Schwachstellen in Programmen auch trojanische Pferde (G 5.21), die durch unachtsame Anwender eingeschleppt und zur Ausführung gebracht werden.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 4.22 | Software-Schwachstellen oder -Fehler | | |
| G 4.33 | Schlechte oder fehlende Authentikation | | |
| G 4.35 | Unsichere kryptographische Algorithmen | | |
| G 5.1 | Manipulation oder Zerstörung von Geräten oder Zubehör | | |
| G 5.2 | Manipulation an Informationen oder Software | | |
| G 5.3 | Unbefugtes Eindringen in ein Gebäude | | |
| G 5.4 | Diebstahl | | |
| G 5.21 | Trojanische Pferde | | |
| G 5.23 | Schadprogramme | | |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen | | |
| G 5.85 | Integritätsverlust schützenswerter Informationen | | |
| G 5.173 | Einbindung von fremden Daten und Schadcode bei Webanwendungen | | |

## 3.3 Gefährdungen der Kommunikation und des Zusammenspiels

Diese Bedrohungen sind für alle Cloud-Dienste und Zugangssysteme im Zusammenspiel zu analysieren. Die Gefährdungen gehen von Systemen und Infrastrukturen aus, die weder die Nutzer noch die Anbieter von Cloud-Diensten kontrollieren können.

Ausfälle von Internetknoten, Providern und Störungen von Leitungen können die Verfügbarkeit von Cloud-Diensten einschränken (G 1.10, G 1.19, G 4.31, G 5.28).

Verbindungen zu Cloud-Diensten werden oftmals über gesicherte Protokolle wie SSL/TLS (https://...) hergestellt. In der Vergangenheit gab es jedoch wiederholt erfolgreiche Manipulationen und Attacken, insbesondere mit kompromittierten privaten Schlüsseln (G 5.83) und gefälschten Zertifikaten (G 5.84), wodurch die Authentifikation unterwandert werden könnte (G 4.33).

Die Gefahren von unzureichender Verschlüsselung (G 4.35, G 5.12, G 5.165) sollten spätestens seit den Enthüllungen über die groß angelegte systematische Überwachung von Datenströmen durch die NSA ernst genommen werden. Eine Analyse des Nachrichtenflusses (G 5.26), also wo überhaupt Daten in welchem Umfang ausgetauscht werden, lässt sich auch ohne Entschlüsselung durchführen und daraus lassen sich eventuell bereits Rückschlüsse auf vertrauliche Vorgänge gewinnen.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 1.10 | Ausfall eines Weitverkehrsnetzes | | |
| G 1.19 | Ausfall eines Dienstleisters oder Zulieferers | | |
| G 4.31 | Ausfall oder Störung von Netzkomponenten | | |
| G 4.33 | Schlechte oder fehlende Authentikation | | |
| G 4.35 | Unsichere kryptographische Algorithmen | | |
| G 5.12 | Abhören von Telefongesprächen und Datenübertragungen | | |
| G 5.26 | Analyse des Nachrichtenflusses | | |
| G 5.28 | Verhinderung von Diensten | | |
| G 5.83 | Kompromittierung kryptographischer Schlüssel | | |
| G 5.84 | Gefälschte Zertifikate | | |
| G 5.165 | Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen | | |

## 3.4 Rechtliche Gefahren

### 3.4.1 Vertragsgestaltung

Wird das dispositive Recht nicht sorgfältig ausgestaltet und verbindlich festgeschrieben, drohen Anbietern von Cloud-Diensten insbesondere unkalkulierbare Haftungsansprüche, die von Kunden oder Geschäftspartnern geltend gemacht werden könnten.

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.1 | Fehlende oder unzureichende Regelungen | | |
| G 2.7 | Unerlaubte Ausübung von Rechten | | |
| G 2.61 | Unberechtigte Sammlung personenbezogener Daten | | |
| G 2.67 | Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten | | |
| G 2.83 | Fehlerhafte Outsourcing-Strategie | | |
| G 2.84 | Unzulängliche vertragliche Regelungen mit einem externen Dienstleister | | |
| G 2.85 | Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens | | |

### 3.4.2 Vertragsverletzung

Auch umfassende rechtliche Regelungen und Schutzversprechen bieten keine hundertprozentige Sicherheit: Verträge, Geschäftsbedingungen und rechtliche Rahmenbedingungen können gebrochen werden – versehentlich (etwa im Zusammenhang mit erfolgreichen externen Angriffen) oder willentlich.

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 1.19 | Ausfall eines Dienstleisters oder Zulieferers | | |
| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten | | |
| G 5.2 | Manipulation an Informationen oder Software | | |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen | | |
| G 5.85 | Integritätsverlust schützenswerter Informationen | | |
| G 5.107 | Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister | | |

# 4 Welche Risiken ergeben sich daraus?

Die Höhe eines Risikos wird definiert als ein Produkt aus den möglichen Konsequenzen und der Wahrscheinlichkeit, dass die Konsequenzen eintreten.

## 4.1 Mögliche Auswirkungen der Bedrohungen auf die Werte analysieren

Hier soll das Ausmaß der Konsequenzen für die einzelnen identifizierten Werte erfasst werden, wenn eine potenzielle Bedrohung Realität wird. Dazu wird folgende dreistufige Skala vorgeschlagen:

| Stufe | Definition | Maximale Dauer |
|---|---|---|
| Moderat | Ein gelegentliches Auftreten ist verkraftbar | Vorübergehende Beeinträchtigung |
| Ernst | Es entstehen eventuell signifikante Verluste | Längerfristiger Schaden |
| Katastrophal | Der Schaden kann ein existenzbedrohendes Ausmaß annehmen | Irreparabel |

*Tabelle 1: Dreistufige Skala möglicher Konsequenzen*

Tabelle 2 zeigt beispielhaft, wie die Konsequenzen ermittelt werden können. Zunächst werden für jedes Bedrohungsszenario jeweils die Gefährdungsstufen für jeden einzelnen potenziell betroffenen Wert abgeschätzt und die zugehörigen Werte-IDs werden entsprechend eingefärbt. Anschließend erfolgt eine Gesamtbeurteilung der möglichen Konsequenzen, die prinzipiell auch höher als die höchste Beurteilung für einzelne Assets ausfallen kann, nicht aber niedriger.

| Bedrohungsszenario/Gefahr | | Potenziell betroffene Werte (ID) | | | Konsequenz |
|---|---|---|---|---|---|
| ID | Bezeichnung | | | | |
| G 4.33 | Schlechte oder fehlende Authentikation | W 1.1 | W 1.2 | W 1.3 | Katastrophal |

*Tabelle 2: Potenzielle Konsequenzen für Werte*

## 4.2 Welche Sicherheitsmaßnahmen sind erforderlich?

Die Wahrscheinlichkeit, dass eine Bedrohung zu den möglichen Konsequenzen führen wird, soll so gering sein, dass das Risiko vertretbar ist. Dazu müssen für jede Bedrohung mit relevantem Gefährdungspotenzial bezüglich der identifizierten Werte geeignete Sicherheitsmaßnahmen getroffen werden. Die Tabelle im Anhang A benennt für die Bedrohungen und die Konsequenzstufen jeweils mögliche Maßnahmenpakete. Die einzelnen Maßnahmen werden im Anhang B beschrieben. Die Analysten haben die Aufgabe, jene Schutzmaßnahmen zu identifizieren, die mindestens notwendig sind, damit sämtliche schlimmstenfalls drohenden Konsequenzen ein tragbares Risiko sind. Für die weitere Anwendung des CSLA ist es zweckdienlich, eine Tabelle dafür anzulegen, so wie es Tabelle 3 exemplarisch zeigt.

| **Mindestens erforderliche Sicherheitsmaßnahme** | | | **Schutzlevel in möglichen Lösungen des Cloud-Dienstes** | | |
|---|---|---|---|---|---|
| **ID** | **Beschreibung** | **Schutzlevel** | *(Name Lösung 1)* | *(Name Lösung 2)* | *(Name Lösung 3)* |
| S 1.1 | Regelung des Zugriffs | Mittel | | | |

*Tabelle 3: Erforderliche Sicherheitsmaßnahmen und Schutzlevel*

# 5 Vertrauen schaffen

Bei jedem Angebot von Cloud-Diensten werden nach derzeitigem Stand der Technik immer Risiken bestehen. Vertrauensvoll genutzt werden nur solche Dienste, bei denen die Risiken in vernünftigem Verhältnis zum zu erwartenden Nutzen stehen. Um trotz bestehender Gefahren die Voraussetzungen zur Entstehung von Vertrauen zu schaffen, muss ein hinreichendes Sicherheitskonzept ausgearbeitet, implementiert und kommuniziert werden.

## 5.1 Schritte planen

Zur Konzeptionierung gilt es, den Handlungsbedarf bezüglich der Sicherheitsmaßnahmen zu erfassen. Bei einem bereits bestehenden Cloud-Dienst wird dazu analysiert, welcher Schutzlevel für die als notwendig erachteten Sicherheitsmaßnahmen jeweils tatsächlich erreicht wird. Eventuell ergibt es Sinn, verschiedene Schutzstufen für Nutzer mit unterschiedlichen Bedürfnissen und Prioritäten bezüglich der Sicherheit anzubieten. Für alle noch nicht umgesetzten Neuentwicklungen oder Weiterentwicklungen sind die angestrebten Schutzlevel ebenfalls zu bestimmen. Die Analyse sollte für jede existierende oder potenzielle Lösungsvariante zur Realisierung und zum Angebot des Cloud-Dienstes einzeln durchgeführt werden und jeweils als eigene Spalte in die Tabelle der erforderlichen und realisierten bzw. vorgesehenen Sicherheitsmaßnahmen eingetragen werden.

| **Mindestens erforderliche Sicherheitsmaßnahme** | | | **Schutzlevel in Angeboten für Cloud-Dienste** | | |
|---|---|---|---|---|---|
| **ID** | **Beschreibung** | **Schutzlevel** | **Aktueller Dienst** | **Weiter-entwicklung** | **Neu-entwicklung** |
| S 1.1 | Regelung des Zugriffs | Mittel | Rudimentär | Mittel | Hoch |
| S 1.2 | Authentifikation | Hoch | Rudimentär | Hoch | Hoch |
| S 1.3 | Schlüssel-management | Mittel | Mittel | Mittel | Hoch |
| S 1.5 | Verschlüsselung | Hoch | Mittel | Hoch | Hoch |

*Tabelle 4: Erforderliche sowie realisierte bzw. vorgesehene Sicherheitsmaßnahmen und Schutzlevel*

Anhand einer tabellarischen Übersicht, wie sie Tabelle 4 beispielhaft zeigt, lässt sich leicht erkennen, ob sämtliche mindestens geforderten Sicherheitsmaßnahmen abgedeckt werden. Außerdem lassen sich die verschiedenen bestehenden sowie potenziellen Schutzlösungen vergleichen – zumindest für einzelne Sicherheitsmaßnahmen. Daraus ergibt sich jedoch nicht notwendigerweise eine Ordnung bezüglich der Gesamtsicherheit der verschiedenen Sicherheitskonzepte, denn die Schwächen und Stärken verschiedener Lösungen können jeweils in anderen Bereichen liegen.

Wenn sich keine eindeutige Rangfolge aus der Gegenüberstellung der Schutzlevel ergibt, obwohl sehr unterschiedliche Schutzlevel für einzelne Sicherheitsmaßnahmen erreicht werden, kann eine Gewichtung der Bedeutung der einzelnen Sicherheitsmaßnahmen anhand der auf dem Spiel stehenden Werte vorgenommen werden. Für jedes Bedrohungsszenario und für jede Gefährdung wurden bereits die potenziell betroffenen Werte identifiziert. Über die Zuordnung der Sicherheitsmaßnahmen zu den Bedrohungsszenarien und Gefahren lässt sich auch für jede Sicherheitsmaßnahme ermitteln, was auf dem Spiel steht. Zu präferieren ist dann die Lösung, die bei den Sicherheitsmaßnahmen, von denen die größten Werte betroffen sind, den höchsten Schutzlevel verspricht.

Sicherheit ist nicht das einzige zu beachtende Kriterium bei der Planung der Sicherheitsmaßnahmen. Ebenso müssen der Preis und die Benutzbarkeit der verschiedenen Lösungsmöglichkeiten berücksichtigt werden. Wenn teurere Konzepte einen höheren Schutzlevel versprechen, sollten die Preisunterschiede direkt jenen Werten gegenübergestellt werden, die auf dem Spiel stehen und für die eine Abweichung beim gebotenen Schutz ermittelt wurde.

Ein Schutzlevel, der weit über den festgestellten Mindestanforderungen liegt, ergibt außerdem unter Umständen wenig Sinn, wenn dadurch die Benutzbarkeit stark beeinträchtigt wird.

## 5.2 Sicherheitsmaßnahmen implementieren

Die aufgrund der Analyse und Planung gewählten Sicherheitsmaßnahmen müssen umgesetzt werden, damit sie Wirkung entfalten können. Einige Bedrohungen für die Werte des Anbieters von Cloud-Diensten lassen sich mit den Sicherheitsmaßnahmen technisch weitgehend oder gar vollständig ausschließen, sofern die Maßnahmen korrekt implementiert werden.

Wenn jedoch ein Cloud-Dienst auch externen Interessenten angeboten wird, wenn auch Werte der (potenziellen) externen Nutzer betroffen sein können, so genügt die interne technische und organisatorische Absicherung durch den Anbieter mithilfe der Sicherheitsmaßnahmen für sich alleine nicht zur Vertrauensbildung seitens der möglichen Kunden, weil dann die Sicherheitsmaßnahmen für die externen Nutzer unsichtbar wären.

Besonderes Augenmerk bei der Umsetzung jeglicher Sicherheitsmaßnahmen sollte auf die korrekte Dokumentation des Vorgehens und aller sicherheitsrelevanten Aktivitäten sowie Vorkommnisse gelegt werden. Eine ausführliche Dokumentation sorgt nicht nur intern für Nachvollziehbarkeit, sondern sie ist auch die Grundlage zur Schaffung von Transparenz gegenüber Kunden und Dritten. Offenheit ist die Voraussetzung zur Schaffung von wohlbegründetem Vertrauen.

Alle realisierten Sicherheitsmaßnahmen sollten in den Verträgen für die Nutzung des Cloud-Angebots oder in ergänzenden rechtsverbindlichen Regelungen wie den allgemeinen Geschäftsbedingungen aufgeführt und möglichst stark garantiert werden. Die verbindliche Zusicherung der Sicherheitsmaßnahmen schafft Rechtssicherheit für alle Beteiligten. Sie signalisiert dem Nutzer, dass Sicherheit ernst genommen wird und dass die Schutzmaßnahmen im Eigeninteresse des Anbieters dauerhaft gewahrt und gewährleistet werden müssen, da andernfalls Schadensersatzansprüche gegen den Anbieter geltend gemacht werden könnten.

## 5.3 Prüfen und prüfen lassen

Ein weiteres wichtiges Konzept zum Aufbau von Vertrauen sind Prüfungen bestimmter kritischer Prozesse und Eigenschaften. Prüfungen können die Qualität von Sicherheitsmaßnahmen bestätigen, idealerweise objektiv. Die Durchführung und die Ergebnisse von Sicherheitsprüfungen sollten in die öffentliche Dokumentation der Sicherheitsmaßnahmen einfließen.

Effektiv im Sinne der Vertrauensbildung sind Prüfungen, wenn sie von möglichst unabhängigen Institutionen durchgeführt werden – oder wenn die Prüfungen sogar durch die (potenziellen) Kunden selbst durchgeführt bzw. zumindest überwacht werden können. Als externe Prüfer sind insbesondere jene Institutionen und Personen interessant, die Konformität mit bestimmten Sicherheitsstandards prüfen und zertifizieren dürfen. Zertifizierungen können beispielsweise durch vom BSI anerkannte Prüfstellen nach ITSEC, Common Criteria (CC), Technischen Richtlinien (TR), dem Signaturgesetz und insbesondere nach ISO 27001 auf Basis des IT-Grundschutzes erteilt werden.

Andererseits sind externe Prüfungen und insbesondere offizielle Zertifikationen mit erheblichen Aufwendungen verbunden. Die Durchführung kostspieliger Prüfungen lohnt besonders dann, wenn der Anbieter bisher nur wenig Vertrauen gewinnen konnte und wenn für die Nutzer viel auf dem Spiel steht.

## 5.4 Kommunizieren

Das Vorhandensein von Sicherheitsmaßnahmen und etwaigen Prüfergebnissen wird erst dann tatsächlich Vertrauen schaffen können, wenn die Sicherheitseigenschaften den (potenziellen) Nutzern bekannt und verständlich gemacht werden. Hier werden kompakte Formen der Darstellung der Ergebnisse der Risikoanalyse und der Sicherheitskonzeption vorgestellt, die insbesondere die Anwendung im Cloud-Sicherheits-Leitfaden für die Nutzer von Cloud-Diensten (CSLN) erleichtern sollen.

### 5.4.1 Risikobericht mit Sicherheitsmaßnahmen für Nutzer

Für die vollständige intuitiv verständliche Darstellung der Analyse aus Sicht des Nutzers wird hier eine grafische Notation vorgeschlagen, die in der CORAS-Methode zur Risikoanalyse vorgestellt wird. Abbildung 2 zeigt exemplarisch, wie die Darstellung als Risikograph mit Sicherheitsmaßnahmen aussehen kann. Abbildung 3 beschreibt kurz die einzelnen Elemente des Graphen.

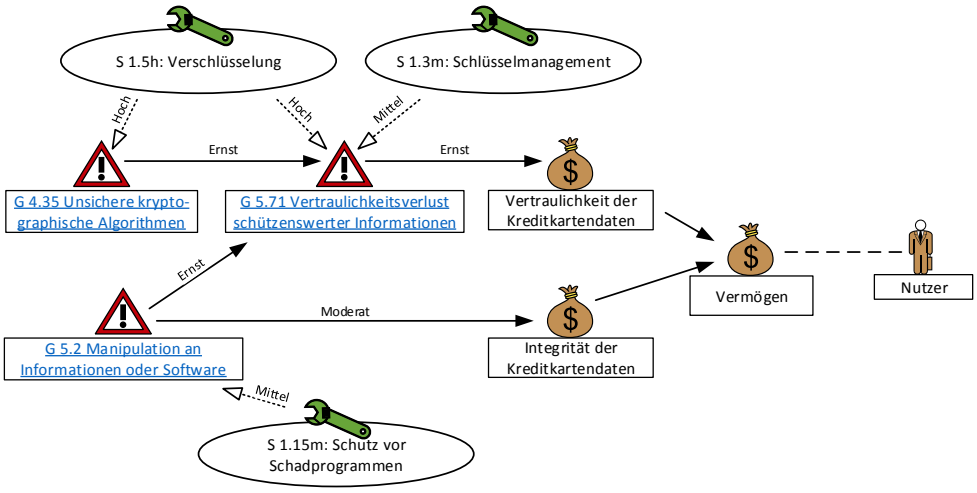



Abbildung 2: Beispielhafter Risikograph mit Sicherheitsmaßnahmen und Schutzlevel

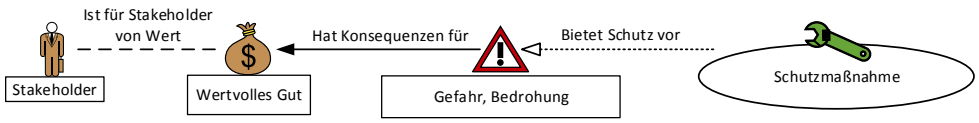



Abbildung 3: Legende für den Risikographen mit Sicherheitsmaßnahmen und Schutzlevel

### 5.4.2 Schutzstärkebericht für Nutzer

Die Darstellung der Sicherheitsmaßnahmen mit Schutzlevel für alle extern tatsächlich angebotenen Cloud-Dienste kann im Wesentlichen wie in Tabelle 4 erfolgen, für den CSLN können jedoch ergänzende Informationen integriert werden: Sicherheitstechnische Maßnahmen, die beispielsweise nur in der Dokumentation erwähnt werden und nicht im Vertrag sowie in ergänzenden rechtsverbindlichen Bestimmungen garantiert werden, bieten eine geringe Verlässlichkeit. Nicht rechtsverbindlich garantierte Sicherheitsmaßnahmen sind in der Liste mit einem Minus zu kennzeichnen.

Eine erhöhte Verlässlichkeit ergibt sich, wenn bestimmte Sicherheitsmaßnahmen nicht nur vom Anbieter selbst rechtsverbindlich zugesichert werden, sondern wenn auch eine unabhängige Partei diese geprüft hat und dies bescheinigt. Durch Zertifikate verbürgte Sicherheitsmaßnahmen sind in der Liste mit einem Pluszeichen hervorzuheben.

Für jene Maßnahmen, die in den Verträgen oder anderen rechtsverbindlichen Dokumenten geregelt sind, sollte jeweils auf die Stellen verwiesen werden, an denen die Regelungen zu finden sind. Ebenso sollte, falls Zertifikate bestehen, auf die Zertifikate verwiesen werden. Tabelle 5 zeigt exemplarisch, wie ein tabellarischer Schutzstärkebericht der realisierten Schutzlevel bei verschiedenen Angeboten für einen Cloud-Dienst aussehen kann.

| **Realisierte Sicherheitsmaßnahmen** | | **Schutzlevel in den Angeboten für Cloud-Dienste** | | | |
|---|---|---|---|---|---|
| **ID** | **Beschreibung** | **Standarddienst** | | **Neuer Premiumdienst** | |
| S 1.1 | Regelung des Zugriffs | Mittel | AGB § 12.1 | Hoch + | Zertifikat X.23a, AGB § 12.1 |
| S 1.2 | Authentifikation | Hoch – | | Hoch + | Zertifikat X.23a, Vertrag § 9 |
| S 1.3 | Schlüssel-management | Mittel – | | Hoch + | Zertifikat X.23c, Vertrag § 9 |
| S 1.5 | Verschlüsselung | Hoch | Vertrag §7.4 | Hoch + | Zertifikat X.22, Vertrag § 7.4 |

*Tabelle 5: Realisierte Sicherheitsmaßnahmen und Schutzlevel, Darstellung für (potenzielle) Nutzer*

# 6 Weiterführende Literatur

## 6.1 IT-Sicherheit

ISO 27000: Information technology – Security techniques – Information security management systems, International Organization for Standardization 2014

BSI: IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik 2005–2014

CWE: Common Weakness Enumeration, Mitre 2006–2014

CAPEC: Common Attack Pattern Enumeration and Classification, Mitre 2007–2014

## 6.2 Risikoanalyse

ISO 31000: Risk management – Principles and guidelines, International Organization for Standardization 2009

CORAS: M. S. Lund, B. Solhaug, K. Stølen: Model-Driven Risk Analysis – The CORAS Approach, Springer (2011)

## 6.3 Rechtliche Grundlagen

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

BDSG: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist

SigG: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

TMG: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist

## 6.4 IT allgemein

UML: Unified Modeling Language, OMG Object Management Group 1997–2014

NIST Cloud Definition: Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, Special Publication 800 – 145, U. S. Department of Commerce 2011

# Cloud-Sicherheits-Leitfaden für Nutzer (CSLN)

# Zusammenfassung

Der vorliegende Cloud-Sicherheits-Leitfaden für Nutzer von Cloud-Diensten (CSLN) bietet kleinen Unternehmen, Selbstständigen und Privatpersonen Hilfestellungen für die sicherheitstechnische Analyse des (möglichen) Einsatzes von externen Cloud-Angeboten (Public Cloud Services). Der CSLN soll insbesondere die Auswahl von geeigneten Cloud-Diensten erleichtern und helfen, ein Bewusstsein für die bestehenden Risiken zu schaffen und zur Risikoreduktion beitragen. Dazu wird eine Methode zur Risikoanalyse vorgestellt, die auch für Personen, die keine IT-Security-Experten sind, mithilfe des CSLN zu bewältigen sein soll. Außerdem wird ein Entscheidungsfindungsprozess zur Auswahl von Cloud-Diensten aus einer Managementperspektive vorgestellt, der die in der Risikoanalyse ermittelten Sicherheitsanforderungen berücksichtigt.

