Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zu den Mindeststandards des BSI zur Nutzung und Mitnutzung externer Cloud-Dienste nach § 8 Abs. 1 BSIG

Hinweise zur Umsetzung und Interpretation – Version 1.0 vom 20.06.2018

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Dokument unterstützt IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe) und IT-Betriebspersonal der Interpretation und der Umsetzung der Mindeststandards des BSI zur

- Nutzung externer Cloud-Dienste – Version 1.0 vom 24.04.2017
- Mitnutzung externer Cloud-Dienste – Version 1.0 vom 20.06.2018.

Der Bedarf an sicheren Cloud-Diensten nimmt auch in der Bundesverwaltung stetig zu. Dabei können sich in der Praxis die Anwendungsbereiche stark unterscheiden. In Abhängigkeit vom Schutzbedarf der zu verarbeitenden Daten nimmt dabei auch die Informationssicherheit eine zunehmend zentrale Rolle ein. Die Einforderung und Umsetzung von Sicherheitsanforderungen ist daher ein wichtiger Bestandteil bei der Inanspruchnahme von Cloud-Diensten.

Vor diesem Hintergrund hat das BSI zunächst zwei grundsätzliche Anwendungsbereiche identifiziert und für diese dann in Form von Mindeststandards zielgerichtete Sicherheitsanforderungen veröffentlicht.

Nutzung externer Cloud-Dienste

In dem ersten Anwendungsbereich hat die Bundesbehörde (hier eine Stelle des Bundes im Sinne des § 8 Abs. 1 BSIG) einen Bedarf an einer IT-Leistung, die nicht durch eigene IT-Ressourcen, sondern über einen externen Cloud-Dienst erbracht werden soll. Hierbei handelt es sich letztendlich um eine sogenannte Make-or-Buy-Entscheidung der Bundesbehörde. Sofern sich die Bundesbehörde für die "Buy"-Option entscheidet, schließt diese mit einem Wirtschaftsunternehmen (Cloud-Anbieter) einen Vertrag über die Erbringung der IT-Leistung ab. Die Bundesbehörde nimmt somit die Rolle des Auftraggebers ein. In diesem Anwendungsbereich finden die Regelungen des Mindeststandards des BSI zur Nutzung externer Cloud-Dienste Anwendung. Nach Einschätzung des BSI handelt es sich hierbei um den Regelfall bei der Inanspruchnahme von externen Cloud-Diensten durch Bundesbehörden.

Mitnutzung externer Cloud-Dienste

Der zweite Anwendungsbereich stellt einen Sonderfall dar, in dem IT-Anwender einer Bundesbehörde externe Cloud-Dienste zwar in Anspruch nehmen, jedoch ohne dass zwischen der Bundesbehörde und dem Cloud-Anbieter ein Vertragsverhältnis darüber besteht. Damit ist die Bundesbehörde nicht Auftraggeber des externen Cloud-Dienstes. Dieser Anwendungsbereich nimmt insbesondere in (internationalen) Projekten oder Arbeitsgruppen eine bedeutende Rolle ein. Die Sicherheitsanforderungen zur Nutzung externer Cloud-Dienste würden hier in einigen Bereichen zu weit greifen.

Trotz der unterschiedlichen Anwendungsbereiche haben beide Mindeststandards aber auch einige Gemeinsamkeiten. Diese sind in den Kapiteln 1.1 bis 1.4 dargestellt. Darauf aufbauend sind im weiteren Verlauf die Umsetzungshinweise zur Nutzung (Kapitel 2) und Mitnutzung. (Kapitel 3) externer Cloud-Dienste aufgeführt.