Hinweis zur Version 0.1:
Dieser Leitfaden befindet sich noch in der Entwicklung. Anregungen zur Verbesserung sind willkommen. Die bisher nur vorläufigen BSI-Grundschutz-Bausteine zum Thema Cloud sind noch nicht vollständig integriert.

# 1 Einleitung zum Cloud-Sicherheits-Leitfaden für Nutzer (CSLN)

## 1.1 Bedeutung von Informationssicherheit im Zusammenhang mit Cloud Computing

Cloud Computing ist eine Bezeichnung für verschiedene Formen von serviceorientierten Virtualisierungen in verteilten Computersystemen. Public-Cloud-Lösungen, bei denen die Cloud-Dienste von fremden Anbietern genutzt werden, haben einen besonders schweren Stand, was Vertrauen und Sicherheit angeht. Der Grund liegt in dem externen Anbieter – diesem muss in der Regel vertraut werden und es bestehen Abhängigkeiten von dessen Leistungen, die nicht kontrolliert werden können. Außerdem existieren je nach Rechtsraum verschiedene rechtliche Schranken bezüglich der Zulässigkeit von Outsourcing.

Dennoch kann nicht einfach pauschal davon ausgegangen werden, dass private Clouds oder herkömmliche Lösungen auf einzelnen physischen Rechnern unter eigener Kontrolle sicherer seien. Viele Anbieter von Public-Cloud-Diensten betreiben schließlich einen erheblichen Aufwand für die Gewährung von Sicherheit, der von Privatpersonen oder Selbstständigen, die keine IT-Experten sind, und von vielen kleinen oder mittelständischen Betrieben kaum geleistet werden kann.

Es ist im Einzelfall abzuwägen, welche Lösungen die größtmögliche Sicherheit mit den verfügbaren Mitteln bieten können. Dabei sind die rechtlichen, sicherheitstechnischen, funktionalen und wirtschaftlichen Anforderungen sowie Interessen oftmals gegensätzlich und es lässt sich eventuell keine eindeutig beste Lösung finden. Der vorliegende Cloud-Sicherheits-Leitfaden für Nutzer (CSLN) soll genau bei diesem Optimierungsproblem helfen und beim Treffen wohlbegründeter Entscheidungen unterstützen.

## 1.2 Aufbau und Funktion des CSLN

Der Cloud-Sicherheits-Leitfaden für Nutzer besteht im Wesentlichen aus einer dreistufigen Methode zur Risikoanalyse für cloudbasierte IKT-Projekte und aus einem Entscheidungsfindungsverfahren zur Beurteilung von Cloud-Diensten. Das Entscheidungsverfahren stützt sich auf die Ergebnisse der Risikoanalyse und untersucht, wie hoch die identifizierten Risiken bei der Nutzung konkreter Cloud-Dienste wären, um die Gesamtlösung zu finden, die das beste Verhältnis aus Sicherheit und Kosten bietet. Abbildung 1 visualisiert die Konzepte.

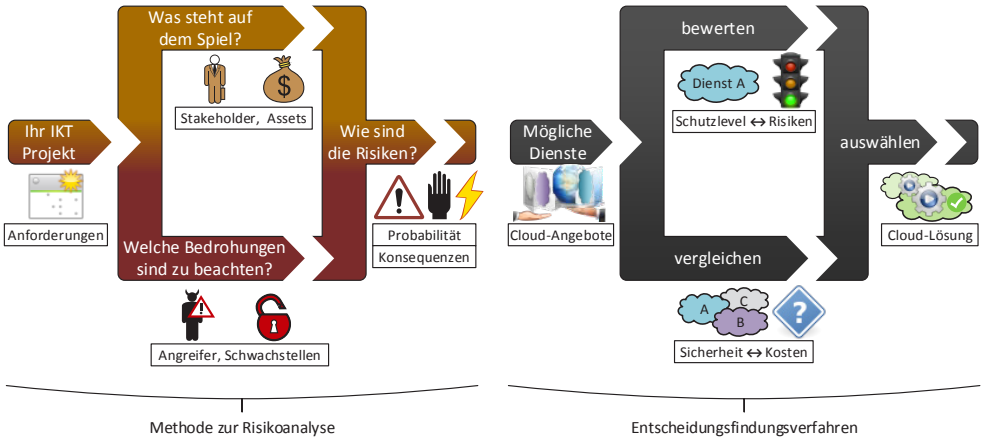



Abbildung 1: Konzeptuelle Übersicht zum Cloud-Sicherheits-Leitfaden für Nutzer (CSLN)

## 1.3 Ein offenes Wort – Limitationen des CSLN

**Einsatzgebiet und Voraussetzungen des CSLN**

Der Cloud-Sicherheits-Leitfaden für Nutzer bietet ausschließlich sicherheitstechnische und sicherheitsökonomische Hilfestellungen für IKT-Projekte, die mithilfe von externen Cloud-Diensten realisiert werden können. Damit der CSLN angewandt werden kann, müssen die funktionalen Anforderungen bekannt sein. Zur Darstellung dieser Anforderungen können beispielsweise UML-Use-Case-Diagramme verwendet werden. Für die Analyse der funktionalen Anforderungen bietet der CSLN keine weiter gehende Unterstützung. Auch die Hilfestellungen des CSLN für die Auswahl der Public-Cloud-Dienste beschränken sich auf die Sicherheitsaspekte. Die Frage, welche Cloud-Dienste benötigt werden, damit das Projekt die sonstigen (insbesondere funktionalen) Anforderungen erfüllen kann, lässt sich nicht mithilfe des CSLN beantworten.

Damit der CSLN angewandt werden kann, müssen außerdem über die externen Cloud-Dienste und deren Betreiber Informationen zu deren Sicherheitsmaßnahmen eingeholt werden. Idealerweise sollten die Anbieter mithilfe des Cloud-Sicherheits-Leitfaden für Anbieter (CSLA) die notwendigen Daten erheben, aufbereiten und allen potenziellen Kunden zur Verfügung stellen.

**IKT-Sicherheit ist und bleibt eine Herausforderung**

Dieser Leitfaden ist als eine erste Orientierungshilfe konzipiert, um eine systematische Auseinandersetzung mit den Themen Sicherheits- und Risikomanagement im Zusammenhang mit Public-Cloud-Technologien zu ermöglichen. Die korrekte und hinreichend gründliche Anwendung der hier vorgestellten Verfahren zur Analyse sowie zur Entscheidungsfindung ist eine anspruchsvolle, interdisziplinäre Aufgabe.

**Sicherheit ist kostspielig**

Maßnahmen, die Sicherheit sowie Vertrauen schaffen und Risiken reduzieren sollen, sind oftmals mit erheblichen Aufwendungen verbunden. Auch die Benutzerfreundlichkeit kann durch starke Sicherheitskonzepte beeinträchtigt werden. Wenn andererseits aufgrund von mangelhaften Sicherheitsmaßnahmen Schäden entstehen, kann dies ebenfalls sehr teuer werden und die weitere Benutzung kann erschwert oder unmöglich werden. Verspieltes Vertrauen kann ein irreparabler Schaden sein. In der Praxis gilt es, vernünftige Kompromisse zu finden.

**Sicherheit ist nie vollkommen**

Auch eine korrekte Befolgung des CSLN kann keine hundertprozentige Sicherheit garantieren. Es wird kein Anspruch auf Vollständigkeit erhoben. Der Gebrauch dieses Leitfadens entbindet nicht von der Sorgfaltspflicht. Auch hier nicht erwähnte potenzielle Bedrohungen sowie Risiken müssen beachtet werden und es gilt, angemessen darauf zu reagieren. Im Zweifelsfall sollte zusätzlich Rat bei Security-Experten und Juristen eingeholt werden – oder es sollte auf den Einsatz von Public-Cloud-Technologien externer Anbieter verzichtet werden.

# 2 Was steht eigentlich auf dem Spiel?

Eine mögliche Annäherung an das Thema Sicherheit besteht darin, sich zunächst mit dem zu beschäftigen, was gefährdet werden könnte – also mit den Dingen, die passieren können, wenn Sicherheit nicht gegeben wäre. Um zu erfassen, welche Gefahren bestehen, sollte zunächst geklärt werden, wer überhaupt betroffen sein könnte, wenn etwas schiefläuft. Dies wird mit der Identifizierung der Stakeholder geleistet. In einem zweiten Schritt sollte dann identifiziert werden, welche Werte der potenziell Betroffenen beeinträchtigt werden könnten. Hierzu dient die Wertanalyse.

Bevor mit der Stakeholder-Analyse und der Wertanalyse begonnen wird, sollten die funktionalen Anforderungen an das IKT-System klar bestimmt, festgeschrieben und verstanden sein. Es ist zweckdienlich, als Vorbereitung eine mögliche generische Lösung zu modellieren, damit ein Bewusstsein dafür entsteht, welche Akteure zu beachten sind, welche Cloud-Dienste aufgrund der funktionalen Anforderungen benötigt werden, was die Cloud-Dienste genau machen sollen und welche Daten sie verarbeiten sollen.

## 2.1 Identifizieren der Stakeholder

Hier werden eine Reihe von generischen Stakeholdern vorgestellt, die typischerweise zu beachten sind. In der Analyse kann je nach Bedarf auch eine präzisere Gliederung mit feiner unterteilten Stakeholder-Typen vorgenommen werden.

### 2.1.1 Nutzer

Nutzer sind im Sinne des CSLN diejenigen natürlichen Personen oder Organisationseinheiten, die selbst die Verwendung von externen Cloud-Diensten erwägen. Nutzer tauchen typischerweise als Akteure in der Analyse der funktionalen Anforderungen auf, die der CSLN voraussetzt.

### 2.1.2 Eigner der Nutzer

Sofern in einem Unternehmen die Verwendung von externen Cloud-Diensten erwogen wird, sind auch die Eigner, die Anteile am Unternehmen besitzen, als Stakeholder zu berücksichtigen.

### 2.1.3 Angestellte

Zusätzlich sind in einem Unternehmen, in dem die Verwendung von Cloud-Diensten erwogen wird, auch die Angestellten zu beachten.

### 2.1.4 Kunden und Geschäftspartner der Nutzer

Die Begriffe Kunden und Geschäftspartner beziehen sich hier nicht auf die Kunden und Geschäftspartner der Anbieter der Cloud-Dienste, sondern auf die Kunden und Geschäftspartner der Nutzer, also jener Unternehmen, natürlichen Personen oder Organisationseinheiten, die die Verwendung von Cloud-Diensten erwägen.

Eigner, Mitarbeiter, Kunden und Geschäftspartner können auch selbst (potenzielle) Nutzer der Cloud-Dienste sein, dies ist jedoch nicht zwangsläufig der Fall.

### 2.1.5 Anbieter

Anbieter sind Unternehmen, die externe Cloud-Dienste zur Verfügung stellen, die die Nutzer bereits verwenden oder deren zukünftige Verwendung sie erwägen.

### 2.1.6 Öffentlich-rechtliche Institutionen

Als öffentlich-rechtliche Stakeholder sind politische Unionen, Staaten und Behörden zu berücksichtigen.

### 2.1.7 Dritte

Personen, die nicht in eine der genannten Kategorien von Stakeholdern passen, aber trotzdem betroffen sein könnten, werden hier als Dritte bezeichnet. Dies können beispielsweise externe Personen sein, über die Daten gesammelt werden, obwohl sie keine Kunden sind.

## 2.2 Analysieren der Werte

In diesem Schritt wird analysiert, was für die identifizierten Stakeholder im Zusammenhang mit dem Projekt von Wert ist bzw. von Wert sein könnte und gefährdet werden könnte. Es ist zweckdienlich, für jeden erfassten Typ von Stakeholder eine eigene Analyse der möglicherweise betroffenen Werte durchzuführen. Jeder einzelne identifizierte Wert sollte mit einer eindeutigen ID versehen werden.

### 2.2.1 Käufliche Werte

Diese Güter sind dadurch gekennzeichnet, dass sie sich auf dem Markt handeln lassen. Mithin ist es relativ einfach möglich, hierfür einen Preis zu ermitteln. Verluste dieser Werte lassen sich oftmals mit Geld wieder ausgleichen. Hierzu gehören:

- Finanzvermögen
  - Bargeld
  - Aktien
  - Bankguthaben

- materielle Sachwerte
  - Immobilien
  - Grundstücke
  - Fahrzeuge
  - Computer und Maschinen

- (informationstechnische) Dienstleistungen

### 2.2.2 Unveräußerliche Werte

Unveräußerliche Werte können prinzipiell nicht durch Kauf erlangt werden. Werden unveräußerliche Werte verletzt, so kann dies trotzdem zu erheblichen, auch direkt finanziellen Verlusten führen. Eventuell drohen zusätzlich juristische Sanktionen. Einmal entstandene Verluste lassen sich mit Geld in der Regel nicht ohne weiteres kompensieren. Beispiele sind:

- Vertrauenswürdigkeit
- Reputation
- Persönlichkeitsrecht

### 2.2.3 Immaterielle Werte

Immaterielle Werte lassen sich durchaus auf einem freien Markt kaufen und verkaufen, zumindest solange sie geheim sind. Für sie lässt sich also prinzipiell ein Verkaufspreis ermitteln. Umgekehrt lassen sich einmal preisgegebene und publik gewordene Informationen jedoch nicht wieder unter Verschluss bringen. Ein Rückkauf im Verlustfall ist allgemein nicht möglich. An immateriellen Werten sind zu beachten:

- private Daten, vertrauliche Kundendaten, Unternehmensdaten, Geschäftsgeheimnisse
  - Authentizität, Integrität, Verfügbarkeit, Geheimhaltung

- urheberrechtlich geschützte Daten

### 2.2.4 Detailgrad der Wertanalyse

Für einzelne Güter wie beispielsweise für Kreditkartendaten von Kunden kann es Sinn ergeben, bereits bei der Wertanalyse genau das, was an dem Gut gefährdet werden könnte, was verloren gehen könnte, als eigenständige Werte zu erfassen. Im Beispiel mit dem Gut Kreditkartendaten würde das bedeuten, statt einfach nur die Kreditkartendaten als Wert zu identifizieren, die Geheimhaltung, die Authentizität, die Integrität und die Gültigkeit (Aktualität) der Kreditkartendaten jeweils als eigene Werte aufzunehmen. Dies erleichtert die Identifikation von relevanten Bedrohungsszenarien sowie Gefährdungen und die anschließende Beurteilung der potenziellen Konsequenzen.

# 3 Welche Bedrohungen sind zu beachten?

Dieses Kapitel besteht im Wesentlichen aus einer Auflistung von Bedrohungsszenarien, denen IKT-Lösungen mit externen Cloud-Diensten typischerweise ausgesetzt sind. Die Aufgabe für den Analysten ist, jene Bedrohungen herauszufiltern und zu verstehen, die Auswirkungen auf die zuvor identifizierten Werte haben könnten. Dazu können die entsprechenden Werte-IDs aus der Wertanalyse in den nachfolgenden Tabellen in die Zeile des jeweiligen Bedrohungsszenarios geschrieben werden.

Die folgende Aufstellung der potenziellen Bedrohungsszenarien orientiert sich an den (teils vorläufigen) BSI-Grundschutz-Katalog-Bausteinen B 1.1.1 Outsourcing, B 5.23 Cloud-Management, B 5.24 Web-Services und B 5.25 Cloud-Nutzung. Die einzelnen Bedrohungen werden mithilfe von Gefahren-IDs aus dem BSI-Grundschutz-Katalog identifiziert. Ausführliche Beschreibungen der einzelnen Gefahren und Bedrohungsszenarien finden sich im BSI-Grundschutz-Katalog.

## 3.1 Bedrohungen durch einen externen Cloud-Dienst und dessen Anbieter

Diese Gefährdungen sind für jeden einzelnen externen Cloud-Dienst separat zu analysieren.

### 3.1.1 Rechtliche Gefahren

Erstens kann es rechtlich unzulässig sein, für bestimmte IT-Dienstleistungen auf externe Anbieter zurückzugreifen. Dies gilt insbesondere, wenn die Dienste der Anbieter in einem anderen Rechtsraum betrieben werden (siehe dazu Richtlinie 95/46/EG). Eventuell rechtlich unzulässiges Outsourcing ist unter der Gefahr G 2.83 einzutragen. Zweitens kann ein externer Anbieter seine Dienste im Rahmen der rechtsverbindlichen Übereinkünfte mit den Nutzern frei gestalten. Wenn dieser Gestaltungsspielraum zu groß ist (G 2.1, G 2.84, G 2.85), so können daraus Nachteile und Schäden für die Nutzer entstehen.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.1 | Fehlende oder unzureichende Regelungen | | |
| G 2.83 | Fehlerhafte Outsourcing-Strategie | | |
| G 2.84 | Unzulängliche vertragliche Regelungen mit einem externen Dienstleister | | |
| G 2.85 | Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens | | |

### 3.1.2 Sich vertragswidrig verhaltende Anbieter

Auch umfassende rechtliche Regelungen und Schutzversprechen bieten keine hundertprozentige Sicherheit: Verträge, Geschäftsbedingungen und rechtliche Rahmenbedingungen können durch den Anbieter gebrochen werden – versehentlich (etwa im Zusammenhang mit erfolgreichen externen Angriffen) oder willentlich.

So kann die garantierte Verfügbarkeit von Cloud-Diensten im laufenden Betrieb unterschritten werden (G 1.19). Die Schäden sind zwar in der Regel temporär begrenzt, aber anhaltende oder wiederkehrende Verfügbarkeitsprobleme können etwa auch zu dauerhaften Imageschäden für Nutzer der Cloud-Dienste gegenüber etwaigen Kunden der Nutzer führen. Anders als bei internen IT-Lösungen können durch die Nutzer externer Cloud-Dienste keine Maßnahmen zur Behebung von Ausfällen ergriffen werden, die Nutzer sind von den Anbietern abhängig. Daher spielt es auch keine Rolle, was der Grund für den Ausfall ist: Selbst wenn beispielsweise externe (Distributed-) Denial-of-Service-Attacken für Ausfälle verantwortlich sein sollten, so ist die Hauptgefahr aus Sicht des Nutzers der Anbieter, der darauf eventuell nicht hinreichend und angemessen reagieren wird.

Vertrauliche Daten können durch Anbieter von Cloud-Diensten willentlich weitergegeben (G 5.107) oder sie können gestohlen werden, wofür bereits ein einmaliger lesender Zugriff auf die Daten genügt (G 3.1, G 5.71). Angriffe können sich sowohl auf die Kommunikationskanäle als auch auf Speichersysteme richten. Selbst wenn Daten immer sicher verschlüsselt gespeichert und übertragen werden, können sie eventuell an der Schnittstelle zu menschlichen Nutzern ausgelesen werden (Analog-Gap). Datendiebstahl beeinträchtigt nicht notwendigerweise das technische Angriffsziel, er ist schwer festzustellen und hinterlässt eventuell keinerlei Spuren. Schaden entsteht erst durch den Missbrauch der gestohlenen vertraulichen Daten. Einmal gebrochene Vertraulichkeit lässt sich kaum reparieren, da Informationen reproduzierbar und mithin kaum aus der Welt zu schaffen sind.

Die Manipulation von Daten (G 3.1, G 5.85) und Programmen (G 5.2) erfordert auch schreibenden Zugriff, den zumindest Anbieter grundsätzlich ausüben können. Manipulationen können anders als der Datendiebstahl unmittelbar Schäden verursachen.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 1.19 | Ausfall eines Dienstleisters oder Zulieferers | | |
| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten | | |
| G 5.2 | Manipulation an Informationen oder Software | | |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen | | |
| G 5.85 | Integritätsverlust schützenswerter Informationen | | |
| G 5.107 | Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister | | |

### 3.1.3 Lock-in

Als Lock-in wird die dauerhafte Abhängigkeit (G 2.86) von einzelnen Anbietern und ihren Cloud-Diensten bezeichnet. Externe Dienste können im Laufe der Zeit vom Anbieter verändert oder ganz eingestellt werden, sodass die bisherige Nutzung nicht fortgeführt werden kann (G 2.85). Eventuell werden die Suche nach alternativen Anbietern, die Entwicklung neuer Lösungen mit anderen Cloud-Diensten sowie gegebenenfalls die Migration bestehender Daten mit hohem Aufwand, Ausfällen und Verlusten verbunden sein.

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.85 | Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens | | |
| G 2.86 | Abhängigkeit von einem Outsourcing-Dienstleister | | |

### 3.1.4 Bedrohungen durch die Cloud-Plattform

Die bisher genannten Bedrohungen betreffen die Nutzung von Cloud-Diensten externer Anbieter und resultieren im Wesentlichen aus der Abhängigkeit von diesen Anbietern. Technische Angriffe gegen Cloud-Plattformen bedrohen hingegen prinzipiell auch interne Cloud-Lösungen.

Grundlage der Cloud ist die Virtualisierung. Die Virtualisierung an sich schafft mindestens eine zusätzliche Ebene, die angegriffen werden kann. Die Virtualisierungsumgebung selbst (G 5.150) und die von ihr bereitgestellten Funktionen (G 5.148) können missbraucht werden, beispielsweise die Erzeugung von Snapshots (G 3.100). Auch die Verwaltung (G 3.102, G 4.76) und die Vernetzung (G 4.75, G 5.147) der Virtualisierung bieten eventuell Angriffspunkte. Schließlich können auch die Tools (G 2.150, G 3.101, G 4.77, G 5.147) und Anwendungen (G 2.151), die in der Virtualisierung betrieben werden, Probleme bereiten.

Eine Klasse von Gefahren bilden unzureichende physische IT-Systeme, auf denen die Virtualisierung betrieben wird (G 2.32, G 2.149, G 3.99, G 4.74, G 4.75, G 4.76, G 4.77). Ursachen können etwa eine zu geringe Redundanz oder mangelhafte Leistungsreserven für den gleichzeitigen Zugriff durch viele Nutzer sein. Es handelt sich oftmals um Planungsfehler (G 2.148), aufgrund des Kostendrucks sind Anbieter von Cloud-Diensten versucht, die technische Basis knapp zu halten.

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.32 | Unzureichende Leitungskapazitäten | | |
| G 2.148 | Fehlerhafte Planung der Virtualisierung | | |
| G 2.149 | Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme | | |
| G 2.150 | Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen | | |
| G 2.151 | Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen | | |
| G 3.99 | Fehlerhafte Netzanbindungen eines Virtualisierungsservers | | |
| G 3.100 | Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme | | |
| G 3.101 | Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen | | |
| G 3.102 | Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen | | |
| G 4.74 | Ausfall von IT-Komponenten in einer virtualisierten Umgebung | | |
| G 4.75 | Störung der Netzinfrastruktur von Virtualisierungsumgebungen | | |
| G 4.76 | Ausfall von Verwaltungsservern für Virtualisierungssysteme | | |
| G 4.77 | Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen | | |
| G 5.147 | Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes | | |
| G 5.148 | Missbrauch von Virtualisierungsfunktionen | | |
| G 5.149 | Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen | | |
| G 5.150 | Kompromittierung des Hypervisors virtueller IT-Systeme | | |

## 3.2 Bedrohungen von IKT-Systemen

Die bei IKT-Systemen allgemein zu beachtenden Angriffsszenarien sind auch bei Cloud-Lösungen zu berücksichtigen – und zwar für alle beteiligten Systeme nicht nur in der Cloud, sondern auch außerhalb, etwa für Zugangssysteme der Nutzer. Zu diesen Bedrohungen zählen insbesondere gezielter Diebstahl (G 4.33, G 4.35, G 5.4, G 5.71), Manipulationen (G 5.1, G 5.3, G 5.85) und die Ausführung von schädlichen Programmen (G 4.22, G 5.2, G 5.173) durch externe Angreifer.

Zu den Werkzeugen von externen Angreifern gehören insbesondere Schadprogramme (G 5.23) wie Computerviren und Spähprogramme (Spyware). Als informationstechnische Türöffner dienen neben Schwachstellen in Programmen auch trojanische Pferde (G 5.21), die durch unachtsame Anwender eingeschleppt und zur Ausführung gebracht werden.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 4.22 | Software-Schwachstellen oder -Fehler | | |
| G 4.33 | Schlechte oder fehlende Authentikation | | |
| G 4.35 | Unsichere kryptographische Algorithmen | | |
| G 5.1 | Manipulation oder Zerstörung von Geräten oder Zubehör | | |
| G 5.2 | Manipulation an Informationen oder Software | | |
| G 5.3 | Unbefugtes Eindringen in ein Gebäude | | |
| G 5.4 | Diebstahl | | |
| G 5.21 | Trojanische Pferde | | |
| G 5.23 | Schadprogramme | | |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen | | |
| G 5.85 | Integritätsverlust schützenswerter Informationen | | |
| G 5.173 | Einbindung von fremden Daten und Schadcode bei Webanwendungen | | |

## 3.3 Gefährdungen der Kommunikation und des Zusammenspiels

Diese Bedrohungen sind für alle Cloud-Dienste und Zugangssysteme im Zusammenspiel zu analysieren. Die Gefährdungen gehen von Systemen und Infrastrukturen aus, die weder die Nutzer noch die Anbieter von Cloud-Diensten kontrollieren können.

Ausfälle von Internetknoten, Providern und Störungen von Leitungen können die Verfügbarkeit von Cloud-Diensten einschränken (G 1.10, G 1.19, G 4.31, G 5.28).

Verbindungen zu Cloud-Diensten werden oftmals über gesicherte Protokolle wie SSL/TLS (https://...) hergestellt. In der Vergangenheit gab es jedoch wiederholt erfolgreiche Manipulationen und Attacken, insbesondere mit kompromittierten privaten Schlüsseln (G 5.83) und gefälschten Zertifikaten (G 5.84), wodurch die Authentifikation unterwandert werden könnte (G 4.33).

Die Gefahren von unzureichender Verschlüsselung (G 4.35, G 5.12, G 5.165) sollten spätestens seit den Enthüllungen über die groß angelegte systematische Überwachung von Datenströmen durch die NSA ernst genommen werden. Eine Analyse des Nachrichtenflusses (G 5.26), also wo überhaupt Daten in welchem Umfang ausgetauscht werden, lässt sich auch ohne Entschlüsselung durchführen und daraus lassen sich eventuell bereits Rückschlüsse auf vertrauliche Vorgänge gewinnen.

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 1.10 | Ausfall eines Weitverkehrsnetzes | | |
| G 1.19 | Ausfall eines Dienstleisters oder Zulieferers | | |
| G 4.31 | Ausfall oder Störung von Netzkomponenten | | |
| G 4.33 | Schlechte oder fehlende Authentikation | | |
| G 4.35 | Unsichere kryptographische Algorithmen | | |
| G 5.12 | Abhören von Telefongesprächen und Datenübertragungen | | |
| G 5.26 | Analyse des Nachrichtenflusses | | |
| G 5.28 | Verhinderung von Diensten | | |
| G 5.83 | Kompromittierung kryptographischer Schlüssel | | |
| G 5.84 | Gefälschte Zertifikate | | |
| G 5.165 | Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen | | |

## 3.4 Gefährdungen aufseiten der Nutzer

Neben den Anbietern von Cloud-Diensten, den IKT-Systemen und Kommunikationskanälen können auch die Nutzer ein Risiko sein. Unwissen, Unachtsamkeit, menschliche Fehler und das gezielte Eingehen von Risiken sind die wichtigsten Ursachen für Gefährdungen durch die Nutzer.

Aus Unwissenheit werden oftmals die gebotenen Sicherheitsmaßnahmen nicht oder falsch umgesetzt, sodass sie keine Wirkung entfalten können (G 2.2, G 2.103). Davon können insbesondere externe Angreifer profitieren.

Sicherheitsmaßnahmen verlangen oftmals wiederkehrende, lästige Tätigkeiten. Gewohnheit und Bequemlichkeit können dazu führen, dass trotz hinreichendem Wissen die nötige Aufmerksamkeit abnimmt und so die Wirksamkeit der Maßnahmen schwindet (G 2.102, G 3.3, G 3.43, G 3.44).

Selbst bei hoher Sensibilität für Sicherheitsrisiken und bei voller Aufmerksamkeit machen Menschen Fehler. Fehler können direkt Schäden verursachen oder externen Angreifern in die Hände spielen (G 3.1, G 3.8).

Wenn mehrere Nutzer dieselben Cloud-Dienste nutzen und teilweise überlappende Zugriffsrechte für die einzelnen Nutzer vergeben werden, so besteht eventuell die Gefahr, dass die gewährten Privilegien entgegen den rechtlichen Nutzungsbedingungen eingesetzt werden, um eigene Interessen durchzusetzen oder um anderen Personen zu schaden (G 2.7, G 3.3, G 5.19).

| **Bedrohungsszenario/Gefahr** | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Potenziell betroffene Werte (ID)** | **Konsequenz** |
| G 2.2 | Unzureichende Kenntnis über Regelungen | | |
| G 2.7 | Unerlaubte Ausübung von Rechten | | |
| G 2.102 | Unzureichende Sensibilisierung für Informationssicherheit | | |
| G 2.103 | Unzureichende Schulung der Mitarbeiter | | |
| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten | | |
| G 3.3 | Nichtbeachtung von Sicherheitsmaßnahmen | | |
| G 3.8 | Fehlerhafte Nutzung von IT-Systemen | | |
| G 3.43 | Ungeeigneter Umgang mit Passwörtern | | |
| G 3.44 | Sorglosigkeit im Umgang mit Informationen | | |
| G 5.19 | Missbrauch von Benutzerrechten | | |

# 4 Welche Risiken ergeben sich daraus?

Die Höhe eines Risikos wird definiert als ein Produkt aus den möglichen Konsequenzen und der Wahrscheinlichkeit, dass die Konsequenzen eintreten.

## 4.1 Mögliche Auswirkungen der Bedrohungen auf die Werte analysieren

Hier soll das Ausmaß der Konsequenzen für die einzelnen identifizierten Werte erfasst werden, wenn eine potenzielle Bedrohung Realität wird. Dazu wird folgende dreistufige Skala vorgeschlagen:

| Stufe | Definition | Maximale Dauer |
|---|---|---|
| Moderat | Ein gelegentliches Auftreten ist verkraftbar | Vorübergehende Beeinträchtigung |
| Ernst | Es entstehen eventuell signifikante Verluste | Längerfristiger Schaden |
| Katastrophal | Der Schaden kann ein existenzbedrohendes Ausmaß annehmen | Irreparabel |

*Tabelle 1: Dreistufige Skala möglicher Konsequenzen*

Tabelle 2 zeigt beispielhaft, wie die Konsequenzen ermittelt werden können. Zunächst werden für jedes Bedrohungsszenario jeweils die Gefährdungsstufen für jeden einzelnen potenziell betroffenen Wert abgeschätzt und die zugehörigen Werte-IDs werden entsprechend eingefärbt. Anschließend erfolgt eine Gesamtbeurteilung der möglichen Konsequenzen, die prinzipiell auch höher als die höchste Beurteilung für einzelne Assets ausfallen kann, nicht aber niedriger.

| Bedrohungsszenario/Gefahr | | Potenziell betroffene Werte (ID) | | | Konsequenz |
|---|---|---|---|---|---|
| ID | Bezeichnung | | | | |
| G 4.33 | Schlechte oder fehlende Authentikation | W 1.1 | W 1.2 | W 1.3 | Katastrophal |

*Tabelle 2: Potenzielle Konsequenzen für Werte*

## 4.2 Welche Sicherheitsmaßnahmen sind erforderlich?

Die Wahrscheinlichkeit, dass eine Bedrohung zu den möglichen Konsequenzen führen wird, soll so gering sein, dass das Risiko vertretbar ist. Dazu müssen für jede Bedrohung mit relevantem Gefährdungspotenzial bezüglich der identifizierten Werte geeignete Sicherheitsmaßnahmen getroffen werden. Die Tabelle im Anhang A benennt für die Bedrohungen und die Konsequenzstufen jeweils mögliche Maßnahmenpakete. Die einzelnen Maßnahmen werden im Anhang B beschrieben. Die Analysten haben die Aufgabe, jene Schutzmaßnahmen zu identifizieren, die mindestens notwendig sind, damit sämtliche schlimmstenfalls drohenden Konsequenzen ein tragbares Risiko sind. Für die weitere Anwendung des CSLN ist es zweckdienlich, eine Tabelle dafür anzulegen, so wie es Tabelle 3 exemplarisch zeigt.

| **Mindestens erforderliche Sicherheitsmaßnahme** | | | **Schutzlevel in Angeboten für Cloud-Dienste** | | |
|---|---|---|---|---|---|
| **ID** | **Beschreibung** | **Schutzlevel** | *(Name Dienst 1)* | *(Name Dienst 2)* | *(Name Dienst 3)* |
| S 1.1 | Regelung des Zugriffs | Mittel | | | |

*Tabelle 3: Erforderliche und realisierte Sicherheitsmaßnahmen und Schutzlevel*

# 5 Cloud-Dienste bewerten, vergleichen, auswählen und nutzen

Bisher wurde die Analyse unabhängig von eventuell in Frage kommenden konkreten Cloud-Angeboten durchgeführt. Das hat den Vorteil, dass dieser erste Teil der Analyse nur einmal für alle in Frage kommenden Cloud-Dienste durchgeführt werden muss. Zunächst gilt es, die benötigten Cloud-Dienste anhand der funktionalen Anforderungen zu beschreiben und Angebote für entsprechende Dienste einzuholen, aus denen dann eine Auswahl zu treffen ist.

## 5.1 Dienste evaluieren anhand der implementierten Sicherheitsmaßnahmen

Die sicherheitstechnische Beurteilung von externen Cloud-Diensten erfolgt anhand der für den Dienst realisierten Sicherheitsmaßnahmen. Dazu wird für jeden eventuell in Frage kommenden Cloud-Dienst eine Liste der verwirklichten Sicherheitsmaßnahmen erstellt. Es bietet sich an, in Tabelle 3 „Erforderliche und realisierte Sicherheitsmaßnahmen und Schutzlevel“ für jeden zu analysierenden Cloud-Dienst eine eigene Spalte anzulegen und dort alle implementierten Schutzlevel einzutragen.

Als primäre Quelle für die Beurteilung des Sicherheitslevels, das ein externer Cloud-Dienst bei einzelnen Maßnahmen bietet, dienen das Vertragsangebot und ergänzende rechtliche Bestimmungen, etwa die allgemeinen Geschäftsbedingungen.

Sicherheitstechnische Maßnahmen, die beispielsweise nur in der Dokumentation erwähnt werden, aber nicht im Vertrag und auch nicht in ergänzenden rechtsverbindlichen Bestimmungen garantiert werden, bieten eine geringe Verlässlichkeit. Nicht rechtsverbindlich garantierte Sicherheitsmaßnahmen sind in der Liste mit einem Minus zu kennzeichnen.

Eine erhöhte Verlässlichkeit ergibt sich, wenn bestimmte Sicherheitsmaßnahmen nicht nur vom Anbieter selbst rechtsverbindlich zugesichert werden, sondern wenn auch eine unabhängige Partei diese geprüft hat und dies bescheinigt. Durch Zertifikate verbürgte Sicherheitsmaßnahmen sind in der Liste mit einem Pluszeichen hervorzuheben. Tabelle 4 zeigt exemplarisch, wie eine Vergleichstabelle der realisierten Schutzlevel bei verschiedenen Angeboten für Cloud-Dienste aussehen kann.

Eventuell gibt es auch alternative Lösungen, die ohne gewisse externe Cloud-Dienste auskommen können. Für die Lösungsmöglichkeiten ohne Cloud sollte ebenfalls der jeweils gegebene Schutzlevel ermittelt und in die Tabelle eingetragen werden.

| Mindestens erforderliche Sicherheitsmaßnahme | | | Schutzlevel in Angeboten für Cloud-Dienste | | |
|---|---|---|---|---|---|
| **ID** | **Beschreibung** | **Schutzlevel** | **Dienst X** | **Dienst Y** | **Dienst Z** |
| S 1.1 | Regelung des Zugriffs | Mittel | Mittel + | Mittel – | Hoch |
| S 1.2 | Authentifikation | Hoch | Hoch + | Hoch | Hoch |
| S 1.3 | Schlüsselmanagement | Mittel | Mittel + | Hoch | Mittel |
| S 1.5 | Verschlüsselung | Hoch | Mittel + | Hoch | Hoch |

*Tabelle 4: Erreichte Schutzlevel bei verschiedenen Angeboten*

## 5.2 Passendste Dienste finden

Cloud-Dienste, die den gemäß der CSLN-Analyse als Minimum identifizierten Schutzlevel unterschreiten, sollten gemieden werden, wenn dies möglich ist. Doch welches Angebot soll angenommen werden, wenn mehrere verschiedene Angebote mindestens das geforderte Sicherheitsniveau bieten?

Die ermittelten Werte für realisierte Schutzlevel erlauben einen Vergleich der Cloud-Dienste für einzelne Schutzlevel. Daraus ergibt sich jedoch nicht notwendigerweise eine Ordnung bezüglich der Gesamtsicherheit der Dienste, denn die Schwächen und Stärken können jeweils in verschiedenen Bereichen liegen.

Wenn sich keine eindeutige Rangfolge aus der Gegenüberstellung der Schutzlevel ergibt, obwohl die Dienste sehr unterschiedliche Schutzlevel für einzelne Sicherheitsmaßnahmen bieten, kann eine Gewichtung der Bedeutung der einzelnen Sicherheitsmaßnahmen anhand der auf dem Spiel stehenden Werte vorgenommen werden. Für jedes Bedrohungsszenario und für jede Gefährdung wurden bereits die potenziell betroffenen Werte identifiziert. Über die Zuordnung der Sicherheitsmaßnahmen zu den Bedrohungsszenarien und Gefahren lässt sich auch für jede Sicherheitsmaßnahme ermitteln, was auf dem Spiel steht. Zu präferieren ist dann der Cloud-Dienst, der bei den Sicherheitsmaßnahmen, von denen die größten Werte betroffen sind, den höchsten Schutzlevel verspricht.

Sicherheit ist nicht das einzige zu beachtende Auswahlkriterium. Ebenso müssen der Preis und die Benutzbarkeit berücksichtigt werden. Der Preisunterschied zwischen verschiedenen Angeboten kann direkt den Werten gegenübergestellt werden, die auf dem Spiel stehen. Ein Schutzlevel, der sehr weit über den festgestellten Mindestanforderungen liegt, ergibt außerdem keinen Sinn, wenn dadurch die Benutzbarkeit stark beeinträchtigt wird.

## 5.3 Nutzung der Cloud-Dienste

Mit der sorgfältigen Auswahl der Cloud-Dienste ist nur ein erster Schritt gemacht. Oftmals ist der Nutzer selbst das größte Sicherheitsrisiko. Es sind insbesondere die in Kapitel 3.4 vorgestellten Bedrohungsszenarien und Gefahren zu beachten und die Einhaltung der dafür als erforderlich identifizierten Sicherheitsmaßnahmen muss sichergestellt werden.

Die mithilfe des CSLN durchgeführte Risikoanalyse und die bei der Auswahl der Cloud-Dienste verwendeten Materialien sollten aufbewahrt werden. Dies kann insbesondere dann nützlich sein, wenn einzelne Cloud-Dienste und deren Nutzungsbedingungen im Laufe der Zeit verändert werden. Eventuell ist dann eine Anpassung der Daten an die neuen Gegebenheiten möglich, ohne wieder eine vollständige Analyse durchführen zu müssen. Wenn nach angekündigten Änderungen kein ausreichendes Sicherheitsniveau mehr gewährleistet wäre, könnte die Suche nach alternativen Cloud-Diensten mit dem vorhandenen Material beschleunigt werden

Für die nicht private Nutzung von Cloud-Diensten sollte außerdem die Risikoanalyse offen kommuniziert werden. Damit lässt sich zeigen, dass das Thema IKT-Sicherheit ernst genommen wird, dass Aufwand betrieben wird, um Sicherheit zu gewährleisten, und dass die bestehenden Restrisiken nicht verheimlicht werden. Dies kann wesentlich dazu beitragen, das Vertrauen von Geschäftspartnern und Kunden zu gewinnen.

# 6 Weiterführende Literatur

## 6.1 IT-Sicherheit

ISO 27000: Information technology – Security techniques – Information security management systems, International Organization for Standardization 2014

BSI: IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik 2005–2014

CWE: Common Weakness Enumeration, Mitre 2006–2014

CAPEC: Common Attack Pattern Enumeration and Classification, Mitre 2007–2014

## 6.2 Risikoanalyse

ISO 31000: Risk management – Principles and guidelines, International Organization for Standardization 2009

CORAS: M. S. Lund, B. Solhaug, K. Stølen: Model-Driven Risk Analysis – The CORAS Approach, Springer (2011)

## 6.3 Rechtliche Grundlagen

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

BDSG: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist

SigG: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

TMG: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist

## 6.4 IT allgemein

UML: Unified Modeling Language, OMG Object Management Group 1997–2014

NIST Cloud Definition: Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, Special Publication 800 – 145, U. S. Department of Commerce 2011

# Anhang A – Bedrohungen mit Konsequenzstufen und passenden Sicherheitsmaßnahmen

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Gesamturteil Konsequenz** | **Sicherheits-maßnahmen** |
| G 1.10 | Ausfall eines Weitverkehrsnetzes | Moderat | S 1.12r |
| | | Ernst | S 1.12m |
| | | Katastrophal | S 1.12h |
| G 1.19 | Ausfall eines Dienstleisters oder Zulieferers | Moderat | S 1.12r |
| | | Ernst | S 1.12m |
| | | Katastrophal | S 1.12h |
| G 2.1 | Fehlende oder unzureichende Regelungen | Moderat | S 1.9r |
| | | Ernst | S 1.9m |
| | | Katastrophal | S 1.9h |
| G 2.102 | Unzureichende Sensibilisierung für Informationssicherheit | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |
| G 2.103 | Unzureichende Schulung der Mitarbeiter | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |
| G 2.148 | Fehlerhafte Planung der Virtualisierung | Moderat | S 1.14r |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 2.149 | Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme | Moderat | S 1.14r |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 2.150 | Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 2.151 | Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen | Moderat | S 1.16r |
| | | Ernst | S 1.16r |
| | | Katastrophal | S 1.16r |
| G 2.2 | Unzureichende Kenntnis über Regelungen | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Gesamturteil Konsequenz** | **Sicherheits-maßnahmen** |
| G 2.32 | Unzureichende Leitungskapazitäten | Moderat | S 1.14r |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 2.7 | Unerlaubte Ausübung von Rechten | Moderat | S 1.2r, S 1.1r, S 1.4r |
| | | Ernst | S 1.2m, S 1.1m, S 1.4m |
| | | Katastrophal | S 1.2h, S 1.1m, S 1.4h |
| G 2.83 | Fehlerhafte Outsourcing-Strategie | Moderat | S 1.16r |
| | | Ernst | S 1.16m |
| | | Katastrophal | S 1.16h |
| G 2.84 | Unzulängliche vertragliche Regelungen mit einem externen Dienstleister | Moderat | S 1.9r, S 1.16r |
| | | Ernst | S 1.9m, S 1.16m |
| | | Katastrophal | S 1.9m, S 1.16h |
| G 2.85 | Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens | Moderat | S 1.16h |
| | | Ernst | S 1.16h |
| | | Katastrophal | S 1.16h |
| G 2.86 | Abhängigkeit von einem Outsourcing-Dienstleister | Moderat | S 1.16h |
| | | Ernst | S 1.16h |
| | | Katastrophal | S 1.16h |
| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten | Moderat | S 1.10r |
| | | Ernst | S 1.10m |
| | | Katastrophal | S 1.10h |
| G 3.100 | Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme | Moderat | S 1.14r |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 3.101 | Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 3.102 | Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen | Moderat | S 1.14h |
| | | Ernst | S 1.14h |
| | | Katastrophal | S 1.14h |
| G 3.3 | Nichtbeachtung von Sicherheitsmaßnahmen | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |
| G 3.43 | Ungeeigneter Umgang mit Passwörtern | Moderat | S 1.3r |
| | | Ernst | S 1.3m |
| | | Katastrophal | S 1.3h |

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Gesamturteil Konsequenz** | **Sicherheits-maßnahmen** |
| G 3.44 | Sorglosigkeit im Umgang mit Informationen | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |
| G 3.8 | Fehlerhafte Nutzung von IT-Systemen | Moderat | S 1.13r |
| | | Ernst | S 1.13m |
| | | Katastrophal | S 1.13h |
| G 3.99 | Fehlerhafte Netzanbindungen eines Virtualisierungsservers | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 4.22 | Software-Schwachstellen oder -Fehler | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 4.31 | Ausfall oder Störung von Netzkomponenten | Moderat | S 1.7r |
| | | Ernst | S 1.7m |
| | | Katastrophal | S 1.7h |
| G 4.33 | Schlechte oder fehlende Authentikation | Moderat | S 1.2r, S 1.1r, S 1.4r |
| | | Ernst | S 1.2m, S 1.1m, S 1.4m |
| | | Katastrophal | S 1.2h, S 1.1m, S 1.4h |
| G 4.35 | Unsichere kryptographische Algorithmen | Moderat | S 1.5r |
| | | Ernst | S 1.5m |
| | | Katastrophal | S 1.5h |
| G 4.74 | Ausfall von IT-Komponenten in einer virtualisierten Umgebung | Moderat | S 1.12r, S 1.14r |
| | | Ernst | S 1.12m, S 1.14m |
| | | Katastrophal | S 1.12h, S 1.14h |
| G 4.75 | Störung der Netzinfrastruktur von Virtualisierungsumgebungen | Moderat | S 1.14r |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 4.76 | Ausfall von Verwaltungsservern für Virtualisierungssysteme | Moderat | S 1.12r, S 1.14r |
| | | Ernst | S 1.12m, S 1.14m |
| | | Katastrophal | S 1.12h, S 1.14h |
| G 4.77 | Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 5.1 | Manipulation oder Zerstörung von Geräten oder Zubehör | Moderat | S 1.7r |
| | | Ernst | S 1.7m |
| | | Katastrophal | S 1.7h |