1.1 Abgrenzung von Cloud-Diensten

Für die korrekte Anwendung der Mindeststandards müssen Cloud-Dienste auch als solche klar identifiziert werden können. Oftmals sind die Grenzen zwischen einem Outsourcing von IT-Leistungen und dem Bezug von Cloud-Diensten fließend. Für die Mindeststandards ist die vom BSI festgelegte Definition zu „Cloud Computing“ anzuwenden:

„*Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.*“

Ausführliche Hintergrundinformationen sind dazu auch auf der BSI-Seite "Cloud Computing Grundlagen"[1] zu finden. Im Zweifel unterstützt aber auch das BSI auf Anfrage.

Als „extern“ sind Cloud-Dienste einzustufen, wenn diese von IT-Unternehmen der Wirtschaft angeboten werden. Cloud-Dienste, die von IT-Dienstleistern des Bundes angeboten gehören daher nicht dazu. Unabhängig von der Anwendung der Mindeststandards richten IT-Dienstleister des Bundes ihre IT-Angebote auf die Sicherheitsbedürfnisse der Bundesverwaltung aus.

1.2 Risikoanalyse und Datenkategorisierung

Der Schutz der zu verarbeitenden Daten nimmt in beiden Anwendungsbereichen eine entscheidende Rolle ein. Aus diesem Grund wird eine Risikoanalyse gefordert. Die Ergebnisse sind für das weitere Beschaffungs- und Einsatzverfahren maßgeblich. Für den Mindeststandard gilt daher, dass die Risikoanalyse nach BSI-Standard 200-3 (Übergangsweise auch 100-3) zu erfolgen hat. Die ermittelten Risiken für die Daten müssen betrachtet und bewertet werden. Für die Risikoanalyse sind insbesondere die aktuellen Veröffentlichungen des BSI zur Cloud-Sicherheit heranzuziehen. Um identifizierten Risiken entgegenwirken, können auch zusätzliche Maßnahmen auf Seite der Behörde erforderlich sein.

Ein weiterer wesentlicher Punkt ist die Bestimmung der zu verarbeitenden Daten. So ist die Einforderung von Sicherheitsanforderungen insbesondere abhängig von den Daten, die in der externen Cloud verarbeitet werden sollen. Aus diesem Grund führen beide Mindeststandards eine Datenkategorisierung ein. In diesem Zusammenhang wird ein Schema eingeführt, anhand dessen die Behörden die Ableitung notwendiger Sicherheitsanforderungen ermitteln können. In der nachfolgenden Tabelle sind die Datenkategorien mit Beschreibungen und Erläuterungen aufgeführt:

Daten-kategorie	Beschreibung	Erläuterung
Kategorie 1	Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB	Hierunter fallen alle Daten, die durch das Strafgesetzbuch besonders geschützt sind. Aus diesem Grund ergeben sich auch erhöhte Sicherheitsanforderungen an die Verarbeitung in einer externen Cloud. Hier reicht in der Regel nur die Umsetzung der Basisanforderungen des Anforderungskatalogs Cloud Computing (kurz C5)[2] durch den Cloud-Anbieter nicht aus. In diesem Zusammenhang ist daher zunächst zu prüfen, ob mit der Umsetzung der optionalen weitergehenden Anforderungen des C5 die Risiken ausreichend abgedeckt sind.
Kategorie 2	personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO (vormals § 3 Absatz 1 BDSG)	Nach der Datenschutz-Grundverordnung (DSGVO) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (zur weiteren Konkretisierung siehe Artikel 4 DSGVO). Für den Schutz personenbezogener Daten ergeben sich daher ebenfalls erhöhte Sicherheitsanforderungen. Es ist daher zu prüfen, welche optionalen weitergehenden Anforderungen des C5 der Cloud-Anbieter zusätzlich umzusetzen hat. Es wird empfohlen in diesem Zusammenhang die

[1] Siehe https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html und hier insbesondere der Bereich „Was unterscheidet Cloud Computing von klassischem IT-Outsourcing?“