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Gesamturteil Konsequenz** | **Sicherheits-maßnahmen** |
| G 5.107 | Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister | Moderat | S 1.9r |
| | | Ernst | S 1.9m |
| | | Katastrophal | S 1.9h |
| G 5.12 | Abhören von Telefongesprächen und Datenübertragungen | Moderat | S 1.5r |
| | | Ernst | S 1.5m |
| | | Katastrophal | S 1.5h |
| G 5.147 | Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes | Moderat | S 1.5r |
| | | Ernst | S 1.5m |
| | | Katastrophal | S 1.5h |
| G 5.148 | Missbrauch von Virtualisierungsfunktionen | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 5.149 | Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen | Moderat | S 1.14m |
| | | Ernst | S 1.14m |
| | | Katastrophal | S 1.14h |
| G 5.150 | Kompromittierung des Hypervisors virtueller IT-Systeme | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 5.165 | Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen | Moderat | S 1.2r, S 1.1r, S 1.4r |
| | | Ernst | S 1.2m, S 1.1m, S 1.4m |
| | | Katastrophal | S 1.2h, S 1.1m, S 1.4h |
| G 5.173 | Einbindung von fremden Daten und Schadcode bei Webanwendungen | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 5.19 | Missbrauch von Benutzerrechten | Moderat | S 1.2r, S 1.1r, S 1.4r |
| | | Ernst | S 1.2m, S 1.1m, S 1.4m |
| | | Katastrophal | S 1.2h, S 1.1m, S 1.4h |
| G 5.2 | Manipulation an Informationen oder Software | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 5.21 | Trojanische Pferde | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |

| Bedrohungsszenario/Gefahr | | | |
|---|---|---|---|
| **ID** | **Bezeichnung** | **Gesamturteil Konsequenz** | **Sicherheits-maßnahmen** |
| G 5.23 | Schadprogramme | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 5.26 | Analyse des Nachrichtenflusses | Moderat | S 1.5r |
| | | Ernst | S 1.5m |
| | | Katastrophal | S 1.5r |
| G 5.28 | Verhinderung von Diensten | Moderat | S 1.7r |
| | | Ernst | S 1.7m |
| | | Katastrophal | S 1.7h |
| G 5.3 | Unbefugtes Eindringen in ein Gebäude | Moderat | S 1.7r |
| | | Ernst | S 1.7m |
| | | Katastrophal | S 1.7h |
| G 5.4 | Diebstahl | Moderat | S 1.7r |
| | | Ernst | S 1.7m |
| | | Katastrophal | S 1.7h |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen | Moderat | S 1.3r, S 1.5r |
| | | Ernst | S 1.3m, S 1.5r |
| | | Katastrophal | S 1.3h, S 1.5r |
| G 5.83 | Kompromittierung kryptographischer Schlüssel | Moderat | S 1.3r |
| | | Ernst | S 1.3m |
| | | Katastrophal | S 1.3h |
| G 5.84 | Gefälschte Zertifikate | Moderat | S 1.15r |
| | | Ernst | S 1.15m |
| | | Katastrophal | S 1.15h |
| G 5.85 | Integritätsverlust schützenswerter Informationen | Moderat | S 1.6r |
| | | Ernst | S 1.6m |
| | | Katastrophal | S 1.6h |

# Anhang B – Sicherheitsmaßnahmen mit Schutzlevel

| ID | Bezeichnung der Maßnahmengruppe | ID und Level | Beschreibung der einzelnen Maßnahmen | Schutzlevel | BSI-Maßnahmen-Nummer |
|---|---|---|---|---|---|
| S 1.1 | Regelung des Zugriffs | S 1.1r | Die Zugriffsrechte sind schriftlich geregelt UND der Zugriff erfolgt erst nach Identifikation sowie Authentifikation | Rudimentär | M 2.8, M 2.109, M 2.220 |
| | | S 1.1m | Die Zugriffsrechte sind schriftlich geregelt sowie dokumentiert UND die Zugriffsrechte sind minimal UND Vergabe sowie Entzug von Zugriffsrechten sind geregelt UND fehlschlagende Zugriffsversuche werden erfasst UND der Zugriff erfolgt erst nach hochsicherer Identifikation sowie Authentifikation | Mittel | M 2.8, M 2.63, M 2.109, M 2.220 |
| | | S 1.1h | Die Zugriffsrechte sind schriftlich geregelt sowie exakt dokumentiert UND die Zugriffsrechte sind minimal UND Vergabe sowie Entzug von Zugriffsrechten sind klar geregelt UND fehlschlagende Zugriffsversuche werden erfasst UND die Rechtevergabe erfolgt mittels Rollen sowie Gruppen UND der Zugriff erfolgt erst nach hochsicherer Identifikation sowie Authentifikation | Hoch | M 2.8, M 2.63, M 2.109, M 2.129, M 2.220 |
| S 1.2 | Authentifikation | S 1.2r | Benutzername plus Passwort | Rudimentär | M 4.133 |
| | | S 1.2m | Benutzername plus Passwort UND Regeln für das Passwort UND Begrenzung der Anzahl der fehlerhaften Login-Versuche | Mittel | M 2.11, M 4.133 |
| | | S 1.2h | Zwei-Faktor-Authentifizierung (mit Hardware-Token ODER Biometrie) UND Passwort UND Regeln für das Passwort UND Begrenzung der Anzahl der fehlerhaften Login-Versuche | Hoch | M 2.11, M 4.133 |
| S 1.3 | Schlüssel-management | S 1.3r | Passwörter, die im Verlustfall einfach durch neue Passwörter ersetzt werden können, werden nicht hinterlegt UND Passwörter, deren Verlust nicht kompensierbar ist, werden sicher hinterlegt | Rudimentär | M 2.11, M 2.22, M 2.46 |
| | | S 1.3m | Passwörter, die im Verlustfall einfach durch neue Passwörter ersetzt werden können, werden nicht hinterlegt UND es sind klare Regeln sowie Prozesse zum Zurücksetzen von Passwörtern definiert UND Passwörter, deren Verlust nicht kompensierbar ist, werden sicher hinterlegt | Mittel | M 2.11, M 2.22, M 2.46, M 2.402 |
| | | S 1.3h | Passwörter, die im Verlustfall einfach durch neue Passwörter ersetzt werden können, werden nicht hinterlegt UND es sind klare Regeln sowie Prozesse zum Zurücksetzen von Passwörtern definiert UND Passwörter, deren Verlust nicht kompensierbar ist ,werden sicher hinterlegt UND alle Passwörter dienen jeweils nur einem Einsatzzweck | Hoch | M 2.11, M 2.22, M 2.46, M 2.402 |

| ID | Bezeichnung der Maßnahmengruppe | ID und Level | Beschreibung der einzelnen Maßnahmen | Schutzlevel | BSI-Maßnahmen-Nummer |
|---|---|---|---|---|---|
| S 1.4 | Identifikation | S 1.4r | Selbstauskunft UND gültige E-Mail-Adresse | Rudimentär | |
| | | S 1.4m | Selbstauskunft UND gültige E-Mail-Adresse UND Speicherung der IP-Adresse | Mittel | |
| | | S 1.4h | Elektronischer Ausweis ODER persönlich, eventuell mithilfe eines speziellen Dienstleisters, beispielsweise PostIdent | Hoch | |
| S 1.5 | Verschlüsselung | S 1.5r | Vertrauliche Daten werden immer nach aktuellem Stand der Technik sicher verschlüsselt übertragen sowie gespeichert | Rudimentär | M 2.164, M 2.165, M 4.34 |
| | | S 1.5m | Vertrauliche Daten werden immer nach aktuellem Stand der Technik sicher verschlüsselt übertragen sowie gespeichert UND die Integrität wird mittels Prüfsummen gewahrt UND bei Übertragung wird die Reihenfolge verschlüsselter Daten durch Zeitstempel oder Nummerierung garantiert | Mittel | M 2.164, M 2.165, M 4.34 |
| | | S 1.5h | Vertrauliche Daten werden immer nach aktuellem Stand der Technik sicher verschlüsselt übertragen sowie gespeichert UND die Integrität wird mittels Prüfsummen gewahrt UND bei Übertragung wird die Reihenfolge verschlüsselter Daten durch Zeitstempel oder Nummerierung garantiert UND bei Übertragungen wird Perfect Forward Secrecy gewährleistet | Hoch | M 2.164, M 2.165, M 4.34 |
| S 1.6 | Sicherung gegen Informationsverluste | S 1.6r | Es werden regelmäßig automatisch Sicherungskopien erzeugt | Rudimentär | M 6.32 |
| | | S 1.6m | Die Wiederherstellbarkeit anhand der Kopien wird regelmäßig überprüft UND es werden regelmäßig automatisch Sicherungskopien erzeugt UND die Sicherungskopien werden verschlüsselt gespeichert UND kryptografische Schlüssel und Programme zur Datensicherung werden ebenfalls gesichert | Mittel | M 6.22, M 6.32, M 6.56 |
| | | S 1.6h | Die Nutzer sind über das Datensicherungskonzept informiert UND die Wiederherstellbarkeit anhand der Kopien wird regelmäßig überprüft UND es werden regelmäßig automatisch Sicherungskopien erzeugt UND die Sicherungskopien werden verschlüsselt gespeichert UND die Datensicherung sowie gegebenenfalls die Wiederherstellung werden dokumentiert UND kryptografische Schlüssel und Programme zur Datensicherung werden ebenfalls gesichert | Hoch | M 2.41, M 2.137, M 6.22, M 6.32, M 6.33, M 6.37, M 6.56 |

| ID | Bezeichnung der Maßnahmengruppe | ID und Level | Beschreibung der einzelnen Maßnahmen | Schutzlevel | BSI-Maßnahmen-Nummer |
|---|---|---|---|---|---|
| S 1.7 | Regelung des Zutritts | S 1.7r | Es gibt eine Zutrittskontrolle zu allen kritischen Orten | Rudimentär | M 2.17 |
| | | S 1.7m | Es gibt eine Zutrittskontrolle zu allen kritischen Orten UND Zutrittsberechtigungen sind minimal UND Zutrittsregelungen sowie Zutrittsvorgänge werden dokumentiert | Mittel | M 1.80, M 2.6, M 2.17 |
| | | S 1.7h | Es gibt eine Zutrittskontrolle zu allen kritischen Orten UND Zutrittsberechtigungen sind minimal UND Zutritt ist immer schnell möglich UND es werden mindestens zwei Authentifikationsmerkmale geprüft UND jede Person muss sich einzeln anmelden sowie abmelden UND Zutrittsregelungen sowie Zutrittsvorgänge werden dokumentiert | Hoch | M 1.2, M 1.73, M 1.80, M 2.6, M 2.17 |
| S 1.8 | Protokollierung von Sicherheitsvorfällen | S 1.8r | Alle Sicherheitsvorfälle werden dokumentiert UND Dokumente zu Sicherheitsvorfällen werden geschützt archiviert | Rudimentär | M 6.134 |
| | | S 1.8m | Alle Sicherheitsvorfälle werden in standardisierter Form dokumentiert UND Dokumente zu Sicherheitsvorfällen werden geschützt archiviert UND Sicherheitsvorfälle werden zeitnah an das Notfallmanagement kommuniziert | Mittel | M 6.119, M 6.134 |
| | | S 1.8h | Alle Sicherheitsvorfälle werden in standardisierter Form dokumentiert UND Dokumente zu Sicherheitsvorfällen werden geschützt archiviert UND Sicherheitsvorfälle werden zeitnah an das Notfallmanagement kommuniziert UND die Dokumentation von Sicherheitsvorfällen ist so umfassend, dass eine möglichst große Nachvollziehbarkeit der Gesamtumstände des Vorfalls erreicht wird | Hoch | M 2.201, M 6.119, M 6.134 |
| S 1.9 | Datenschutzerklärung | S 1.9r | Es ist eine rechtsverbindliche Datenschutzerklärung vorhanden UND es werden nur die unbedingt erforderlichen Daten erfasst | Rudimentär | M 2.501, M 2.504 |
| | | S 1.9m | Es ist eine rechtsverbindliche Datenschutzerklärung vorhanden UND es werden nur die unbedingt erforderlichen Daten erfasst UND alle Nutzer werden darüber informiert, wie sie unerwünschte Datenspuren vermeiden können | Mittel | M 2.501, M 2.503, M 2.504, M 5.155 |
| | | S 1.9h | Es ist eine rechtsverbindliche Datenschutzerklärung vorhanden UND es werden nur die unbedingt erforderlichen Daten erfasst UND alle Nutzer werden darüber informiert, wie sie unerwünschte Datenspuren vermeiden können, UND es wird ein Datenschutzbeauftragter mit klar definierten Zuständigkeiten sowie entsprechenden Handlungsmöglichkeiten benannt | Hoch | M 2.501, M 2.502, M 2.503, M 2.504, M 2.505, M 5.155 |
| S 1.10 | Aufbewahrung, Löschung und Rückgabe von Daten | S 1.10r | Speicher- sowie Löschfristen sind geregelt UND kryptografische Verschlüsselung von personenbezogenen sowie kritischen Daten wird garantiert | Rudimentär | M 2.431, M 2.505, M 4.34 |
| | | S 1.10m | Speicher- sowie Löschfristen sind geregelt UND kryptografische Verschlüsselung von personenbezogenen sowie kritischen Daten wird garantiert UND physikalisch sicheres Löschen wird garantiert UND Löschansprüche sowie Auskunftsansprüche sind klar geregelt | Mittel | M 2.431, M 2.505, M 2.515, M 4.32, M 4.34 |
| | | S 1.10h | Speicher- sowie Löschfristen sind geregelt UND kryptografische Verschlüsselung von personenbezogenen sowie kritischen Daten wird garantiert UND physikalisch sicheres Löschen wird garantiert UND es besteht eine umfassende vertragliche Regelung zum Umgang mit personenbezogenen sowie kritischen Daten mit präziser Zweckbindung, Löschanspruch sowie Auskunftsanspruch | Hoch | M 2.431, M 2.505, M 2.511, M 2.515, M 4.32, M 4.34 |

| ID | Bezeichnung der Maßnahmengruppe | ID und Level | Beschreibung der einzelnen Maßnahmen | Schutzlevel | BSI-Maßnahmen-Nummer |
|---|---|---|---|---|---|
| S 1.11 | Festlegung des Ortes der Datenhaltung | S 1.11r | Safe Harbor (EU + Schweiz + USA) | Rudimentär | M 2.503 |
| | | S 1.11m | EU | Mittel | M 2.503 |
| | | S 1.11h | Deutschland | Hoch | M 2.503 |
| S 1.12 | Notfallmanagement für Ausfälle | S 1.12r | Es existiert ein Plan für den Umgang mit Ausfallsituationen | Rudimentär | M 6.110, M 6.111, M 6.112, M 6.113, M 6.114 |
| | | S 1.12m | Es existiert ein Plan für den Umgang mit Ausfallsituationen UND Ausfallsituationen werden dokumentiert | Mittel | M 6.110, M 6.111, M 6.112, M 6.113, M 6.114, M 6.119 |
| | | S 1.12h | Es existiert ein Plan für den Umgang mit Ausfallsituationen UND Ausfallsituationen werden regelmäßig geübt UND Ausfallsituationen werden dokumentiert | Hoch | M 6.110, M 6.111, M 6.112, M 6.113, M 6.114, M 6.117, M 6.118, M 6.119, M 6.120 |
| S 1.13 | Sensibilisierung | S 1.13r | Ansprechpartner zu Sicherheitsfragen stehen bereit UND es werden Informationsmaterialien zu Sicherheitsaspekten offeriert | Rudimentär | M 3.46, M 2.198 |
| | | S 1.13m | Ansprechpartner zu Sicherheitsfragen stehen bereit UND es werden Informationsmaterialien zu Sicherheitsaspekten offeriert UND es werden Einführungen zum Thema IT-Sicherheit angeboten | Mittel | M 3.46, M 2.198, M 3.26 |
| | | S 1.13h | Ansprechpartner zu Sicherheitsfragen stehen bereit UND es werden Informationsmaterialien zu Sicherheitsaspekten offeriert UND es werden Einführungen zum Thema IT-Sicherheit sowie weiter gehende Schulungen angeboten | Hoch | M 3.46, M 2.198, M 3.4, M 3.5, M 3.26 |
| S 1.14 | Absicherung der Virtualisierung | S 1.14r | Es werden Garantien zur Performance, Verfügbarkeit und Reaktionszeit gegeben | Rudimentär | M 2.329 |
| | | S 1.14m | Es werden Garantien zur Performance, Verfügbarkeit und Reaktionszeit gegeben UND die Leistungsdaten sowie Integrität werden regelmäßig überwacht UND Start-Update und Terminierung der Virtualisierungsserver und der virtuellen Systeme sind geregelt UND die Nutzungsbedingungen regeln, was in der Virtualisierung erlaubt ist (z. B. Einsatz von Gastprogrammen) | Mittel | M 2.329, M 2.444, M 2.448, M 4.346 |
| | | S 1.14h | Es werden Garantien zur Performance, Verfügbarkeit und Reaktionszeit gegeben UND die Leistungsdaten sowie Integrität werden regelmäßig überwacht UND Start-Update und Terminierung der Virtualisierungsserver und der virtuellen Systeme sind geregelt UND die Nutzungsbedingungen regeln, was in der Virtualisierung erlaubt ist (z. B. Einsatz von Gastprogrammen) UND Isolation sowie Kapselung sind verbindlich geregelt (UND die Zeitsynchronität der Virtualisierungen ist verbindlich festgelegt sowie technisch gewährleistet – nur falls Synchronität erforderlich ist) | Hoch | M 2.329, M 2.444, M 2.447, M 2.448, M 4.346, M 4.348 |

| ID | Bezeichnung der Maßnahmengruppe | ID und Level | Beschreibung der einzelnen Maßnahmen | Schutzlevel | BSI-Maßnahmen-Nummer |
|---|---|---|---|---|---|
| S 1.15 | Schutz vor Schadprogrammen | S 1.15r | Konzept zum Schutz vor Schadprogrammen ist in Regeln verankert UND es werden Programme zum Schutz vor Schadsoftware eingesetzt sowie aktuell gehalten UND alle eingehenden Daten werden automatisch geprüft | Rudimentär | M 2.154, M 2.157, M 2.159, M 2.160, M 2.224, M 4.3 |
| | | S 1.15m | Konzept zum Schutz vor Schadprogrammen ist in Regeln verankert UND es werden Programme zum Schutz vor Schadsoftware eingesetzt sowie aktuell gehalten UND alle eingehenden Daten werden automatisch geprüft UND Informationen zu aufgespürten Schadprogrammen werden zentral erfasst sowie archiviert UND für den Notfall werden Rettungsmittel vorrätig gehalten | Mittel | M 2.154, M 2.157, M 2.158, M 2.159, M 2.160, M 2.224, M 4.3, M 6.24 |
| | | S 1.15h | Konzept zum Schutz vor Schadprogrammen ist in Regeln verankert UND es werden Programme zum Schutz vor Schadsoftware eingesetzt sowie aktuell gehalten UND alle eingehenden Daten werden automatisch geprüft UND Informationen zu aufgespürten Schadprogrammen werden zentral erfasst sowie archiviert UND für den Notfall werden Rettungsmittel vorrätig gehalten UND es werden Materialien/Schulungen zur Sicherheit vor Schadprogrammen angeboten, insbesondere zum Verhalten, wenn der Verdacht besteht, dass ein Befall mit Schadprogrammen vorliegen könnte | Hoch | M 3.4, M 3.5, M 2.154, M 2.157, M 2.158, M 2.159, M 2.160, M 2.224, M 4.3, M 6.23, M 6.24 |
| S 1.16 | Outsourcing | S 1.16r | Zuständigkeiten, Rechte und Pflichten sind verbindlich geregelt UND die (technische, rechtliche) Machbarkeit ist geprüft | Rudimentär | M 2.250, M 2.253 |
| | | S 1.16m | Zuständigkeiten, Rechte und Pflichten sind verbindlich geregelt UND die (technische, rechtliche) Machbarkeit ist geprüft UND das Sicherheitskonzept mit allen zugehörigen Maßnahmen ist explizit verbindlich geregelt UND für Änderungen sowie Abweichungen im laufenden Betrieb sind Vereinbarungen getroffen | Mittel | M 2.250, M 2.251, M 2.253, M 2.254, M 2.256 |
| | | S 1.16h | Zuständigkeiten, Rechte und Pflichten sind verbindlich geregelt UND die (technische, rechtliche) Machbarkeit ist geprüft UND das Sicherheitskonzept mit allen zugehörigen Maßnahmen ist explizit verbindlich geregelt UND für Änderungen sowie Abweichungen sind Vereinbarungen getroffen UND für Migration sowie Beendigung des Vertragsverhältnisses sind verbindliche Regeln festgelegt | Hoch | M 2.250, M 2.251, M 2.253, M 2.254, M 2.255, M 2.256, M 2.307 |

# Anhang C – Definitionen und Erläuterungen

## Grundlagen

**Cloud**
Der Begriff Cloud wird hier ausschließlich im Sinne von Cloud Computing verstanden, wie er vom NIST definiert wurde. Cloud Computing ermöglicht es, über Computernetzwerke einen geteilten Pool von konfigurierbaren IT-Ressourcen zu nutzen, wobei die Nutzung schnell und ohne großen Aufwand möglich ist. Es umfasst die Konzepte Software als Service, Plattform als Service und Infrastruktur als Service.

**Public Cloud**
Externe Cloud-Dienste werden von einem fremden Betreiber entwickelt und öffentlich (Public Cloud) beziehungsweise zumindest nicht zum Betreiber gehörenden Kunden zur Verfügung gestellt.

**Risiko**
Der Begriff Risiko wird hier im Sinne der ISO 31000 verwendet. Er beschreibt den Effekt einer Unsicherheit auf bestimmte Werte. Das Risiko wird als ein Produkt aus Wahrscheinlichkeit, dass der Effekt eintritt, und der Schwere der Konsequenzen verstanden.

**Risikoanalyse**
Hier wird Risikoanalyse als Begriff für das gesamte Risk-Assessment im Sinne der ISO 31000 verwendet. In der ISO 31000 bezeichnet Risk-Analysis hingegen nur einen Teil des Risk-Assessments. Risikoanalyse meint in diesem Dokument ausdrücklich alle Bestandteile des Risk-Assessments, also Risk-Identification, Risk-Analysis und Risk-Evaluation.

**Sicherheit**
Mit Sicherheit ist hier primär Informationssicherheit im Sinne von ISO 27000 gemeint.

## Zu den Gefahren und Bedrohungen (Kapitel 3)

**Authentikation**
Sicherstellung, dass Informationen bestimmte Eigenschaften erfüllen. Insbesondere, dass Daten von einer bestimmten Person stammen. Im Deutschen sind auch die Begriffe Authentifikation sowie Authentifizierung anstelle von Authentikation (englisch Authentication) üblich.

**Cloud-Plattform**
Die IT-Systeme, die die Cloud-Dienste realisieren und bereitstellen.

**Integritätsverlust**
Manipulation von Daten, Verlust von der Korrektheit der Informationen.

**Lock-in**
Abhängigkeit von bestimmten Diensten externer Cloud-Anbieter.

**Schadcode, Schadprogramme**
Ausführbarer Code, der unerwünschte Wirkungen entfalten kann (Malware). Hierzu zählen insbesondere Viren, trojanische Pferde, Spyware und Adware.

**Snapshots**
Momentaufnahmen von IT-Systemen, die gespeichert und analysiert werden können. Bei Virtualisierung können in der Regel komplette Gastsysteme so erfasst werden.

**Trojanische Pferde**
Ein scheinbar nützliches Programm beinhaltet selbst Schadsoftware oder enthält eine Hintertür (Backdoor), durch die Angreifer weitere Attacken starten können.

**Verhinderung von Diensten**
Die Verfügbarkeit von Diensten wird zeitweise oder dauerhaft beeinträchtigt (Denial of Service), beispielsweise durch eine Überlastung mit Anfragen.

**Virtualisierung**
Bei der Virtualisierung werden durch Softwareprogramme IT-Infrastrukturen (Hardware und Software) nachgebildet (emuliert) und so zur Nutzung bereitgestellt, als handle es sich um reale IT-Systeme.

**Zertifikate**
Digitale Zertifikate bescheinigen die Authentizität von öffentlichen Schlüsseln, die beispielsweise zur Authentifikation des Inhabers des Zertifikats und zum Aufbau von sicheren Kanälen zur Kommunikation benutzt werden können. Zertifikate werden von bestimmten Parteien nach Identitätsprüfung ausgestellt. Auf die Korrektheit dieser Parteien muss dabei vertraut werden.

# Anhang D – Bausteine für die Sicherheitsmaßnahmen

Die folgenden Textbausteine, Erläuterungen, Hilfestellungen und exemplarisch aufgeführten konkreten Technologien sollen die Auffindung der Sicherheitsmaßnahmen sowie der erreichten Schutzlevel aus den Vertragsangeboten, Regelungen und Geschäftsbedingungen der Anbieter von Cloud-Diensten erleichtern.

## Zu S 1.1 Regelung des Zugriffs

Die Zugriffsrechte sind schriftlich geregelt
- Nutzungsbedingungen/Use of Service
  - Rechte
  - Einschränkungen
  - Pflichten

… sowie exakt dokumentiert
- Nutzungsbedingungen/Use of Service
  - Verantwortlichkeiten
  - Veränderungen/Updates der Nutzungsbedingungen

Die Zugriffsrechte sind minimal
- Datenschutzerklärung (siehe S 1.9) – insbesondere Weitergabe von Daten

Vergabe sowie Entzug von Zugriffsrechten sind klar geregelt
- Zur Sperrung eventuell kompromittierter Zugriffsdaten/Zugriffsgeräte …
- Vertragsende/Expiration, Termination

Fehlschlagende Zugriffsversuche werden erfasst
- Automatisches Logging gescheiterter Zugriffsversuche (siehe S 1.8)

Die Rechtevergabe erfolgt mittels Rollen sowie Gruppen
- Hierzu zählen insbesondere Regelungen zu Möglichkeiten, anderen Nutzern gezielt Zugriffsrechte auf eigene Inhalte einzuräumen oder zu entziehen

Der Zugriff erfolgt erst nach hochsicherer Identifikation sowie Authentifikation
- S 1.4, S 1.2

## Zu S 1.2 Authentifikation

Benutzername plus Passwort
- Statt Passwort zur Authentifikation wird auch die Bezeichnung Persönliche Identifikationsnummer (PIN-Code) verwendet
- Username and password

Regeln für das Passwort
- Das Passwort muss mindestens X Zeichen lang sein
- Das Passwort muss verschiedene Arten von Zeichen enthalten
  - Kleinbuchstaben
  - Großbuchstaben
  - Zahlen
  - Sonderzeichen

Begrenzung der Anzahl der fehlerhaften Login-Versuche
- Sperrung nach X fehlerhaften Passwort-(PIN-Code-)Eingaben

Zwei-Faktor-Authentifizierung mit Hardware-Token
- Authentifikation mit Smart-Card, SIM-Card und Passwort (PIN-Code)
- Multi-Factor Authentication with hardware token and password

Zwei-Faktor-Authentifizierung mit Biometrie
- Authentifikation mit Fingerabdruck-Scanner und Passwort-/Hardware-Token
- Authentifikation mit Iris-Scanner und Passwort-/Hardware-Token
- Authentifikation mit Gesichtserkennung und Passwort-/Hardware-Token
- Multi-Factor Authentication with biometric authentication and password or hardware token

## Zu S 1.3 Schlüsselmanagement

Schlüssel, die im Verlustfall einfach durch neue Schlüssel ersetzt werden können, werden nicht hinterlegt
- Von Passwörtern werden nur sichere Einweg-Hash-Werte mit Salt gespeichert

Es sind klare Regeln sowie Prozesse zum Zurücksetzen von Schlüsseln definiert
- Verfahren zum sofortigen Sperren von Schlüsseln und zur Anforderung neuer Schlüssel

Schlüssel, deren Verlust nicht kompensierbar ist, werden sicher hinterlegt
- Es werden Sicherungskopien räumlich getrennt und vor unbefugtem Zugriff geschützt aufbewahrt (siehe S 1.6)

Alle Schlüssel dienen jeweils nur einem Einsatzzweck
- NICHT: Single Sign-on

## Zu S 1.4 Identifikation

Selbstauskunft
Gültige E-Mail-Adresse
- Zusendung eines Bestätigungslinks an die angegebene E-Mail-Adresse

Speicherung der IP-Adresse
Elektronischer Ausweis
- Neuer/elektronischer Personalausweis

Persönlich, eventuell mithilfe eines speziellen Dienstleisters
- beispielsweise PostIdent

## Zu S 1.5 Verschlüsselung

Vertrauliche Daten werden immer nach aktuellem Stand der Technik sicher verschlüsselt übertragen
- Nutzung von Secure-Sockets-Layer-Software (SSL) für die Datenübertragung
- Nutzung von Transport Layer Security (TLS) für die Datenübertragung
- Nutzung von https

... sowie gespeichert
- Datenträgerverschlüsselung
  - zum Beispiel mit AES, Triple DES

Die Integrität wird mittels Prüfsummen gewahrt
- Message Authentication Code
  - zum Beispiel HMAC, CMAC

Bei Übertragung wird die Reihenfolge verschlüsselter Daten durch Zeitstempel oder Nummerierung garantiert
- Nutzung von IPsec
- Nonce
- Sequenznummern

Bei Übertragungen wird Perfect Forward Secrecy gewährleistet
- Verwendung von Einwegschlüsseln
- Transport Layer Security (TLS) mit Diffie-Hellman-Schlüsselaustausch

## Zu S 1.6 Sicherung gegen Informationsverluste

Es werden regelmäßig automatisch Sicherungskopien erzeugt
- Backup-Kopien werden beim Speichern oder Ändern von Daten automatisch angelegt
- Neue Backup-Kopien werden immer am … um … Uhr generiert

Die Sicherungskopien werden räumlich getrennt aufbewahrt
- Die Backup-Datenträger werden in einem separaten Serverraum aufbewahrt
- Die Backup-Kopien werden verteilt an den Standorten … gespeichert

Die Wiederherstellbarkeit anhand der Backup-Kopien wird regelmäßig überprüft
- Die Integrität der Daten und der Backup-Kopien wird wöchentlich/täglich automatisch kontrolliert

Die Sicherungskopien werden vor unbefugten Zugriffen geschützt
- Verschlüsselung der Sicherungsdaten (siehe S 1.5)
- Physische Abschirmung der Sicherungsdatenträger (siehe S 1.7)

Schlüssel für den Schutz der Datensicherung gegen unbefugte Zugriffe werden ebenfalls gesichert
- Schlüsselmanagement für die Gewährleistung des berechtigten Zugriffs auf die Backup-Daten (siehe S 1.3)

Die Datensicherung sowie gegebenenfalls die Wiederherstellungen werden dokumentiert (siehe auch S 1.8)
- Automatisches Logging aller Vorgänge zur Datenprüfung und zur Datenreparatur
- Information der Nutzer über sicherheitsrelevante Vorfälle

## Zu S 1.7 Regelung des Zutritts

Es gibt eine Zutrittskontrolle zu allen kritischen Orten
- Absicherung der Rechenzentren/Serverräume gegen physische Gefährdungen durch Eindringlinge
  - Durch Verschluss
  - Durch Überwachung

Zutrittsberechtigungen sind minimal
- NICHT Auslagerung auf Infrastrukturen anderer Anbieter

Zutrittsregelungen sowie Zutrittsvorgänge werden dokumentiert
- Automatisches Logging (siehe S 1.8)

Zutritt ist immer schnell möglich
- Schlüsselmanagement (siehe S 1.3)

Es werden mindestens zwei Authentifikationsmerkmale geprüft
- Siehe S 1.2

Jede Person muss sich einzeln anmelden sowie abmelden
- Vollständige Aufenthaltskontrolle

## Zu S 1.8 Protokollierung von Sicherheitsvorfällen

Alle Sicherheitsvorfälle werden in standardisierter Form dokumentiert
- Automatisches Logging aller potenziell kritischen Ereignisse

Dokumente zu Sicherheitsvorfällen werden geschützt archiviert
- Verschlüsselung der Logging-Daten (siehe S 1.5)
- Physische Abschirmung der Logging-Datenträger (siehe S 1.7)

Sicherheitsvorfälle werden zeitnah an das Notfallmanagement kommuniziert
- Automatische Benachrichtigung der gemäß Notfallplan (S 1.12) zuständigen Personen

Die Dokumentation von Sicherheitsvorfällen ist so umfassend, dass eine möglichst große Nachvollziehbarkeit der Gesamtumstände des Vorfalls erreicht wird
- Das Logging aller potenziell kritischen Ereignisse erfasst den kompletten Systemzustand

## Zu S 1.9 Datenschutzerklärung

Es ist eine rechtsverbindliche Datenschutzerklärung vorhanden
- Privacy statement, privacy policy and practices, data protection

Es werden nur die unbedingt erforderlichen Daten erfasst
- Genaue Auflistung aller erhobenen Informationen jeweils mit Begründung, warum diese Daten erfasst werden, was mit den Daten passiert und wie lange sie wo gespeichert werden

Alle Nutzer werden darüber informiert, wie sie unerwünschte Datenspuren vermeiden können
- Anleitung zum Löschen der personenbezogenen Daten
- Hilfestellung zur Unterdrückung der automatischen Erfassung und Verfolgung
  - Beispielsweise Cookies

Es wird ein Datenschutzbeauftragter mit klar definierten Zuständigkeiten sowie entsprechenden Handlungsmöglichkeiten benannt
- Für Fragen und Beschwerden zum Thema Datenschutz ...

## Zu S 1.10 Aufbewahrung, Löschung und Rückgabe von Daten

Speicher- sowie Löschfristen sind geregelt
- Die Daten X werden für einen Zeitraum von Y gespeichert
- Die Löschung erfolgt ab X innerhalb von Y

Der Schutz von personenbezogenen sowie kritischen Daten vor unbefugtem Zugriff wird garantiert
- Verschlüsselung der personenbezogenen sowie kritischen Daten (siehe S 1.5)
- Physische Abschirmung der Datenträger mit personenbezogenen sowie kritischen Daten (siehe S 1.7)

Physikalisch sicheres Löschen wird garantiert
- Die Speicherorte zu löschender Daten werden beim Löschvorgang garantiert überschrieben

Löschansprüche sowie Auskunftsansprüche sind klar geregelt
- Grundsätzlicher Rechtsanspruch auf die Löschung von Daten
- Anleitung zum Löschen von Daten
- Die Informationen X werden auf Anfrage Y hin bereitgestellt

Es besteht eine umfassende vertragliche Regelung zum Umgang mit personenbezogenen sowie kritischen Daten mit präziser Zweckbindung, Löschanspruch sowie Auskunftsanspruch
- Datenschutzerklärung mit genauer Auflistung aller erhobenen Informationen jeweils mit Begründung, warum diese Daten erfasst werden, was mit den Daten passiert und wie lange sie wo gespeichert werden (S 1.9)

## Zu S 1.11 Festlegung des Ortes der Datenhaltung

Safe Harbor (EU + Schweiz + USA)
- US-Unternehmen, die explizit am Safe-Harbor-Programm teilnehmen
  - Enrolled in the U.S. Department of Commerce Safe Harbor Program, compliance with EU Directive 95/46/EC on the protection of personal data
- ODER in der EU/EWR bzw. in gleichgestellten Staaten bezüglich des Datenschutzes (s. u.)

EU und gleichgestellt bezüglich des Datenschutzes
- In EU-Mitgliedsstaaten
- In Staaten des EWR
- Derzeit auch: Andorra, Argentinien, Australien, Kanada, Schweiz, Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay (http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)

Inländisch
- Ausschließlich inländische Datenhaltung

## Zu S 1.12 Notfallmanagement für Ausfälle

Es existiert ein Plan für den Umgang mit Ausfallsituationen
- Sollte der Dienst nur beeinträchtigt verfügbar sein oder ausfallen, so …

Ausfallsituationen werden dokumentiert
- Automatisches Logging (S 1.8)

Potenzielle Ausfallszenarien werden regelmäßig simuliert sowie geübt
- Regelmäßige Sicherheitstests, Penetrationstests
- Die Wiederherstellbarkeit anhand der Backup-Kopien wird regelmäßig überprüft (S 1.6)

## Zu S 1.13 Sensibilisierung

Ansprechpartner zu Sicherheitsfragen stehen bereit
- Für Fragen, Anregungen und Beschwerden zum Thema Sicherheit …

Es werden Informationsmaterialien zu Sicherheitsaspekten offeriert
- Eigenes Informationsportal (z. B. Trust-Center)
- Webseite/Paper zum Thema Security

Es werden Einführungen zum Thema IT-Sicherheit angeboten
- Tutorials (auch online, in Video-Form)

… sowie weiter gehende Schulungen angeboten …
- Workshops (auch online, in Video-Form)

## Zu S 1.14 Absicherung der Virtualisierung

Es werden Garantien zur Performance, Verfügbarkeit und Reaktionszeit gegeben
- Verfügbarkeit des Services von mindestens X % der Zeit
- Die durchschnittlich/minimal bereitgestellte Leistung während der Verfügbarkeit beträgt mindestens X pro Y
- Die durchschnittliche Reaktionszeit während der Verfügbarkeit beträgt maximal X

Die Leistungsdaten sowie die Integrität werden regelmäßig überwacht
- Die Verfügbarkeit des Services wird laufend überwacht
- Die Wiederherstellbarkeit anhand der Backup-Kopien wird regelmäßig überprüft (S 1.6)

Start, Update und Terminierung der Virtualisierungsserver und der virtuellen Systeme sind geregelt
- Die Cloud-Plattform wird im laufenden Betrieb jeweils auf dem aktuellsten Stand gehalten

Die Nutzungsbedingungen regeln, was in der Virtualisierung erlaubt ist (z. B. Einsatz von Gastprogrammen)
- Acceptable Use Policy

Isolation sowie Kapselung sind verbindlich geregelt
- Es werden keine Dienste in derselben Cloud-Umgebung betrieben, die …

Die Zeitsynchronität der Virtualisierungen ist verbindlich festgelegt sowie technisch gewährleistet (falls Synchronität erforderlich ist)
- Für das Timing wird garantiert …

## Zu S 1.15 Schutz vor Schadprogrammen

Konzept zum Schutz vor Schadprogrammen ist in Regeln verankert
- Eigener Abschnitt zum Schutz vor Schadprogrammen
- Antivirus-/Antimalware-Protection

Es werden Programme zum Schutz vor Schadsoftware eingesetzt sowie aktuell gehalten
- Antivirenprogramm und Antimalwareprogramm mit automatisch aktualisierten Signaturen

Alle eingehenden Daten werden automatisch geprüft
- Echtzeitscanner

Informationen zu aufgespürten Schadprogrammen werden zentral erfasst sowie archiviert
- Automatisches Logging aller Vorkommnisse im Zusammenhang mit Schadprogrammen (S 1.8)

Für den Notfall werden Rettungsmittel vorrätig gehalten
- Recovery-Medien
- Ausweichsysteme

Es werden Materialien/Schulungen zur Sicherheit vor Schadprogrammen angeboten, insbesondere zum Verhalten, wenn der Verdacht besteht, dass ein Befall mit Schadprogrammen vorliegen könnte

- Sensibilisierung gegenüber Schadprogrammen (S 1.13)
- Erste Maßnahmen, wenn der Verdacht besteht, dass ein Schadprogramm aktiviert wurde:
  - Sperrung von Zugängen
  - Erfassung und Beseitigung des Schadprogramms
  - gegebenenfalls Wiederherstellung
  - Ansprechpartner

## Zu S 1.16 Sicheres Outsourcing

Zuständigkeiten, Rechte und Pflichten sind verbindlich geregelt

- Service-Agreement
  - Right to use
  - Responsibilities
- Datenschutz (S 1.9) und Aufbewahrung, Löschung und Rückgabe von Daten (S 1.10)

Die (technische, rechtliche) Machbarkeit ist geprüft

- Acceptable Use Policy
- Compliance with the Law

Das Sicherheitskonzept mit allen zugehörigen Maßnahmen ist explizit verbindlich geregelt

- Rechtsverbindlich werden alle erforderlichen Sicherheitsmaßnahmen garantiert (S 1.1 bis S 1.16)

Für Änderungen sowie Abweichungen im laufenden Betrieb sind Vereinbarungen getroffen

- Bei Änderung der Nutzungsbedingungen erfolgt eine Vorabinformation mindestens X Monate vor der Einführung der Änderung
- Für den Fall, dass die vereinbarten Leistungen nicht gewährt werden können ...

Für Migration sowie Beendigung des Vertragsverhältnisses sind verbindliche Regeln festgelegt

- Die ordentliche Kündigung ist mit einer Frist von X jeweils zum Y möglich
- Der Vertrag läuft bis zum X und wird automatisch um Y verlängert, wenn nicht bis zum Z schriftlich gekündigt wird
- Der Vertrag läuft bis zum X und wird nicht automatisch verlängert

# Datenschutz-Zertifizierung durch private Stellen

## 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“

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ wird im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) vom Kompetenzzentrum Trusted Cloud in Kooperation mit Projektpartnern des Technologieprogramms Trusted Cloud durchgeführt.

Am Pilotprojekt sind alle maßgeblichen Interessenvertreter beteiligt. Dazu gehören insbesondere Datenschutzbehörden und Privatwirtschaft, d. h. Anbieter und Nutzer von Cloud-Diensten, sowie Stellen mit Erfahrung in Normung und Zertifizierung von IT Diensten. Die Zahl der Projektbeteiligten ist begrenzt, um die Arbeitsfähigkeit der Gruppe sicherzustellen. Das Pilotprojekt wird von Prof. Dr. Georg Borges (Universität des Saarlandes) vom Kompetenzzentrum Trusted Cloud geleitet.

# Die Bedeutung der datenschutzrechtlichen Compliance-Zertifizierung

Die Bedeutung von Zertifizierungen im Bereich des Datenschutzes und die rechtliche Einordnung der Zertifizierung als öffentliche Aufgabe oder private Tätigkeit folgen aus der aktuellen Diskussion zu einer datenschutzrechtlichen Compliance-Zertifizierung und zum Entwurf der europäischen Datenschutz-Grundverordnung.

## Bedarf an einer datenschutzrechtlichen Compliance-Zertifizierung

Die Zertifizierung im Bereich des Datenschutzes ist Gegenstand einer vielschichtigen Diskussion, in der sehr unterschiedliche Ziele und Ansätze einer solchen Zertifizierung vertreten werden. Dabei zeigt sich in jüngster Zeit, dass insbesondere ein Bedarf an einer Zertifizierung von Diensten besteht, in der die Erfüllung der datenschutzrechtlichen Anforderungen durch den zertifizierten Dienst geprüft und durch ein Zertifikat bestätigt wird.

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ hat in ihrem im September 2012 veröffentlichten Dokument „Datenschutzrechtliche Lösungen für Cloud Computing. Ein rechtspolitisches Thesenpapier“[1] ein Konzept für eine solche Zertifizierung einschließlich ihrer zentralen Elemente beschrieben.

## Gegenstand der datenschutzrechtlichen Compliance-Zertifizierung

Unter Zertifizierung versteht das Konzept der AG Rechtsrahmen die Wissensbekundung der Zertifizierungsstelle über die Erfüllung der datenschutzrechtlichen Anforderungen an den geprüften Dienst. Ergebnis der Zertifizierung in diesem Zusammenhang ist deshalb die Erteilung eines Testats über die Einhaltung der einschlägigen rechtlichen Normen. Insofern wird zutreffend synonym auch der Begriff „Compliance-Zertifikat“ verwendet.

Die datenschutzrechtliche Compliance-Zertifizierung ist von Verfahren abzugrenzen, die mit der Erteilung eines Gütesiegels enden können, da in einem Gütesiegel-Verfahren nicht nur die einschlägigen rechtlichen Normen die Prüfungskriterien sind, sondern auch darüber hinausgehende oder abweichende datenschutzrechtliche Bewertungen berücksichtigt werden können. Ebenso ist sie von allen Verfahren abzugrenzen, in denen einzelne oder mehrere datenschutzrechtliche Aspekte berücksichtigt werden, aber nicht die Gesamtheit der gesetzlichen (datenschutzrechtlichen) Anforderungen geprüft wird.

Im Pilotprojekt „Datenschutz-Zertifizierung für Cloud Computing“ des BMWi-Technologieprogramms „Trusted Cloud“ werden die Elemente einer datenschutzrechtlichen Compliance-Zertifizierung für Cloud-Dienste ausgearbeitet.[2] Das Pilotprojekt beruht auf dem Konzept der AG Rechtsrahmen und strebt an, die Kernelemente einer datenschutzrechtlichen Compliance-Zertifizierung zu erarbeiten. Dabei werden auf der Grundlage der gesetzlichen Anforderungen einheitliche Prüfanforderungen, das Trusted-Cloud-Datenschutzprofil für Cloud-Dienste, entwickelt.

1 Das Papier ist abrufbar über www.trusted-cloud.de

2 Siehe zum Pilotprojekt unter www.trusted-cloud.de/569.php

# Zertifizierung durch Behörden oder private Stellen?

Im Rahmen einer datenschutzrechtlichen Compliance-Zertifizierung ist es von zentraler Bedeutung, ob das Zertifizierungsverfahren als ein öffentlich-rechtliches oder als ein privatrechtliches Verfahren ausgestaltet ist und ob die Zertifizierungsstelle eine Behörde oder ein privates Unternehmen ist.

Diese Frage ist bisher nicht umfassend gesetzlich geregelt. Das Konzept der AG Rechtsrahmen des Cloud Computing spricht sich dafür aus, dass die Zertifizierung durch geeignete private Stellen erfolgt. Die Anforderungen an private Zertifizierungsstellen und an das Zertifizierungsverfahren sollten nach diesem Konzept gesetzlich geregelt sein.