[2] Siehe https://www.bsi.bund.de/C5

		behördlichen Datenschutzbeauftragten einzubinden.
Kategorie 3	Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)	Hierunter fallen Daten die nach der VSA eingestuft sind (VS - Nur für den Dienstgebrauch, VS - Vertraulich, Geheim, Streng Geheim). Es wird empfohlen in diesem Zusammenhang die zuständigen Geheimschutzbeauftragten einzubinden.
Kategorie 4	sonstige Daten	Kategorie 4 ist eine sogenannte "Auffangkategorie". Hierunter sind alle Daten zu fassen, die nicht den Kategorien 1, 2 oder 3 zu zuordnen sind. Hierbei handelt es sich dann im Regelfall um Daten für die eine Umsetzung der Basisanforderungen nach C5 ausreichend ist.

Tabelle 1: Datenkategorisierung mit Erläuterungen

1.3 Informationsaustausch

Für beide Mindeststandards gibt es einen "Informationsaustausch". Hinweise und häufig gestellte Fragen sind auf der BSI-Seite https://www.bsi.bund.de/mindeststandards (unter „Informationsaustausch“) eingestellt.

1.4 Praxisbeispiele

Als Hilfestellung sind nachfolgend sechs unterschiedliche Praxisbeispiele aufgeführt. In der Spalte „Mindeststandard“ wird aufgeführt, ob und welcher Mindeststandard auf dieses Praxisbeispiel anzuwenden ist. Die Begründung soll so eine korrekte Anwendung der beiden Mindeststandards in der Praxis unterstützen.

Praxisbeispiel	**Mindest-standard**	**Begründung**
Eine Bundesbehörde hat sich gegen den Eigenbetrieb einer CRM-Software entschieden. Sie bezieht diese IT-Leistung als Cloud-Dienst über ein externes Wirtschaftsunternehmen. Mithilfe dieser Software verwaltet die Bundesbehörde u. a. Adressdaten von Außenkontakten.	Nutzung externer Cloud-Dienste	Die Bundesbehörde hat mit dem Cloud-Anbieter einen Vertrag geschlossen und ist damit Auftraggeber des externen Cloud-Dienstes. Eine Verarbeitung von dienstlichen Daten erfolgt zumindest im Rahmen der Adressdatenverwaltung. Diese sind der Datenkategorie 2 - personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO - zuzuordnen (siehe Kapitel 1.2).
Das IT-Referat einer Bundesbehörde bezieht skalierbaren Datenspeicher über einen externen Cloud-Anbieter. Der Datenspeicher wird genutzt, um kurzfristig auch große Datenmengen nicht eingestufter Informationen mit externen Partnern teilen zu können.	Nutzung externer Cloud-Dienste	Auftraggeber ist das IT-Referat und somit die Bundesbehörde. Diese hat mit dem Cloud-Anbieter einen Vertrag geschlossen. Es ist zu klären, welche Daten künftig über den externen Cloud-Dienst verarbeitet werden dürfen (siehe Kapitel 1.2).
IT-Anwender eines Fachreferates sind eingeladen im Rahmen einer internationalen Arbeitsgruppe für den	Mitnutzung externer Cloud-	Auftraggeber des externen Cloud-Dienstes ist die europäische Institution. Die Bundesbehörde hat keinen Einfluss auf die

Austausch von Dokumenten eine Webplattform zu nutzen. Dieser Cloud-Dienst wird im Auftrag einer europäischen Institution von einem externen Cloud-Anbieter betrieben. Die IT-Anwender laden in diesem Zusammenhang Dokumente auf ihre dienstlichen Arbeitsplatzrechner herunter, bearbeiten diese dort mit einem Textverarbeitungsprogramm und stellen die neuen Versionen in den externen Cloud-Dienst ein. Weiterhin nutzen sie die Möglichkeit, an virtuellen Diskussionen teilzunehmen.	Dienste	Verträge und damit auch nicht auf Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Die Bundesbehörde muss daher bewerten, ob die eigenen Daten künftig in diesem externen Cloud-Dienst verarbeitet werden dürfen. Hierzu sind die Daten zunächst auf Basis der Datenkategorisierung zu bewerten. Zusammen mit den Ergebnissen aus der Risikoanalyse erfolgt nun ein Abgleich mit dem vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2 des Mindeststandards. Danach erfolgt eine bewusste Entscheidung für oder gegen die Mitnutzung des externen Cloud-Dienstes.
Im Rahmen eines Forschungsprojektes arbeiten IT-Anwender aus einem Fachreferat einer Bundesbehörde mit einer internationalen Universität zusammen. Der dortige Lehrstuhl hat zur Berechnung komplexer geometrischer Forschungsdaten einen leistungsstarken virtuellen Server gemietet. Dieser wird von einem Wirtschaftsunternehmen in einer externen Cloud betrieben. Die IT-Anwender des Fachreferates können über einen Remote-Fernzugriff auf den virtuellen Server zugreifen und so die hohe Rechenleistung des virtuellen Servers nutzen. In diesem Zusammenhang werden auch wissenschaftliche Daten der Bundesbehörde verarbeitet.	Mitnutzung externer Cloud-Dienste	Auftraggeber ist der Lehrstuhl der internationalen Universität. Die Bundesbehörde hat keinen Einfluss auf die Verträge und damit auch nicht auf die Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Auch hier muss die Bundesbehörde zunächst bewerten, ob die wissenschaftlichen Daten künftig in diesem externen Cloud-Dienst verarbeitet werden dürfen. Hierzu sind die eigenen wissenschaftlichen Daten zunächst auf Basis der Datenkategorisierung zu bewerten. Zusammen mit den Ergebnissen aus der Risikoanalyse erfolgt nun ein Abgleich mit dem vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2 des Mindeststandards. Danach erfolgt eine bewusste Entscheidung für oder gegen die Mitnutzung des externen Cloud-Dienstes.
IT-Anwender der behördeneigenen Bibliothek greifen für Literaturrecherchen auch auf externe Datenbanken zu. Die Datenbanken werden als Webdienst angeboten und ausschließlich mit Inhalten und Daten des externen Anbieters befüllt. Der Dienst steht als lizenzpflichtiger Service zur Verfügung.	-	Auf dem ersten Blick scheinen alle Voraussetzungen für die Anwendung des Mindeststandards zur Nutzung externer Cloud-Dienste erfüllt zu sein. So handelt es sich vermutlich um einen externen Cloud-Dienst, den die Bundesbehörde als Auftragnehmer nutzt. Jedoch zielen beide Mindeststandards insbesondere darauf ab, für die Verarbeitung von (dienstlichen) Daten entsprechende Sicherheitsanforderungen zu setzen. Die Verarbeitung von diesen besonders schützenswerten Daten (siehe Kapitel 1.2) erfolgt aber bei sogenannten Such- und Recherchediensten oder auch Webdiensten mit Registrierungszwang grundsätzlich nicht. Die Prüfung und Umsetzung der Sicherheitsanforderungen aus den beiden

		Mindeststandards würde in diesen Fällen zu weit greifen. Unabhängig davon sind solche Dienste trotzdem hinsichtlich ihrer Anforderungen zur Informationssicherheit zu überprüfen und zu bewerten. Sie sind jedoch nicht Regelungsgegenstand dieser beiden Mindeststandards.
Das IT-Referat einer Bundesbehörde bezieht für ein Webprojekt einen Cloud-Dienst über das Informationstechnikzentrum Bund (ITZ Bund). Über die Nutzung des Cloud-Dienstes wurde ein entsprechendes Service-Level-Agreement (SLA) abgeschlossen.	-	Zwar ist die Bundesbehörde hier in der Rolle des Auftraggebers, jedoch handelt es sich beim ITZ Bund nicht um ein Unternehmen aus der IT-Wirtschaft. Cloud-Angebote der IT-Dienstleister des Bundes sind daher nicht externe Cloud-Dienste im Sinne der Mindeststandards zur Nutzung und Mitnutzung externer Cloud-Dienste (siehe Kapitel 1.1). Die beiden Mindeststandards finden in diesen Fällen daher keine Anwendung.