So heißt es in These 8 des Thesenpapiers wie folgt: „Das Testat sollte (auch) durch qualifizierte private Stellen vergeben werden. […]“[3]

These 10 führt ergänzend dazu u. a. aus: „Die Akkreditierung sollte durch geeignete, insbesondere fachlich qualifizierte und unabhängige Stellen erfolgen. Die EU-Datenschutz-Grundverordnung sollte die Anforderungen an die Akkreditierungsstellen im Grundsatz regeln, die Benennung der Akkreditierungsstellen den Mitgliedstaaten überlassen.“

Im Rahmen der europäischen Datenschutz-Grundverordnung können entscheidende Weichenstellungen für den rechtlichen Charakter der Zertifizierung erfolgen.

3 AG Rechtsrahmen, Datenschutzrechtliche Lösungen für Cloud Computing (Fn. 1), These 8 (S. 18).

# Rechtliche Grundlagen der datenschutzrechtlichen Compliance-Zertifizierung

Eine allgemeine gesetzliche Regelung der datenschutzrechtlichen Compliance-Zertifizierung besteht bisher in Deutschland auf Bundesebene nicht; der eine solche Regelung erlaubende § 9a BDSG von 2001 wurde bislang nicht ausgefüllt. In Einzelfällen sieht das Gesetz eine datenschutzrechtliche Compliance-Zertifizierung vor. So ist nach § 18 Abs. 3 Nr. 4, 2. Halbs. De-Mail-Gesetz die Erfüllung der datenschutzrechtlichen Anforderungen an den De-Mail-Dienst durch ein Zertifikat der BfDI nachzuweisen. Auf Landesebene besteht in Schleswig-Holstein auf Grundlage des § 4 Abs. 2 LDSG die Datenschutzgütesiegelverordnung[4], die die Vergabe eines Datenschutzgütesiegels regelt. In Bremen wurde 2004 auf Grundlage von § 7b BremDSG die Bremische Datenschutzauditverordnung (BremDSAuditV) erlassen, auf deren Basis ein Bremisches Datenschutzaudit-Gütesiegel vergeben werden kann, jedoch ausschließlich für öffentliche Stellen des Landes Bremen. Mit Ende 2014 tritt die BremDSAuditV außer Kraft. Seit 2011 sind die öffentlichen Einrichtungen Mecklenburg-Vorpommerns durch § 5 Abs. 2 DSG M-V gehalten, vorrangig zertifizierte IT-Produkte einzusetzen. Das Prüfverfahren dazu ist im Benehmen mit dem Landesbeauftragten für den Datenschutz durchzuführen[5].

Gesetzliche Regeln zu Aspekten der Zertifizierung bestehen vor allem auf europäischer Ebene in Form der Verordnung 765/2008.[6] In Ausführung der Verordnung wurden in den Mitgliedstaaten Gesetze über Akkreditierungen erlassen, in Deutschland durch das Akkreditierungsstellengesetz (AkkStelleG).[7] Die Bedeutung der Verordnung 765/2008 und des AkkStelleG für eine datenschutzrechtliche Zertifizierung ist nicht abschließend geklärt. Soweit die datenschutzrechtliche Zertifizierung künftig durch die europäische Datenschutz-Grundverordnung geregelt werden sollte, ginge diese der VO 765/2008 jedoch vor.

Die europäische Datenschutz-Grundverordnung könnte eine gesetzliche Regelung der datenschutzrechtlichen Zertifizierung bringen oder jedenfalls entscheidende Weichen stellen. Jedoch ist derzeit noch unklar, welche Position die Verordnung enthalten wird.

4 Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) vom 30.11.2013 (GVOBl. 2013, S. 536).

5 Landesrechtliche Erwähnungen finden sich darüber hinaus in § 11c Brandenburgisches Datenschutzgesetz und § 4 Abs. 2 i.V.m. § 10a Datenschutzgesetz Nordrhein-Westfalen.

6 Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften zur Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates, ABl. EU Nr. L 218/30 vom 13.08.2008.

7 Gesetz über die Akkreditierungsstelle (AkkStelleG) vom 31.07.2009, BGBl. I S. 2625.

# Datenschutz-Zertifizierung im Entwurf der Datenschutz-Grundverordnung

Der Entwurf der Europäischen Kommission zur Datenschutz-Grundverordnung (DSGVO) enthält in Art. 39 eine – sehr allgemeine – Bezugnahme auf Zertifizierungen, enthält aber keine Festlegungen in Bezug auf den rechtlichen Charakter der Zertifizierung und die Eigenschaften der Zertifizierungsstelle. In der Diskussion der Datenschutz-Grundverordnung im Europäischen Parlament und im Ministerrat sind auch zu Art. 39 weitreichende Änderungsvorschläge erarbeitet worden.

Der am 12. März 2014 verabschiedete Entwurf des Europäischen Parlamentes[8] sieht eine umfangreiche Regelung zur Zertifizierung in Art. 39 DSGVO (EP) vor. Die zentrale Grundlage soll Art. 39 Abs. 1a DSGVO (EP) sein, der wie folgt lautet: „Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird […].“

Die hier genannte Zertifizierung entspricht im Grundgedanken dem Konzept der datenschutzrechtlichen Compliance-Zertifizierung, wie sie auch im Thesenpapier der AG „Rechtsrahmen des Cloud Computing“ entwickelt wird.

Im Vorschlag des Europäischen Parlaments wird die Zertifizierung jedoch vor allem als Aufgabe der Aufsichtsbehörden gesehen. Dies ergibt sich aus Art. 39 Abs. 1a DSGVO (EP), aber auch aus Art. 39 Abs. 1d DSGVO (EP), dessen letzter Satz lautet: „Die endgültige Zertifizierung erteilt die Aufsichtsbehörde.“

Das Europäische Parlament spricht sich demnach dafür aus, dass eine Zertifizierung durch die Aufsichtsbehörden möglich sein soll und dass die verantwortliche Stelle einen Anspruch auf Zertifizierung gegen die Aufsichtsbehörden hat. Der rechtliche Charakter des Zertifizierungsverfahrens wird im Vorschlag des Europäischen Parlaments nicht abschließend festgelegt. Es wird auch nicht eindeutig geregelt, ob die Zertifizierung den Aufsichtsbehörden vorbehalten sein soll oder ob auch private Stellen die Möglichkeit haben sollen, ein Compliance-Zertifikat mit der Bedeutung des Art. 39 Abs. 1d DSGVO (EP) auszustellen.

Im aktuellen Entwurf der italienischen Ratspräsidentschaft vom 3. Oktober 2014[9] wird die Ergänzung des Art. 39 durch einen Art. 39a vorgeschlagen, in dem die Anforderungen an die Zertifizierung und das zugrunde liegende Zertifizierungsverfahren näher geregelt werden. Nach Art. 39a Abs. 1 DSGVO (RP) muss die Zertifizierungsstelle unabhängig sein und über eine hinreichende Sachkunde verfügen. Sie muss weiterhin auch akkreditiert sein. Art. 39a Abs. 2 DSGVO (RP) nennt mehrere Bedingungen für die Akkreditierung von Zertifizierungsstellen. Der Entwurf des Ministerrats geht also davon aus, dass die Zertifizierung jedenfalls auch eine Aufgabe privater, akkreditierter Zertifizierungsstellen ist.

8 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), ordentliches Gesetzgebungsverfahren: erste Lesung

9 Ratsdokument Nr. 13772/14 vom 3.10.2014, abrufbar unter http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT.

# Gründe für eine Zertifizierung durch Aufsichtsbehörden[10] oder private Stellen

Die Frage, ob die Datenschutz-Zertifizierung nach der Datenschutz-Grundverordnung durch Aufsichtsbehörden oder durch private Stellen erteilt werden soll, ist im Licht der Vor- und Nachteile der in Betracht kommenden Optionen zu bewerten.

## Zertifizierung als Aufgabe der Aufsichtsbehörden

Für die Einordnung der datenschutzrechtlichen Compliance-Zertifizierung als Aufgabe öffentlicher Träger, insbesondere der Aufsichtsbehörden, können gewichtige Argumente genannt werden.

- Aufsichtsbehörden haben aufgrund ihrer Kontrolltätigkeit eine klare Vorstellung von den Anforderungen datenschutzrechtlicher Vorschriften und können deshalb die Datenschutzkonformität eines Datenumgangs sachgerecht beurteilen.

- Eine Zertifizierung durch Aufsichtsbehörden kann für das Unternehmen Rechtssicherheit schaffen, da anzunehmen ist, dass die Behörde bei ihrer Aufsichtstätigkeit einer von ihr vorgenommenen Zertifizierung nicht widersprechen wird. Damit würde die Zertifizierung jedenfalls eine faktische Selbstbindung der Aufsichtsbehörde auslösen.

- Behördliche Zertifizierungsverfahren einschließlich der Kostenregelung können vom Staat durch Verwaltungsnormen transparent geregelt werden und unterliegen einer rechtsstaatlichen Kontrolle.

- Aufsichtsbehörden können als Zertifizierer dienen, wenn keine geeigneten privaten Anbieter zur Verfügung stehen, und sind deshalb ein wichtiges Instrument, um der Wirtschaft den Zugang zur Zertifizierung zu ermöglichen.

10 Der Begriff umfasst in Anlehnung an die Terminologie des Entwurfs der Datenschutz-Grundverordnung die Datenschutzaufsichtsbehörden sowie sonstige Stellen, die eine Aufsichtsfunktion wahrnehmen, insbesondere die Datenschutzbeauftragten des Bundes und der Länder.

## Zertifizierung als Aufgabe privater Stellen

Für die Einordnung der datenschutzrechtlichen Compliance-Zertifizierung als Aufgabe privater Stellen, insbesondere geeigneter Unternehmen, sprechen ebenfalls wichtige Gründe.

- Audits und Zertifizierungen durch private Stellen sind im Bereich der Informationstechnologie weit verbreitet und haben sich bewährt. Diese umfassen auch schon datenschutzrechtliche Anforderungen.

- Wenn die Zertifizierung als private Wirtschaftstätigkeit erfolgen kann, können Marktmechanismen genutzt werden. Durch Wettbewerb können sich effiziente und kostengünstige Zertifizierungen herausbilden. Dies gewährleistet, dass das vom Europäischen Parlament angestrebte Ziel einer erschwinglichen und kostengünstigen Zertifizierung erreicht wird.

- Die freiwillige Zertifizierung sollte von der behördlichen Kontrolle durch Aufsichtsbehörden getrennt sein, da es sonst leicht zu einer Vermischung von Aufsichtstätigkeit und gebührenfinanzierter Zertifizierung kommen kann.

- Aufsichtsbehörden können aufgrund einer Zertifizierungstätigkeit, durch die sie Einnahmen erzielen, hinsichtlich ihrer sonstigen Beratungsaufgaben, aber auch hinsichtlich ihrer Kontrolltätigkeit befangen sein.

- Aufsichtsbehörden haben nicht die erforderlichen Kapazitäten, um den gesamten Zertifizierungsbedarf der Privatwirtschaft abzudecken. Diese Kapazitäten können auch nur mit Schwierigkeiten aufgebaut werden, da nicht gesichert ist, dass das entsprechende Personal der Aufsichtsbehörden anderweitig eingesetzt werden kann. Es sind daher problematische Verzögerungen bei der Erteilung von Zertifikaten zu erwarten.[11]

- Wenn zahlreiche Zertifizierungsanträge eingehen und diese innerhalb einer bestimmten Frist erledigt sein müssen, kann dies aufgrund der beschränkten Kapazitäten der Aufsichtsbehörden auch dazu führen, dass andere Aufgaben nicht mehr angemessen erfüllt werden können.

11 Im Bereich des Schienenverkehrs wird in Deutschland derzeit eine Gesetzesänderung vorbereitet, die die bisher dem Eisenbahn-Bundesamt vorbehaltene Zulassung von Schienenfahrzeugen für private Prüfunternehmen öffnet, um bisher eingetretene Verfahrensverzögerungen zu vermeiden.

## Keine Beschränkung der Compliance-Zertifizierung auf Aufsichtsbehörden

Der Vorschlag des Europäischen Parlaments zu einem neu gefassten Art. 39 DSGVO (EP) kann dahingehend verstanden werden, dass die datenschutzrechtliche Compliance-Zertifizierung den Aufsichtsbehörden vorbehalten sein soll. Der Vorschlag könnte auch dahin verstanden werden, dass zwar private Stellen Zertifizierungen vergeben können, dass aber jedenfalls die zentrale rechtliche Wirkung des Zertifikats nach Art. 26 der Entwürfe zur DSGVO einem von den Aufsichtsbehörden verliehenen Zertifikat vorbehalten sein soll. Nach Art. 26 darf der Auftraggeber auf eine Zertifizierung im Sinne des Art. 39 vertrauen.[12] Damit wäre faktisch eine Beschränkung auf Aufsichtsbehörden begründet, da die Compliance-Zertifizierung gerade auf die Wirkung des Art. 26 abzielt.

Eine Monopolisierung der datenschutzrechtlichen Compliance-Zertifizierung bei den Aufsichtsbehörden wäre problematisch. Eine Notwendigkeit, die Zertifizierung staatlichen Stellen vorzubehalten, ließe sich nur begründen, wenn private Stellen die erforderliche Unabhängigkeit und Eignung nicht aufwiesen. Dies wird man auch im Bereich der datenschutzrechtlichen Zertifizierung nicht annehmen können. Prüfungen und Zertifizierungen werden in den meisten Bereichen, namentlich bei der Zertifizierung technischer Produkte, von privaten Stellen durchgeführt. Dies gilt auch bei Produkten mit hohen Sicherheitsanforderungen. Auch der europäische Gesetzgeber setzt in anderen Bereichen auf ein Modell der Zertifizierung durch private Stellen. Insoweit ist an die Verordnung 765/2008[13] zu erinnern, die für Produktzertifizierungen nach bestimmten Normen eine Akkreditierung privater Zertifizierungsstellen („Konformitätsbewertungsstellen“) vorsieht.

Die Nutzung von Marktmechanismen für die Ermittlung angemessener Preise erscheint auch im Bereich der datenschutzrechtlichen Prüfungen und Zertifizierungen richtig. Allerdings ist es – insbesondere bei privatwirtschaftlicher Zertifizierung im Wettbewerb – erforderlich, die Einhaltung hinreichender Prüfanforderungen durch gesetzliche Anforderungen an die Zertifizierungsstellen und das Zertifizierungsverfahren zu sichern, wie es das Konzept der AG „Rechtsrahmen des Cloud Computing“ und der Entwurf der Ratspräsidentschaft vorsehen.[14]

Die Regelung zur Zertifizierung in der zu verabschiedenden DSGVO sollte dahin gehen, die Zertifizierung sowohl durch private Stellen als auch durch Aufsichtsbehörden zuzulassen. Damit könnte auch den unterschiedlichen Situationen in den Mitgliedstaaten Rechnung getragen werden. So mag es Mitgliedstaaten geben, in denen eine staatliche Stelle schon deswegen erforderlich ist, weil ein Markt für eine rein privatwirtschaftlich organisierte Zertifizierung nicht besteht. Es ist aber auch möglich, dass in einigen Mitgliedstaaten der Aufbau eines öffentlichen Verwaltungsapparats (einschließlich entsprechender Verwaltungsverfahrensregeln) zur umfassenden Durchführung der Zertifizierungen nicht zu leisten ist und daher Marktmechanismen greifen sollten, um ein funktionierendes Zertifizierungssystem zeitnah und erfolgreich zu realisieren.

Eine Beschränkung der Zertifizierung auf Aufsichtsbehörden ist daher abzulehnen.

12 Vgl. Art. 26 Abs. 2 lit. a DSGVO (RP); Art. 26 Abs. 3 lit. a DSGVO (EP).

13 Vgl. Fn. 6.

14 Vgl. Thesen 6–10 Thesenpapier AG Rechtsrahmen (Fn. 1); Art. 39a DSGVO (RP).

# Schlussfolgerungen

Datenschutzrechtliche Compliance-Zertifizierungen, wie sie auch im Entwurf der Datenschutz-Grundverordnung vorgesehen sind, leisten einen wichtigen Beitrag zur Rechtssicherheit und zur Verbesserung des Datenschutzniveaus bei modernen IT-Dienstleistungen, insbesondere im Cloud Computing.

Die Möglichkeit, datenschutzrechtliche Compliance-Zertifizierungen nach der europäischen Datenschutz-Grundverordnung zu vergeben, ist nicht auf Aufsichtsbehörden zu beschränken, sondern muss auch durch private Stellen erfolgen können. Dies sollte in der Datenschutz-Grundverordnung klargestellt werden.

# Anhang

Entwurf der Europäischen Kommission für eine „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ vom 25.1.2012 mit Änderungsvorschlägen des Europäischen Parlaments i. d. F. des Beschlusses vom 12.3.2014 und des Europäischen Rates i. d. F. des Entwurfs der Ratspräsidentschaft vom 3.10.2014.

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| **Erwägung 77**<br><br>Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen. | **Erwägung 77**<br><br>Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und standardisierte Datenschutzprüfzeichen eingeführt werden, die den betroffenen Personen einen raschen, zuverlässigen und überprüfbaren Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen. Ein „Europäisches Datenschutzsiegel“ sollte auf europäischer Ebene eingeführt werden, um unter betroffenen Personen Vertrauen und für die für die Verarbeitung Verantwortlichen Rechtssicherheit zu schaffen sowie gleichzeitig die Verbreitung europäischer Datenschutzstandards außerhalb der EU zu fördern, indem es nichteuropäischen Unternehmen vereinfacht wird, Zugang zu europäischen Märkten zu erhalten, indem sie sich zertifizieren lassen. | **Erwägung 77**<br><br>Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen. |
| **Artikel 39: Zertifizierung**<br><br>1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung. | **Artikel 39: Zertifizierung**<br><br>1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung. | **Artikel 39: Zertifizierung**<br><br>1. Die Mitgliedstaaten, der Europäische Datenschutzausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen, die von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern durchgeführt werden, eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen. |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | 1a. Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird, insbesondere mit den Grundsätzen der Artikel 5, 23 und 30, den Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter und den Rechten der betroffenen Person. | 1a. Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 2a genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 42 Absatz 2e geeignete Garantien bieten. Diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher Instrumente oder auf andere Weise die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden. |
| | 1b. Die Zertifizierung ist freiwillig, erschwinglich und über ein transparentes und nicht übermäßig aufwendiges Verfahren zugänglich. | |
| | 1c. Die Aufsichtsbehörden und der Europäische Datenschutzausschuss arbeiten im Rahmen des Kohärenzverfahrens gemäß Artikel 57 zusammen, um ein harmonisiertes datenschutzspezifisches Zertifizierungsverfahren zu gewährleisten, einschließlich harmonisierter Gebühren innerhalb der Union. | |
| | 1d. Während des Zertifizierungsverfahrens kann die Aufsichtsbehörde spezialisierte dritte Prüfer akkreditieren, die Prüfung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für sie durchzuführen. Dritte Prüfer verfügen über ausreichend Personal, sind unparteiisch und in Bezug auf ihre Aufgaben frei von Interessenkonflikten. Aufsichtsbehörden entziehen die Akkreditierung, wenn es Grund zu der Annahme gibt, dass der Prüfer seine Aufgaben nicht korrekt erfüllt. Die endgültige Zertifizierung erteilt die Aufsichtsbehörde. | |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | 1e. Die Aufsichtsbehörden erteilen den für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, denen nach der Prüfung zertifiziert wird, dass sie personenbezogene Daten im Einklang mit dieser Verordnung verarbeiten, das standardisierte Datenschutzzeichen mit der Bezeichnung „Europäisches Datenschutzsiegel“. | |
| | 1f. Das „Europäische Datenschutzsiegel“ ist so lange gültig, wie die Verarbeitungsprozesse des zertifizierten für die Verarbeitung Verantwortlichen oder des zertifizierten Auftragsverarbeiters weiter vollständig dieser Verordnung entsprechen. | |
| | 1g. Unbeschadet des Absatzes 1f ist die Zertifizierung höchstens fünf Jahre gültig. | |
| | 1h. Der Europäische Datenschutzausschuss richtet ein öffentliches elektronisches Register ein, in dem die Öffentlichkeit Einsicht in alle gültigen und ungültigen Zertifikate, die von den Mitgliedstaaten ausgestellt wurden, nehmen kann. | |
| | 1i. Der Europäische Datenschutzausschuss kann auf eigene Initiative zertifizieren, dass ein technischer Standard zur Verbesserung des Datenschutzes mit dieser Verordnung vereinbar ist. | |
| 2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen. | 2. Die Kommission wird ermächtigt, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat und nach Anhörung von Interessenträgern, insbesondere Industrieverbänden und nichtstaatlichen Organisationen, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in den Absätzen 1a bis 1h genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Akkreditierung der Prüfer, der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen. Mit diesen delegierten Rechtsakten werden den betroffenen Personen durchsetzbare Rechte übertragen. | 2. Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörde, die gemäß Artikel 51 oder 51a zuständig ist. |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | | 2a. Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde anhand der von der zuständigen Aufsichtsbehörde genehmigten Kriterien oder – gemäß Artikel 57 – durch den Europäischen Datenschutzausschuss erteilt. |
| 3. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen. | 3. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen. | 3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 39a oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten. |
| | | 4. Die Zertifizierung wird einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die einschlägigen Voraussetzungen weiterhin erfüllt werden. Sie wird durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden. |
| | | 5. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z. B. über das Europäische E-Justiz-Portal. |
| | | **Artikel 39a<br>Zertifizierungsstelle<br>und -verfahren**<br><br>1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat teilt mit, ob diese Zertifizierungsstellen akkreditiert wurden von<br><br>(a) der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde und/oder |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | | **Artikel 39a Zertifizierungsstelle und -verfahren**<br><br>(b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde. |
| | | 2. Die Zertifizierungsstelle nach Absatz 1 kann zu diesem Zweck nur akkreditiert werden, wenn<br><br>(a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;<br><br>(aa) sie sich verpflichtet hat, die Kriterien nach Artikel 39 Absatz 2a, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – von dem Europäischen Datenschutzausschuss genehmigt wurden, einzuhalten;<br><br>(b) sie Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzsiegel und -prüfzeichen festgelegt hat;<br><br>(c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;<br><br>(d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | | 3. Die Akkreditierung der Zertifizierungsstellen nach Absatz 1 erfolgt anhand der Kriterien, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder, gemäß Artikel 57, von dem Europäischen Datenschutzausschuss genehmigt wurden. Im Fall einer Akkreditierung nach Absatz 1b ergänzen diese Anforderungen diejenigen, die in der Verordnung 765/2008 und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind. |
| | | 4. Die Zertifizierungsstelle nach Absatz 1 ist unbeschadet der Verantwortung, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die Stelle die Anforderungen erfüllt. |
| | | 5. Die Zertifizierungsstelle nach Absatz 1 teilt der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit. |
| | | 6. Die Anforderungen nach Absatz 3 und die Kriterien nach Artikel 39 Absatz 2a werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht. Die Aufsichtsbehörde übermittelt diese auch dem Europäischen Datenschutzausschuss. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z. B. über das Europäische E-Justiz-Portal. |

| EU-KOMMISSION | EUROPÄISCHES PARLAMENT | EUROPÄISCHER RAT |
|---|---|---|
| | | (6a) Unbeschadet der Bestimmungen des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind. |
| | | 7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen festzulegen, die für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind [, einschließlich der Bedingungen für die Erteilung und den Widerruf der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung und der Anforderungen für ein standardisiertes „Europäisches Datenschutzsiegel“ in der Union und in Drittländern]. |
| | | (7a) Der Europäische Datenschutzausschuss gibt der Kommission gegenüber eine Stellungnahme zu den Kriterien und Anforderungen, auf die in Absatz 7 Bezug genommen wird, ab. |
| | | 8. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen festlegen. Die betreffenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen. |

## Das Thesenpapier zur Datenschutz-Zertifizierung durch private Stellen

Das rechtspolitische Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“ wurde vom Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ und von der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erstellt.