Tabelle 2: Praxisbeispiele mit Zuordnungen und Begründungen

2 Umsetzungshinweise zur Nutzung externer Cloud-Dienste

Der Mindeststandard führt einen Prozess ein, mit dem sich Risiken der externen Cloud-Nutzung zuverlässig identifizieren, bewerten und behandeln lassen. Damit bleiben diese für die Behörde als Cloud-Kunde beherrschbar. Hierfür werden die Phasen Beschaffung, Einsatz und Beendigung von externen Cloud-Diensten betrachtet. Für jede Phase werden entsprechende Sicherheitsanforderungen zur Gewährleistung der Informationssicherheit aufgestellt.

Die Sicherheitsanforderungen sind bereits in existierenden Standards, Normen und Regelungen als relevant identifiziert worden und sind daher den Cloud-Anbietern bereits bekannt. Eine ganz zentrale Bedeutung bei der Bewertung von externen Cloud-Diensten nimmt der Anforderungskatalog Cloud Computing (kurz: C5) ein. Dieser adressiert vorrangig Cloud-Anbieter und definiert Basisanforderungen für die Informationssicherheit, die aus Sicht des BSI nicht unterschritten werden sollten. Die Kompatibilität der Basisanforderungen zu international anerkannten Standards stellt dabei die Akzeptanz und Praktikabilität der Umsetzung und Einhaltung auf Seiten der Cloud-Anbieter sicher.

Zentrale Forderung des Mindeststandards ist es daher, dass Bundesbehörden bei einer Nutzung von externen Cloud-Diensten von ihren externen Cloud-Anbietern mindestens die Umsetzung der Basisanforderungen des C5 fordern.

Neben Basisanforderungen an die Informationssicherheit von Cloud-Diensten sind jedoch auch Rahmenbedingungen, unter denen der Cloud-Dienst erbracht wird, für die sichere Nutzung relevant. Bei der Entscheidung, einen Cloud-Dienst zu nutzen, benötigt die Bundesbehörde Transparenz über die Rahmenbedingungen. Durch diese Transparenz wird die Bundesbehörde erst in die Lage versetzt, ein Cloud-Angebot hinsichtlich seiner eigenen Anforderungen an die Informationssicherheit beurteilen zu können. Diesen Ansatz verfolgt der C5 mit den sogenannten Umfeldparametern. Diese Transparenzanforderungen erfragen relevante Angaben über die Diensterbringung, wie z. B. die Lokation der Daten oder welche Funktionen an Unterauftragnehmer ausgelagert sind.

Ob die vom Cloud-Anbieter getroffenen Maßnahmen zur Umsetzung der Basisanforderungen angemessen und wirksam sind, wird im Rahmen von transparenten Prüfungen durch ein Prüfteam mindestens jährlich validiert.[3] Der C5 stellt für seine Prüfung Anforderungen an Prüfteam, Audit und Prüfbericht. So wie die Anforderungen an die Informationssicherheit basieren auch die Anforderungen an Prüfteam, Audit und Prüfbericht auf etablierten internationalen Prüfungsstandards.[4]

Dieser Mindeststandard greift die Themenkomplexe Informationssicherheit, Transparenz der Cloud-Diensterbringung und Nachweis über diese Aspekte durch geeignete Prüfungen auf. Rahmenbedingungen für die Cloud-Diensterbringung werden konkretisiert. Zudem wird vorgegeben, wie die Prüfnachweise des Cloud-Anbieters für das Informationssicherheitsmanagement der jeweiligen Bundesbehörde genutzt werden sollen. Daneben bleibt die Verantwortung für die IT-Objekte, die die Bundesbehörde im Rahmen ihrer IT-Grundschutzkonzeption innehat, unberührt und wird durch die Nutzung externer Cloud-Dienste lediglich angepasst.

Nachfolgend sind die Sicherheitsanforderungen mit entsprechenden Umsetzungshinweisen nach den Phasen Beschaffung (Kapitel 2.1), Einsatz (Kapitel 2.2) und Beendigung (Kapitel 2.3) dargestellt.

[3] Die Prüfung beauftragt der jeweilige Cloud-Anbieter. Dieser kann dann den Prüfbericht seinen Kunden zur Verfügung stellen.

[4] Siehe hierzu auch https://www.bsi.bund.de/c5

2.1 Sicherheitsanforderungen "Beschaffungsphase"

Die Sicherheitsanforderungen an die Beschaffungsphase teilen sich auf in Anforderungen an die Leistungsbeschreibung bzw. Ausschreibungsphase (CD.01 bis CD.03), sowie an den eigentlichen Vertragsabschluss (CD.04 bis CD.13).

CD.01: Systembeschreibung und weitergehende Informationen fordern

*„Die Vorlage der Systembeschreibung **(1)** des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. Sie muss die Vorgaben **(2)** nach C5 erfüllen und ist insbesondere auf Mitwirkungspflichten **(3)** und Maßnahmen hin zu prüfen. Zur Beurteilung des Cloud-Anbieters können weitergehende Informationen im Rahmen der Leistungsbeschreibung gefordert werden. Zudem sind mit Hilfe der Leistungsbeschreibung Basis- und Zusatzleistungen **(4)** festzulegen."*

Anforderung CD.01 adressiert die Leistungsbeschreibung, die bereits in der Startphase einer Beschaffung oder Ausschreibung benötigt wird.

Zu (1): Die Systembeschreibung ist nach C5 die Beschreibung des die Cloud-Dienste betreffenden internen Kontrollsystems. Die Verantwortung für die Systembeschreibung und deren Inhalt liegt bei den gesetzlichen Vertretern des Cloud-Anbieters. Durch Erklärung des Managements werden Angemessenheit und in der Regel auch Wirksamkeit des internen Kontrollsystems bestätigt. Hierbei eingeschlossen sind auch die Prozesse und Verfahren zur Einrichtung und Durchführung der dargestellten Kontrollen.

Zu (2): Der Mindestumfang der Systembeschreibung ergibt sich in sinngemäßer Anwendung des ISAE 3402 (oder des/der alternativ herangezogenen Standards, vgl. C5, Abschnitt 3.2). Exemplarisch benennt der C5 folgende Bestandteile:

- Art und Umfang der erbrachten Cloud-Dienste,
- Grundsätze, Verfahren und Maßnahmen zur Erbringung (Entwicklung und/oder Betrieb) des Cloud-Dienstes, einschließlich der eingerichteten Kontrollen,
- Beschreibung der eingesetzten Infrastruktur-, Netzwerk- und Systemkomponenten für Entwicklung und Betrieb des Cloud-Dienstes, einschließlich der geographischen Lage der Datenverarbeitung und Speicherung,
- Regelung des Umgangs mit bedeutsamen Vorkommnissen und Verhältnissen, die Ausnahmen vom Regelbetrieb darstellen, wie beispielsweise der Ausfall kritischer IT-Systeme,
- Rollen und Zuständigkeiten des Cloud-Anbieters und des Cloud-Kunden, einschließlich Mitwirkungspflichten und erforderlicher korrespondierender Kontrollen beim Cloud-Kunden,
- an Unterauftragnehmer vergebene oder ausgelagerte Funktionen.

Zu (3): Mitwirkungspflichten nehmen bei Cloud-Diensten eine wichtige Rolle ein. Daher muss die Bundesbehörde diese kennen. Die Anforderung soll daher entsprechend sensibilisieren.