## Mitwirkende/Autoren

**Dr. Thorsten B. Behling, WTS Rechtsanwaltsgesellschaft mbH**

**Oliver Berthold,** Berliner Beauftragter für Datenschutz und Informationsfreiheit

**Prof. Dr. Georg Borges,** Kompetenzzentrum Trusted Cloud

**Dirk Bungard,** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

**Mathias Cellarius,** SAP SE

**Dr. Astros Chatziastros,** TMF e.V.

**Susanne Dehmel,** BITKOM

**Thomas Doms,** TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria

**Dr. Alexander Duisberg,** Bird & Bird LLP

**Günther Eble,** Kommunale Informationsverarbeitung Baden-Franken

**Alexander Glaus,** Deutsche Bank AG

**Björn Hajek, LL.M.,** Infineon Technologies AG

**Dr. Marc Hilber, LL.M.,** Oppenhoff & Partner

**Claudia Husz,** regio IT

**Dr. Hubert Jäger,** Uniscon universal identity control GmbH

**Nicolas Kölsch,** WTS Consulting

**Rudi Kramer,** DATEV eG

**Thomas Kranig,** Bayerisches Landesamt für Datenschutzaufsicht

**Steffen Kroschwald,** Universität Passau

**Johannes Landvogt,** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

**Dirk Piesker,** Deutsche Telekom AG

**Patrick Quellmalz,** VOICE e.V.

**Christoph Rechsteiner,** SAP SE

**Frederick Richter,** Stiftung Datenschutz

**Stephan Sädtler,** Universität Passau

**Gunther Schiefer,** Karlsruher Institut für Technologie

**Gabriel Schulz,** Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

**Antonius Sommer,** TÜViT GmbH

**Dr. Christoph Sutter,** TÜViT GmbH

**Karin Vedder,** Bayerisches Landesamt für Datenschutzaufsicht

**Dr. Joseph Walenta,** Deutsches Herzzentrum Berlin

**Dr. Mathias Weber,** BITKOM

**Andreas Weiss,** Eurocloud Deutschland_eco e.V.

**Magda Wicker,** Universität Kassel

**Monika Wojtowicz,** TÜViT GmbH

# Schweigepflicht bei der Auslagerung von IT-Dienstleistungen

## 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.

# Einführung

Auch Angehörige von Berufsgruppen, die einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, lagern IT-Dienstleistungen an externe Spezialisten aus (sogleich Ziff. 1). Dies gilt nicht nur für etablierte IT-Dienstleistungen wie die (Fern-) Wartung von EDV-Systemen, sondern zunehmend auch für innovative IT-Angebote. So eröffnet Cloud Computing auch Berufsgeheimnisträgern wesentlich erweiterte Möglichkeiten, externe IT-Dienstleistungen in Anspruch zu nehmen und dadurch ihre eigenen Dienste zu verbessern.

Allerdings besteht bei Berufsgeheimnisträgern erhebliche Rechtsunsicherheit, ob die Auslagerung von IT-Dienstleistungen mit der strafbewehrten Schweigepflicht vereinbar ist. Das Papier erörtert die Probleme der geltenden Rechtslage (Ziff. 2–3) anhand relevanter Fallgruppen von IT-Dienstleistungen (Ziff. 4) und plädiert aufgrund der hohen Bedeutung für die Praxis (Ziff. 5–6) für eine Änderung des Gesetzes (Ziff. 7). Schließlich werden mögliche Optionen für eine Gesetzesänderung dargestellt (Ziff. 8).

# 1 Zunehmende Inanspruchnahme von externen IT-Dienstleistern durch Berufsgeheimnisträger

Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB, zu denen u.a. Ärzte, Rechtsanwälte, Steuerberater und Angehörige von Unternehmen der privaten Kranken-, Unfall- und Lebensversicherung gehören, bedienen sich zur Erfüllung ihrer Aufgaben bzw. zum Betrieb ihres Unternehmens zunehmend externer Dienstleister. Grund für solche Auslagerungen sind teils die Einsparung von Kosten oder begrenzte räumliche Kapazitäten, vor allem aber die Erforderlichkeit von besonderem Fachwissen, über das häufig nur spezialisierte Dienstleister verfügen. Dies gilt angesichts der ständig wachsenden Bedeutung der elektronischen Datenverarbeitung insbesondere für Dienstleistungen im IT-Bereich. So werden an externe Spezialisten Aufgaben ausgelagert, die in Zeiten manueller Datenverarbeitung in den Praxen, Kanzleien und Unternehmen selbst erbracht worden sind.

Grundlage für die Auslagerung war die Entwicklung der Informations- und Kommunikationstechnologie, die eine zunehmende Vernetzung ermöglicht. Bedient sich Informations- und Kommunikationstechnologie öffentlicher Netze, eröffnen sich Möglichkeiten des Zugriffs aber auch für Unbefugte. Werden mit Hilfe von Informations- und Kommunikationstechnologie IT-Leistungen ausgelagert, könnten vertrauliche Informationen an einen weiteren Personenkreis – beispielsweise an die Mitarbeiter des IT-Dienstleisters – gelangen. Der Einsatz von Informations- und Kommunikationstechnologie birgt folglich Risiken. Um den Betroffenen derartiger Informationsverarbeitung, also etwa den Patienten oder Mandanten, zu schützen, hat der Gesetzgeber die Weitergabe von Daten datenschutzrechtlich streng reglementiert und sie unter bestimmten Voraussetzungen sogar unter Strafe gestellt.

# 2 Datenschutzrechtliche Vorgaben bezüglich der Einschaltung von externen Dienstleistern

Schaltet ein Unternehmen beispielsweise zur Speicherung von Daten oder zur Wartung von EDV-Anlagen einen externen Dienstleister ein, werden dem Dienstleister häufig personenbezogene Daten von Kunden überlassen; zumindest kann ein Zugriff des Dienstleisters auf solche Daten dabei nicht immer ausgeschlossen werden. Das Unternehmen verschafft somit dem externen Dienstleister die Möglichkeit, von Daten Kenntnis zu nehmen, die dem BDSG unterliegen.

Auf rein datenschutzrechtlicher Ebene, d. h. bei Sachverhalten, die nicht dem strafrechtlichen Berufsgeheimnisschutz unterliegen, kann die Datenweitergabe gegebenenfalls durch einen Vertrag mit dem Dienstleister über eine sogenannte Auftragsdatenverarbeitung nach § 11 BDSG rechtmäßig ausgestaltet werden: Unter bestimmten, im Gesetz näher geregelten Voraussetzungen wird der Dienstleister datenschutzrechtlich als eine Art interne Stelle des Auftraggebers angesehen, sodass eine Datenweitergabe an ihn keine Übermittlung im datenschutzrechtlichen Sinne darstellt (vgl. § 3 Abs. 8 Satz 3 BDSG).

§ 11 BDSG wird als allgemeine Regelung jedoch verdrängt, wenn bereichsspezifische Vorschriften zur Auftragsdatenverarbeitung den Sachverhalt abschließend regeln. So enthalten beispielsweise die meisten Landeskrankenhausgesetze für den Bereich der Krankenhäuser gegenüber § 11 BDSG vorrangige Regelungen, die für die Einschaltung externer Dienstleister zum Teil besonders strenge Vorgaben vorsehen oder eine Verarbeitung nur durch andere Krankenhäuser zulassen (z. B. Art. 27 Abs. 4 Satz 6 des Bayerischen Krankenhausgesetzes). Eine weitere Spezialregelung stellt beispielsweise für Sozialdaten § 80 SGB X dar. Handelt es sich beim Auftraggeber um eine öffentliche Stelle, sind statt § 11 BDSG zudem die entsprechenden Vorschriften des jeweiligen Landesdatenschutzgesetzes anzuwenden, soweit nicht auch diese gegenüber speziellen Regelungen zurücktreten. Sollen externe Dienstleister mit der Verarbeitung von Daten beauftragt werden, ist daher im Einzelfall zu prüfen, welche datenschutzrechtlichen Bestimmungen auf den Auftraggeber und den betroffenen Sachverhalt Anwendung finden und welche Vorgaben dementsprechend für die vorgesehene Auftragsdatenverarbeitung zu beachten sind.

Soweit die Überlassung personenbezogener Daten im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG erfolgt und daher keine Übermittlung im datenschutzrechtlichen Sinne darstellt (s. o.), ist zu berücksichtigen, dass diese Privilegierung auf den Bereich des Datenschutzrechts beschränkt ist. Eine etwaige Strafbarkeit nach § 203 Abs. 1 StGB bleibt hiervon jedoch unberührt (vgl. § 1 Abs. 3 Satz 2 BDSG). Auch soweit sich eine datenschutzrechtliche Rechtfertigung nach § 28 BDSG oder Spezialnormen (z. B. Forschung) ergibt, berührt dies die etwaige Strafbarkeit nach § 203 StGB nicht.

# 3 Strafbarkeitsrisiko bei der Einschaltung von externen Dienstleistern

Unabhängig von der datenschutzrechtlichen Beurteilung einer Auftragsdatenverarbeitung sowie den berufsrechtlichen Regelungen besteht die strafrechtliche Problematik, dass die Beauftragung externer Dienstleister als eine unbefugte Offenbarung von Berufsgeheimnissen angesehen werden kann, die – auch bei Vorliegen einer Auftragsdatenverarbeitung – nach § 203 Abs. 1 StGB strafbar ist.[1] Zur Frage, unter welchen Umständen von einer Offenbarung von Berufsgeheimnissen auszugehen ist, insbesondere ob hierfür bereits die Möglichkeit der Kenntnisnahme ausreicht oder ob der Dienstleister tatsächlich von den Daten Kenntnis nehmen muss, bestehen unterschiedliche Auffassungen. Da sich Berufsgeheimnisträger deshalb nicht sicher sein können, unter welchen Voraussetzungen die Einschaltung eines externen Dienstleisters eine unbefugte Offenbarung darstellt, unterliegen sie zumindest latent einem ständigen Strafbarkeitsrisiko, das in erster Linie die Geschäftsleitung und die sonst verantwortlich handelnden Personen trifft. In der Praxis führt dieses Risiko häufig dazu, dass Unternehmen, vor allem Kranken-, Lebens- und Unfallversicherungen, Krankenhäuser und andere Einrichtungen im Gesundheitswesen sowie Rechtsanwälte und Steuerberater, so weit wie möglich von der Einschaltung externer Dienstleister absehen, wenn diese mit vom Berufsgeheimnis geschützten Daten in Berührung kommen könnten. Dieser Umstand trägt wohl mit dazu bei, dass im Bereich der Verarbeitung von durch § 203 StGB geschützten Daten kaum Rechtsprechung zum Einsatz externer Dienstleister existiert (s. hierzu auch unten Ziff. 6). Dies führt dazu, dass moderne Technologien, wie z. B. Cloud Computing, in den betroffenen Wirtschaftsbereichen kaum zum Einsatz kommen und dadurch Wettbewerbsnachteile entstehen.

1 Werden Dienstgeheimnisse verletzt, kommt in besonderen Fällen darüber hinaus eine Strafbarkeit nach § 353b StGB in Betracht.

# 4 Exemplarische Darstellung von Fallkonstellationen im Bereich von IT-Dienstleistungen

Die Komplexität der Datenverarbeitung in Computersystemen und -netzwerken nimmt auch bei Berufsgeheimnisträgern kontinuierlich zu. Die Vertreter dieser Berufe und ihre Angestellten sind daher häufig nicht in der Lage, die technische Betreuung ihrer IT-Systeme selbst zu übernehmen bzw. auftretende technische Probleme selbst zu lösen. Nachfolgend wird für einige praxisrelevante Fallgruppen das Problem des Strafbarkeitsrisikos beim Einsatz von IT-Dienstleistern dargestellt.

## Wartung durch externe Dienstleister

Eine Wartung der IT durch externe Techniker vor Ort ist oftmals zeit- und kostenaufwendig. Über elektronische Kommunikationsmittel, insbesondere über das Internet, ist es allerdings möglich, aus der Ferne auf die Systeme zuzugreifen und die erforderliche Wartung durchzuführen.[2] Um technische Anlagen fernwarten zu können, muss ein Zugriff von einem entfernten Arbeitsplatz des Technikers auf die Anlage des Arztes, Anwalts oder Steuerberaters über eine Telekommunikationsverbindung ermöglicht werden (sogenannter Remote Access). Dabei kann der Techniker aber beispielsweise auch auf die im System abgelegten Datenordner und Daten zugreifen (Remote Terminal). Er kann sogar ganz die Kontrolle über das System übernehmen und z. B. die Benutzeroberfläche des Nutzers (inkl. Maus- und Tastatureingaben) einsehen oder selbst steuern (Remote Desktop).

Im Rahmen der Fernwartung können auch geschützte Geheimnisse im Sinne des § 203 StGB über öffentliche Kommunikationswege übertragen werden. Indem die Fernwartung ausschließlich über gesicherte Verbindungen, beispielsweise unter Nutzung von VPN-Tunneln, durchgeführt wird, kann der Berufsgeheimnisträger zwar einen Zugriff unbefugter Dritter auf die Datenübertragung zwischen seinem System und dem Fernwartungstechniker verhindern. Nicht auszuschließen ist allerdings, dass der Techniker selbst im Rahmen seiner Tätigkeit – beabsichtigt oder unbeabsichtigt – die auf dem System des Berufsgeheimnisträgers vorgenommenen Eingaben und gespeicherten Daten einsieht und dabei Berufsgeheimnisse zur Kenntnis nimmt. Indem der Berufsgeheimnisträger eine Fernwartung in Auftrag gibt und dadurch den Zugriff auf sein System eröffnet, ermöglicht er die Kenntnisnahme von Berufsgeheimnissen zumindest potenziell. Bereits hierin kann eine strafbare Offenbarung von Berufsgeheimnissen (gegebenfalls durch Unterlassen) durch den Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB liegen.

Die gleichen Probleme ergeben sich bei traditionellen Formen der IT-Wartung, bei denen ein Techniker in den Räumen des Berufsgeheimnisträgers auf dessen IT-Systeme Zugriff nimmt. Auch hier kommt eine Strafbarkeit des Berufsgeheimnisträgers nach § 203 StGB in Betracht.

2 Als Wartung definiert beispielsweise § 3 Abs. 3 Nr. 5 BbgDSG die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware. Nach § 3 Abs. 3 Nr. 6 BbgDSG ist Fernwartung die Wartung der Soft- und Hardware von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtungen zur Datenübertragung vorgenommen wird.

## Cloud-Storage-Dienste

In den letzten Jahren sind zahlreiche Dienste auf den Markt gekommen, mit denen Nutzer Daten von einem PC oder Smartphone auf einem entfernten Rechnersystem speichern, dort bearbeiten und Dritten zugänglich machen können. Der bekannteste dieser Dienste stammt vom US-amerikanischen Anbieter Dropbox. Es gibt mittlerweile zahlreiche derartige Dienste in verschiedensten Ausprägungen. Insbesondere haben auch die großen Hersteller von mobilen Betriebssystemen derartige Funktionen in ihre Angebote integriert (etwa iCloud® und Google Drive®). Ebenso bietet Microsoft mit seinem Angebot „OneDrive“ eine ebenfalls integrierte Synchronisationslösung für Daten an und versucht, mit dem Produkt „Office 365“ sogar die IT-Ressourcen seiner Kunden in seinen Rechenzentren zu bündeln, statt dass diese auf den Endgeräten der Kunden vorgehalten werden müssten. Auch wenn sich einige der bekannten Dienste nicht für den Einsatz durch Berufsgeheimnisträger eignen, gibt es daneben auch zahlreiche spezifische Cloud-Speicherdienste für Berufsgeheimnisträger.

Die Gemeinsamkeit solcher Cloud-Storage-Dienste ist die Möglichkeit, eine einmal über das Internet im System des Dienstleisters abgelegte Datei grundsätzlich von jedem mit dem Internet verbundenen geeigneten Endgerät abzurufen. Ein Nutzer kann die von ihm hochgeladenen Dateien regelmäßig anderen Nutzern zugänglich machen, z. B. durch das Versenden eines durch den Cloud-Storage-Dienst bereitgestellten Internetlinks. Möglich ist es in vielen Fällen auch, Dateien oder ganze Ordner insgesamt öffentlich zugänglich zu machen.

Die Grundidee solcher Dienste ist es, die Übertragung von größeren Datenmengen zu ermöglichen und dabei die technischen und praktischen Begrenzungen von beispielsweise E-Mails oder lokalen Speichermedien zu umgehen. Dies ist bislang auch der Hauptanwendungsfall von Cloud-Lösungen, wobei sogenannte „Collaboration“-Funktionen, also das gemeinsame, gleichzeitige Betrachten und Bearbeiten von Dateien, z. B. von Textdokumenten oder Präsentationen, in der allgemeinen Unternehmenspraxis stetig zunehmen.

Das Verwenden von Cloud-Storage-Diensten eröffnet verschiedene Anknüpfungspunkte für eine mögliche Strafbarkeit nach § 203 Abs. 1 StGB. So kann ein „Offenbaren“ schon im Hochladen einer Datei in die Systeme eines Cloud-Storage-Dienstleisters gesehen werden, denn dadurch wird sie zumindest dem Cloud-Storage-Dienstleister zugänglich gemacht. Zwar geben viele Anbieter an, das Hochladen über den Browser oder die entsprechende App auf mobilen Endgeräten erfolge über verschlüsselte, also durch Dritte nicht ohne weiteres einsehbare Verbindungen. Allerdings erfolgt in aller Regel weder die Speicherung noch die Verarbeitung der Daten in den Systemen des Cloud-Storage-Dienstleisters vollständig verschlüsselt; dies gilt insbesondere für die zahlreichen kostenlos angebotenen Dienste. Hinzu kommt, dass – soweit erkennbar – die Mehrheit der Cloud-Storage-Dienstleister ihrerseits Kapazitäten bei (weiteren) Rechenzentrumsbetreibern bezieht, um ihre Cloud-Dienste anbieten zu können. Damit besteht aus Sicht des Nutzers regelmäßig die Gefahr, dass es zu einer Kenntnisnahme der nach § 203 Abs. 1 StGB geschützten Daten durch noch andere Personen als den eigentlichen Vertragspartner kommt.

Man wird sicherlich einwenden können, dass es Berufsgeheimnisträgern zumutbar ist, im Rahmen ihrer Berufsausübung auf qualitativ höherwertige Anbieter von Cloud-Storage-Diensten zurückzugreifen. Die oben erwähnte Unsicherheit über die praktische Reichweite von § 203 Abs. 1 StGB einerseits und der Mangel an Diensten, die eine Ende-zu-Ende-Vollverschlüsselung enthalten, andererseits führen allerdings dazu, dass den von § 203 Abs. 1 StGB erfassten Berufsgruppen die Effizienzvorteile und Arbeitserleichterungen durch Cloud-Storage-Dienste faktisch nicht zur Verfügung stehen.

## Konfliktprüfungen

Insbesondere Steuerberater und Rechtsanwälte sind verpflichtet, widerstreitende Interessen bei der Beratung zu vermeiden. Für Steuerberater folgt dies aus § 6 BOStB, für Rechtsanwälte aus § 43a BRAO i.V.m. § 3 BORA. Dabei gilt diese Pflicht nicht nur für den einzelnen Berater, sondern im rechtsanwaltlichen Umfeld grundsätzlich auch für rechtsanwaltliche Berufsausübungs- oder Bürogemeinschaften gleich welcher Art (§ 3 Abs. 2 Satz 1 BORA) sowie im Steuerberatungskontext auch für Sozietäten, Steuerberatungsgesellschaften, Partnerschaftsgesellschaften, Anstellungsverhältnisse oder sonstige Formen der Zusammenarbeit (§ 6 Abs. 3 BOStB). Die Pflicht zur Vermeidung widerstreitender Interessen ist also sehr weit gefasst. Dies bestätigt auch § 33 BORA, wonach diese Pflicht auch dann gilt, wenn etwa Rechtsanwälte mit Steuerberatern kooperieren.

Gerade im Umfeld von Großkanzleien, die überregional, gegebenfalls sogar international über Niederlassungen, gesonderte Gesellschaften und/oder Kooperationspartner tätig werden, führt die Erfüllung dieser Pflicht zu erheblichen Herausforderungen. So ist trotz der häufig fehlenden Kenntnis der Einzelmandate im überregionalen oder internationalen Netzwerk sicherzustellen, dass keine Tätigkeit für mehrere Mandanten in derselben Rechtssache erfolgt. Denn eine solche wäre nur nach umfassender Information des Mandanten zulässig, wenn dieser sich sodann mit der Vertretung ausdrücklich einverstanden erklärt und die Belange der Rechtspflege nicht entgegenstehen (vgl. exemplarisch § 3 Abs. 2 Satz 2 BORA). Eine solche Aufklärung ist aber wiederum nur möglich, wenn feststeht, dass ein potenzieller Interessenkonflikt besteht.

Aus diesen Gründen lässt sich die Konfliktprüfung im Umfeld überregional agierender Kanzleien, Sozietäten und sonstiger Formen der überörtlichen Zusammenarbeit in der Regel nur durch den Einsatz technischer Lösungen realisieren, sogenannter Conflict-Check-Software. Diese muss vor der Mandatsaufnahme naturgemäß die Mandatsinformationen aller Beratungspartner miteinander abgleichen, um sicherstellen zu können, dass der Gegner des potenziellen Mandanten nicht bereits durch einen anderen Berater des Netzwerkes vertreten wird. Die Conflict-Check-Software wird dabei in aller Regel zentral gehostet sein, wobei sich hierzu vor allem Cloud-Lösungen anbieten. Denn bereits heute werden solche Softwareanwendungen regelmäßig entweder zentral bei einer (Berufs-)Gesellschaft der Beratungsgruppe gehostet oder es wird hierfür die Infrastruktur eines externen IT-Dienstleisters genutzt. Größere Beratungsgruppen verfügen mitunter auch über eine eigene IT-Gesellschaft, die die Software als zentraler IT-Dienstleister in der Gruppe bereitstellt bzw. auf ihren Systemen im Auftrag der Gruppengesellschaften betreibt. Unabhängig aber davon, ob die Software gruppenintern oder -extern gehostet wird, unterhalten international oder überregional tätige Kanzleien heute oft keine eigenen Server mehr. Eine technische Offenlegung der bestehenden Mandatsbeziehungen gegenüber der hostenden Gruppengesellschaft oder dem IT-Dienstleister – und damit einem Dritten – ist in aller Regel unumgänglich. Bereits hierin kann aber wiederum eine strafbare Offenbarung von Berufsgeheimnissen im Sinne des § 203 Abs. 1 StGB durch die beteiligten Berufsgeheimnisträger gesehen werden.