Zu (4): Basis- und Zusatzleistungen müssen klar ersichtlich sein. Der Bundesbehörde muss dargestellt werden welche Leistungen der Vertrag umfasst und welche Kosten dafür entstehen.

CD.02: Zertifizierungen oder Bescheinigungen unabhängiger Dritter festlegen

*„In der Leistungsbeschreibung muss festgelegt werden, welche Nachweise (z. B. Zertifizierungen und Prüfberichte) unabhängiger Dritter zur Beurteilung des Cloud-Dienstes erforderlich sind. Hierbei müssen die Ergebnisse der Datenkategorisierung **(1)** und Risikoanalyse **(2)** entsprechend berücksichtigt werden."*

Die Bundesbehörde hat vor der Inanspruchnahme des Cloud-Dienstes eine Datenkategorisierung und Risikoanalyse durchzuführen (siehe Kapitel 1.2). Werden dabei Risiken identifiziert, die nicht über die Basisanforderungen des C5 abgedeckt werden können, ist festzulegen, mithilfe welcher weitergehenden Anforderungen des C5 diesen wirksam entgegengewirkt werden können. Es können auch zusätzliche Nachweise eingefordert werden. Diese sind von der Bundesbehörde festzulegen und zu dokumentieren, so dass sie bereits in der Leistungsbeschreibung als Anforderung an den Cloud-Anbieter erfasst sind.

Werden alle identifizierten Risiken bereits mit der Umsetzung der Basisanforderungen ausreichend abgedeckt, müssen nicht zwingend weitere Zertifikate oder Nachweise gefordert werden. Die Anforderung CD.02 gilt dann bereits als erfüllt.

CD.03: Systembeschreibung und weitergehende Informationen auswerten

„Die Systembeschreibung und die weitergehenden Informationen müssen hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität und nachteiliger Regelungen ausgewertet werden. Die Leistungsbeschreibung muss bereits genau definieren, welche Angaben vom Bieter erwartet werden. Sofern die durch den Bieter vorgelegten Unterlagen Unklarheiten enthalten, muss geprüft werden, ob diese im Rahmen der Aufklärung aufzulösen sind oder zu Lasten des Bieters gehen."

Die Bundesbehörde hat die Ergebnisse und Angebote der Ausschreibung zu bewerten. Hierbei sind insbesondere die mit CD.01 geforderte Systembeschreibung, sowie - optional - die mit CD.02 geforderten weitergehenden Anforderungen und / oder zusätzlichen Nachweise auszuwerten.

CD.04: Sicherheitsnachweise vertraglich zusichern

*„Der Cloud-Anbieter muss regelmäßig Sicherheitsnachweise über die angemessene und wirksame Umsetzung der Basisanforderungen nach C5 **(1)**, die aktuelle Dokumentation der Systembeschreibung **(2)**, die Aktualität von vertraglich zugesicherten Zertifizierungen **(3)** sowie die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen **(4)** vorlegen.*

*Diese Sicherheitsnachweise sollten durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes **(5)** nach C5 erbracht werden. Andere Nachweise **(6)** bedürfen der begründeten Einzelfallentscheidung. Prüfberichte und Nachweise dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. Die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Anbieter ist vertraglich zuzusichern **(7)**."*

Diese Anforderung stellt sicher, dass die festgelegten Anforderungen nach CD.01 auch vertraglicher Bestandteil werden.

Zu (1): Die Basisanforderungen sind im C5 festgelegt. Sie bestehen aus 114 Anforderungen, die sich in 17 Themengebiete gliedern. Damit setzen sie die untere Schwelle der Informationssicherheit, die aus Sicht des BSI nicht unterschritten werden sollte.

Zu (2): Systembeschreibung siehe Sicherheitsanforderung CD.01.

Zu (3): gemeint sind damit insbesondere die optionalen Nachweise nach Sicherheitsanforderung CD.02.