## Cloud-Lösungen für medizinische Versorgung und Forschung

Krankenhäuser sind mittelständische regionale Unternehmen oder auch Einrichtungen in öffentlicher Trägerschaft mit eigenen IT-Infrastrukturen, deren Betrieb aufwendig ist. Der Bedarf an nutzerorientierter Unterstützung der medizinischen Leistungserstellung durch Systeme der Informations- und Kommunikationstechnologie ist hoch, seine Befriedigung aber kostenintensiv. Innovation scheitert daher oft an den verfügbaren Budgets (Kostenträgerschaft und anteilige Infrastrukturkosten im Gesundheitswesen). Cloud-Computing stellt eine Alternative dar, vorausgesetzt, die hohen Anforderungen an Datenschutz und Datensicherheit, Interoperabilität, Skalierbarkeit sowie Verfügbarkeit werden erfüllt.

Dienste für softwaregestützte Bewertungs- und Analyseaufgaben im Bereich der medizinischen Diagnostik (z. B. Mustererkennung, Patternvergleiche) oder auch für die Beurteilung von Bildmaterial durch einen Spezialisten, ferner behandlungsbegleitende Services, wie z. B. AMTS[3]-Prüfungsprogramme, ließen sich mittels Cloud so bereitstellen, dass jederzeit auf sie zugegriffen werden kann und Ergebnisse ohne Zeitverzug abgerufen werden können.

Diese Dienste werfen Schwierigkeiten auf, wenn die Daten nicht nur über eine Cloud übertragen, sondern in der Cloud unverschlüsselt verarbeitet werden. Aber gerade die Verarbeitung von Daten in der Cloud erspart sowohl dem Anbieter der Services als auch den Krankenhäusern als Kunden den Betrieb eines eigenen Rechenzentrums mit der erforderlichen Performanz und Redundanz und ermöglicht den Nutzern einen flexibleren Zugriff auf eine professionell betriebene Wirkumgebung. Ein zusätzliches Add-on ist die sichere Archivierung. Gleichzeitig können solche Services vielen Krankenhäusern zur Verfügung gestellt werden, z. B. für die Verbesserung der Patientensicherheit. Durch sehr hohe technische Sicherheitsmaßnahmen (Verschlüsselung, Zwei-Faktor-Authentifizierung beim Zugriff) ist eine Offenbarung wesentlich unwahrscheinlicher, als das im stationären Alltag der Krankenhäuser möglich ist.

Das Risiko einer unbefugten Offenbarung medizinischer Daten durch Nutzung eines Cloud-Dienstes hat sich auch im Rahmen der Forschungen des Trusted-Cloud-Programms als schwer überwindbare Hürde erwiesen. So kann die Gestaltung einer geschlossenen und institutsübergreifenden Prozesskette mit einer medienbruchfreien und durchgängigen Verlaufsdokumentation, wie sie für eine klinikübergreifende stationäre Versorgung von Patienten erforderlich wäre, nicht ohne den standardisierten Austausch medizinischer Daten zwischen stationären und ambulanten Einrichtungen umgesetzt werden. Zwingend benötigt wird ein auf IHE-Konzepten[4] basierender „Master Patient Index“ (MPI), der alle Indices eines Patienten aus verschiedenen Krankenhäusern referenziert und dazu dient, die Informationen aus den verschiedenen Quellen unter einer gemeinsamen Identität zusammenführen zu können. Er prüft Patientendaten auf Übereinstimmung. Dazu müssen sie entschlüsselt sein. Ist der MPI in der Cloud lokalisiert, findet eine Verarbeitung von Patientendaten außerhalb des Krankenhauses statt. Somit ist der Tatbestand der Offenbarung erfüllt bzw. die ärztliche Schweigepflicht gebrochen worden, selbst wenn durch geeignete technische Maßnahmen sichergestellt ist, dass keine andere Person Kenntnis von diesen Daten erlangt, außer diejenige, die vom Krankenhaus beauftragt ist, die Zusammenführung der Daten zu überwachen.

3 AMTS = Arzneimitteltherapiesicherheit.

4 IHE = Integrating the Healthcare Enterprise Initiative.

Es verwundert daher nicht, dass Bundesärztekammer und Kassenärztliche Bundesvereinigung die Nutzung von Cloud-Diensten kritisch sehen und sie nur unter Bedingungen als zulässig erachten, die eine Entwicklung zukunftsorientierter Cloud-Lösungen für das Gesundheitswesen erschweren.

Weitere relevante Felder mit stark wachsendem Bedarf an IT-Unterstützung sind die Entwicklung der individualisierten Medizin und die Erforschung und Behandlung seltener Krankheiten. In der Forschung auf diesen Feldern ist schon heute die Verarbeitung und Zusammenführung großer Mengen medizinischer Daten erforderlich, was die IT-Kapazitäten vieler Krankenhäuser übersteigt. Dabei ist davon auszugehen, dass die heute für die Forschung geltenden Anforderungen an IT-Unterstützung morgen auch den Standard in der Versorgung charakterisieren.

# 5 De lege lata keine rechtssicheren Lösungen möglich

Eine Beauftragung externer Dienstleister ist zwar auch im Hinblick auf die strafbewehrte Schweigepflicht möglich, wenn der Patient, Mandant bzw. Kunde den zur Verschwiegenheit Verpflichteten von seiner Schweigepflicht entbindet. Die Einholung einer Schweigepflichtentbindung ist in der Regel aber nicht praktikabel. So würde bereits die Entscheidung eines einzigen Patienten, der eine solche Entbindung ablehnt, dazu führen, dass der Arzt im Ergebnis für alle seine Patienten auf die Einschaltung eines externen Dienstleisters verzichten muss; denn eine Differenzierung nach einzelnen Patienten ist beispielsweise bei der externen Betreuung oder Wartung eines EDV-Systems nicht möglich. Würde der Arzt den Dienstleister wechseln wollen, müsste er unter Umständen zudem für alle Patienten eine neue Einwilligung hinsichtlich des neuen Dienstleisters einholen. Dies würde beispielsweise bei der externen Archivierung von Unterlagen auch diejenigen Patienten betreffen, deren Behandlung schon Jahre zurückliegt, deren Daten aber wegen entsprechender Aufbewahrungspflichten noch gespeichert sind. Deshalb stellt eine Einwilligung keine ausreichende Lösung dar, um Berufsgeheimnisträgern die Einbeziehung externer Dienstleister rechtssicher zu ermöglichen. Auch wenn in Einzelfällen durch technische und organisatorische Lösungen eine Offenbarung verhindert werden kann, ist eine flächendeckende Lösung dadurch nicht möglich.

Vor diesem Hintergrund werden in der juristischen Beratungspraxis verschiedene Argumente vorgetragen, um den Tatbestand einer unbefugten Offenbarung auszuschließen. So wird beispielsweise versucht, den Begriff des berufsmäßig tätigen Gehilfen, dem Berufsgeheimnisse zulässigerweise offenbart werden dürfen, dahingehend auszuweiten, dass darunter auch externe Dienstleister zu verstehen sind. Ein anderer Ansatz bemüht sich, durch eine Kombination von technischen und organisatorischen Maßnahmen – angelehnt an § 11 BDSG – das mögliche Offenbaren von Berufsgeheimnissen so weit einzuschränken, dass eine Strafbarkeit nach § 203 StGB im Ergebnis zu verneinen wäre. Da jedoch alle bisher entwickelten Argumentationsansätze umstritten sind, schaffen sie den Berufsgeheimnisträgern keine sichere Rechtsgrundlage für den Einsatz externer Dienstleister. Daher verbleibt für Berufsgeheimnisträger stets das Risiko, durch die Einbeziehung externer Dienstleister die Schweigepflicht zu verletzen und daher strafrechtliche Konsequenzen fürchten zu müssen.

# 6 Große Bedeutung für die Praxis

Aus dem Umstand, dass aus der Praxis kaum Strafverfahren zu § 203 StGB wegen des Einsatzes von IT-Dienstleistern bekannt sind, darf nicht der Schluss gezogen werden, dass es sich bei dieser Rechtsunsicherheit um ein rein akademisches Problem handelt, dem in der Praxis keine Bedeutung zukommt.[5] Dass es zu § 203 StGB nur wenig Rechtsprechung gibt, dürfte insbesondere damit zusammenhängen, dass es sich bei diesem Straftatbestand um ein sogenanntes Antragsdelikt handelt, d.h. um ein Delikt, dessen Verfolgung einen Strafantrag des Betroffenen voraussetzt. An einem solchen Strafantrag wird es in der Regel aber fehlen. Denn den Betroffenen wird eine Offenbarung ihrer Geheimnisse oftmals nicht bekannt sein, da sie regelmäßig keinen Einblick in die interne Organisation der Praxis bzw. Kanzlei haben. Andere werden bewusst von einem Strafantrag absehen, da sie weiterhin beabsichtigen, den Arzt oder Rechtsanwalt aufzusuchen, und daher das Vertrauensverhältnis nicht zusätzlich belasten wollen oder weil sie eine außergerichtliche Lösung anstreben. Selbst wenn im Einzelfall ein Strafverfahren eingeleitet werden sollte, kann dies gegebenenfalls trotz eines Strafantrags durch eine Einstellung beendet werden.

Das entscheidende Problem für die Praxis besteht darin, dass wegen des Strafbarkeitsrisikos IT-Projekte unterlassen werden und Effizienzvorteile durch Nutzung von IT-Diensten nicht erzielt werden können. In der Praxis werden im Vorfeld von IT-Projekten häufig Anfragen bei Datenschutzbeauftragten, Kanzleien und Aufsichtsbehörden gestellt, ob das Vorhaben rechtskonform umgesetzt werden kann. Werden die Anfragenden auf die oben geschilderten Schwierigkeiten hingewiesen, nehmen sie nicht selten Abstand von den geplanten Projekten. Dass in solchen Fällen die Umsetzung mangels tragfähiger Strukturen unterbleibt, zeigt, dass noch größerer Bedarf an Regelungen besteht, die eine rechtssichere Lösung solcher Fallgestaltungen erlauben. Auch aus Sicht der Praxis wird demnach die derzeitige Ausgestaltung der Schweigepflicht den komplexen Strukturen der heutigen Arbeitswelt nicht mehr gerecht. Sie ist insbesondere nicht in der Lage, den Schutz des Rechts auf informationelle Selbstbestimmung mit den Erfordernissen der Berufswelt in Einklang zu bringen, und führt zu erheblicher Rechtsunsicherheit für alle Beteiligten.

Diese Problematik verschärft sich durch aktuelle gesetzliche Entwicklungen. So gibt der Gesetzgeber bestimmten Berufsgruppen (z. B. den Rechtsanwälten) über das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013 (BGBl. I S. 3786) die elektronische Kommunikation vor. Dabei fehlt diesen Berufsgruppen die rechtliche Möglichkeit, sich hierzu externe technische Unterstützung zu verschaffen, ohne die Verwirklichung des Tatbestands des § 203 StGB zu riskieren. Für den Bereich des Gesundheitswesens ist der Entwurf für ein E-Health-Gesetz angekündigt, um die Chancen der Telemedizin zu nutzen. Dabei soll eine Telematikstruktur die Beteiligten im Gesundheitswesen so verbinden, dass sie die für die Behandlung wichtigen medizinischen Informationen schnell, sicher und unbürokratisch austauschen können. Wenn Ärzte dabei die technische Hilfe externer Dienstleister benötigen, laufen sie jedoch ebenfalls Gefahr, sich nach § 203 Abs. 1 StGB strafbar zu machen. Die in § 203 StGB genannten Berufsgruppen benötigen deshalb Rechtssicherheit bei der Einbindung externer Kräfte.

5 Als aktuelles Beispiel ist das Urteil des Landgerichts Flensburg vom 05.07.2013 (Az.: 4 O 54/11) zu nennen, in dem das (Zivil-)Gericht die Beauftragung eines externen Dritten mit der Pflege und Wartung der EDV-Anlage einer Arztpraxis als Verstoß gegen die ärztliche Schweigepflicht nach § 203 Abs. 1 StGB angesehen hat.

# 7 Notwendigkeit einer Gesetzesänderung

Vor diesem Hintergrund empfiehlt die AG „Rechtsrahmen des Cloud Computing“, die im Rahmen des Technologieprogramms „Trusted Cloud“ eingerichtet wurde, durch eine Änderung der rechtlichen Rahmenbedingungen die nötige Rechtssicherheit zu schaffen. Denn nur durch eine Gesetzesänderung kann sichergestellt werden, dass Berufsgeheimnisträger, die den Schutz der ihnen anvertrauten Geheimnisse ernst nehmen wollen, sich auch bei der Auslagerung von (IT-)Dienstleistungen gesetzeskonform verhalten können.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit wiederholt auf dieses Problem aufmerksam gemacht. So hat sie zuletzt Ende 2013 an die Regierungen und Parlamente von Bund und Ländern appelliert, für die zunehmende Einschaltung technischer Dienstleister, insbesondere durch Ärzte, angewiesene datenschutzgerechte Regelungen zu verabschieden.

Das Strafbarkeitsrisiko, das Berufsgeheimnisträger derzeit bei der Einschaltung von externen Dienstleistern zwangsläufig eingehen müssen, ist ihnen nicht länger zumutbar. Eine Änderung der rechtlichen Rahmenbedingungen erscheint dabei nicht nur im Hinblick auf die in § 203 StGB und § 353b StGB normierte Strafbarkeit, sondern auch in Bezug auf damit zusammenhängende strafprozessuale Vorschriften wie die Regelungen zum Zeugnisverweigerungsrecht und insbesondere zum Beschlagnahmeverbot erforderlich.

# 8 Potenzielle Lösungsansätze im Rahmen einer Gesetzesänderung

Für eine Gesetzesänderung sieht die AG „Rechtsrahmen des Cloud Computing“ derzeit im Wesentlichen vier Optionen. Diese sollen im Folgenden als Lösungsansätze zur Rechtsgestaltung in Grundzügen dargestellt werden.

## Gesetzliche Änderung des Gehilfenbegriffs

Vorstellbar wäre, externe IT-Dienstleister in den Kreis der Gehilfen im Sinne des § 203 Abs. 3 Satz 2 StGB mit einzubeziehen. Nach § 203 Abs. 3 Satz 2 StGB stehen den Berufsgeheimnisträgern ihre berufsmäßig tätigen Gehilfen gleich. Hieraus wird mehrheitlich der Umkehrschluss gezogen, dass der Berufsgeheimnisträger Geheimnisse an seine Gehilfen (typischerweise etwa seine Praxis- und Kanzleihilfen) weitergeben darf, ohne die Geheimnisse zu offenbaren und sich strafbar zu machen.

Allerdings setzt § 203 Abs. 3 Satz 2 StGB den berufsmäßig tätigen Gehilfen dem Berufsgeheimnisträger in erster Linie insofern gleich, als eine Offenbarung von Geheimnissen durch ihn ebenso strafbar sein soll wie für den Berufsgeheimnisträger. § 203 Abs. 3 Satz 2 StGB ist insofern eine Strafnorm und kein strafrechtlicher Entlastungstatbestand für die Berufsgeheimnisträger.[6] Die Erweiterung des Gehilfenkreises um einen Dienstleister würde z. B. den Cloud-Anbieter ebenfalls einem Strafbarkeitsrisiko aussetzen. Unklar ist, inwieweit eine Erweiterung des Gehilfenkreises den cloudnutzenden Berufsgeheimnisträger von seiner Strafbarkeit befreien würde. Überdies müssten beim Cloud Computing nur deutsche Cloud-Anbieter und nicht die vermutlich viel zahlreicheren ausländischen Cloud-Anbieter eine effektive Strafverfolgung fürchten.

6 Die Einbindung in den Kreis der zum Wissen Berufenen durch die herrschende Meinung ist nur insofern nachvollziehbar, als durch die Strafandrohung gegenüber dem Gehilfen der Schutz für den Betroffenen wohl derart gewährleistet wird, dass von seiner mutmaßlichen Einwilligung ausgegangen werden kann.

## Bezugnahme zur datenschutzrechtlichen Auftragsdatenverarbeitung

In § 203 StGB oder auch im Datenschutzrecht könnte eine Auftragsdatenverarbeitung auch für Berufsgeheimnisse vorgesehen werden, die sich mit § 11 BDSG deckt oder zumindest in den Tatbestandsmerkmalen daran anlehnt. Diskutiert wird deshalb auch eine entsprechende Anwendung des § 11 BDSG auf den Berufsgeheimnisschutz im Strafrecht. Die Weitergabe von Berufsgeheimnissen an einen Dienstleister wäre dann nicht strafbar, wenn dieser unter Weisungs- und Kontrollanforderungen beauftragt wurde, die mit den Vorgaben von § 11 BDSG vergleichbar sind.

Gegen eine solche Lösung können allerdings rechtssystematische Einwände erhoben werden. Eine Regelung im Datenschutzrecht wäre nicht ausreichend. Nach § 1 Abs. 3 Satz 2 BDSG bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, von den Regelungen des Bundesdatenschutzgesetzes „unberührt". Zumindest hinsichtlich konkurrierender Zulässigkeitsfragen verdrängt das strafbewehrte Verbot der Offenbarung von Geheimnissen nach § 203 StGB die Zulässigkeit einer Datenweitergabe nach § 11 BDSG. Das Datenschutzrecht und seine Auftragsdatenverarbeitung einerseits sowie der strafbewehrte Berufsgeheimnisschutz andererseits haben darüber hinaus auch unterschiedliche Schutzrichtungen.

Fraglich ist, ob ein ausdrücklicher Verweis in § 203 StGB auf das Datenschutzrecht, etwa § 11 BDSG, eine geeignete Lösung darstellt. Der Berufsgeheimnisschutz hat, anders als das Datenschutzrecht, nicht die Reglementierung des Umgangs mit jeglichen personenbezogenen Daten im Blick. § 203 StGB schützt vielmehr das besondere Vertrauensverhältnis zwischen dem Berufsgeheimnisträger und dem Betroffenen. In diesem Verhältnis werden Geheimnisse – zum Teil aus faktischem Zwang oder im Vertrauen auf die besondere Qualifikation und Integrität des Berufsgeheimnisträgers – „anvertraut". Der Schutz der Auftragsdatenverarbeitung zielt nicht auf ein solches Vertrauens- und Näheverhältnis, sondern entsprechend § 11 Abs. 2 Satz 1 BDSG auf die Sicherstellung der technischen und organisatorischen Datensicherheit sowie die Möglichkeit zur Weisung und Kontrolle gegenüber der auftragnehmenden Stelle ab. Zudem würde eine spezifisch auf die Auftragsdatenverarbeitung abzielende Lösung nicht die Fälle abdecken, in denen der IT-Dienst auf anderer gesetzlicher Grundlage (z. B. § 28 BDSG, Forschungsklauseln) beruht.

## Erlaubnis in Berufsgesetzen

Durch die Normierung einer Offenbarungsbefugnis in den Berufsordnungen könnte eine folgenlose Offenbarung gegenüber IT-Dienstleistern, ähnlich wie schon in § 49b Abs. 4 BRAO für die Abtretung von Vergütungsforderungen, ermöglicht werden. Eine Offenbarung kann dann auch keine strafrechtlichen Folgen mehr haben, denn was in den Berufsordnungen ausdrücklich erlaubt ist, kann durch § 203 StGB nicht strafrechtlich sanktioniert sein.

Eine solche Regelung ausschließlich in den Berufsordnungen würde jedoch zu einer Zersplitterung der Offenbarungsbefugnisse führen und zumindest solche in § 203 StGB genannten Berufsgeheimnisträger von der Rechtsunsicherheit nicht befreien können, die sich auf keine Berufsordnung oder keine entsprechende Regelung in ihrer Berufsordnung stützen können.

## Konkretisierung des Offenbarungsbegriffs

Eine gesetzliche Neuregelung könnte schließlich eine Konkretisierung des Offenbarungsbegriffs zum Ziel haben. Eine Regelung würde folglich am Tatbestandsmerkmal der „unbefugten Offenbarung fremder Geheimnisse“ aus § 203 Abs. 1 StGB ansetzen.

Hierbei könnte zum einen näher geregelt werden, ob und in welchen Fällen es zu einer strafbaren, da unbefugten Offenbarung kommt. Insbesondere könnte de lege ferenda klargestellt werden, ob und in welchen Fällen eine tatsächliche Kenntnisnahme des Dritten erfolgen muss und wann bereits die Ermöglichung der Kenntnisnahme für eine strafbare Offenbarung genügt. Zum anderen könnte der Offenbarungsbegriff dahingehend konkretisiert werden, dass die Weitergabe von Informationen an externe Dienstleister unter bestimmten, technisch oder rechtlich abstrakt bezeichneten Voraussetzungen noch keine Offenbarung im Sinne des § 203 Abs. 1 StGB darstellt.

Die Schwierigkeit für diesen Ansatz besteht darin, Tatbestand und Voraussetzungen einer privilegierten Weitergabe hinreichend konkret zu beschreiben und gleichwohl alle relevanten Fallgruppen zu erfassen.

# Fazit

Derzeit besteht für Berufsgeheimnisträger bei Einschaltung externer IT-Dienstleister erhebliche Rechtsunsicherheit in Bezug auf eine Strafbarkeit nach § 203 StGB. Sowohl bei traditionellen Dienstleistungen wie IT-Wartung als auch bei neuen Formen wie Cloud Computing existiert für Berufsgeheimnisträger ein erhebliches Strafbarkeitsrisiko. Dies verhindert, dass das Potenzial dieser Dienste ausgeschöpft wird.

Zur Beseitigung des Strafbarkeitsrisikos und der bestehenden Rechtsunsicherheit ist eine Gesetzesänderung erforderlich. Insoweit bestehen unterschiedliche Lösungsansätze, die im Einzelnen diskutiert werden müssen. Insgesamt erscheint es dringend erforderlich, den Gesetzgebungsprozess unverzüglich in Gang zu setzen, um Berufsgeheimnisträgern die rechtssichere Nutzung von IT-Diensten zu ermöglichen.

## Das Thesenpapier zur Schweigepflicht bei der Auslagerung von IT-Dienstleistungen

Das rechtspolitische Thesenpapier „Schweigepflicht bei der Auslagerung von IT-Dienstleistungen“ wurde durch Mitglieder der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ unter der Leitung von Prof. Dr. Georg Borges erarbeitet.

## Mitwirkende/Autoren

**Dr. Thorsten B. Behling,** WTS Rechtsanwaltsgesellschaft mbH

**Prof. Dr. Georg Borges,** Kompetenzzentrum Trusted Cloud

**Mathias Cellarius,** SAP SE

**Dr. Astros Chatziastros,** TMF e.V.

**Dr. Johannes Drepper,** TMF e.V.

**Dr. Alexander Duisberg,** Bird & Bird LLP

**Günther Eble,** Kommunale Informationsverarbeitung Baden-Franken

**Alexander Glaus,** Deutsche Bank AG

**Björn Hajek, LL.M.,** Infineon Technologies AG

**Dr. Marc Hilber, LL.M.,** Oppenhoff & Partner

**Dr. Hubert Jäger,** Uniscon universal identity control GmbH

**Kristian Klodt,** QSC AG

**Rudi Kramer,** DATEV eG

**Thomas Kranig,** Bayerisches Landesamt für Datenschutzaufsicht

**Steffen Kroschwald,** Universität Kassel

**Jan Pohle,** DLA Piper International LLP

**Stephan Sädtler,** Universität Passau

**Gunther Schiefer,** Karlsruher Institut für Technologie

**Gabriel Schulz,** Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

**Karin Vedder,** Bayerisches Landesamt für Datenschutzaufsicht

**Dr. Joseph Walenta,** Deutsches Herzzentrum Berlin

**Magda Wicker,** Universität Kassel

www.bmwi.de