Zu (4): Damit wird sichergestellt, dass Datensicherungskonzepte in der Praxis regelmäßig getestet und erprobt sind.

Zu (5): Der C5 gibt hinsichtlich Prüfung und Berichterstattung entsprechende Regelungen vor (siehe C5, Kap. 3.2 - 3.4). Der Prüfbericht muss der Bundesbehörde zugänglich gemacht werden, damit diese die Umsetzung prüfen kann.

Zu (6): andere Nachweise: Verfügt ein Cloud- Anbieter über kein Testat oder kann dieser keinen Prüfbericht nach C5 vorlegen, können auch andere Nachweise genutzt werden, um die Umsetzung der geforderten Sicherheitsanforderungen nachzuweisen. Diese Ausnahmen sind aber besonders zu begründen. Die Gleichwertigkeit ist durch den Cloud-Anbieter nachzuweisen. Das BSI berät auch hier auf Anfrage.

Zu (7): In diesem Zusammenhang soll geregelt werden, was nicht durch den Prüfbericht abgedeckt werden kann. Dies können z. B. zusätzlich geforderte regelmäßige Penetrationstests durch externe Sicherheitsanbieter sein. Diese Regelungen sind optional und auf den Anwendungsfall abzustimmen.

CD.05: Zusätzliche Anforderungen vertraglich zusichern

„Ermittelte Gefährdungen bzw. Risiken, die nicht bereits durch Basisanforderungen nach C5 abgedeckt sind, müssen über zusätzliche Anforderungen abgedeckt werden. Für die zusätzlichen Anforderungen ist zu vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden. Die Stelle des Bundes hat zu prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen sind einzuhalten und werden im Übrigen durch diesen Mindeststandard nicht berührt."

Hierdurch wird sichergestellt, dass die mit CD.02 ggfls. festgelegten zusätzlichen Zertifikate oder Bescheinigungen unabhängiger Dritter auch vertraglicher Bestandteil werden. Die Benennung basiert daher auf den Ergebnissen der Risikoanalyse und Datenkategorisierung und ist damit optional.

CD.06: Recht auf Prüfungen und Kontrollen vertraglich zusichern

*„Grundsätzlich müssen der Stelle des Bundes eigene Prüfrechte **(1)** vertraglich zugesichert werden. Es ist darauf zu achten, dass die Prüfrechte so ausgestaltet sind, dass die Stelle des Bundes ihre gesetzlichen Anforderungen erfüllt. Im Übrigen sind die Prüfrechte so auszugestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Stelle des Bundes selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.*

*Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse kann in begründeten Ausnahmefällen auf eigene Prüfrechte verzichtet werden, soweit Rechtsvorschriften nicht entgegenstehen. Diese Entscheidung ist unter Risikogesichtspunkten zu treffen und zu dokumentieren. Sofern der Cloud-Anbieter keinen Prüfbericht **(2)** nach C5 vorlegen kann, muss die Stelle des Bundes dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können."*

Zu (1): Prüfrechte nehmen bei der Inanspruchnahme von Cloud-Diensten eine wichtige Funktion ein. Sie sind insbesondere dann relevant, wenn Daten der Kategorien 1 oder 3 in der Cloud verarbeitet werden sollen. Die vertraglich zugesicherten Prüfrechte nimmt die Bundesbehörde insbesondere dann wahr, wenn Zweifel an der korrekten Umsetzung der vereinbarten Sicherheitsanforderungen bestehen. Mit der Prüfung kann die Bundesbehörde auch einen Dritten - z. B. ein Wirtschaftsprüfungsunternehmen, das Testierungen nach C5 vornimmt - beauftragen. Das Ergebnis der Überprüfung ist zu dokumentieren.

Auf den Anwendungsfall bezogen ist zu bewerten, ob eigene Prüfrechte erforderlich sind und wie diese auszugestalten sind. In begründeten Ausnahmefällen kann auf eigene Prüfrechte verzichtet werden.

Zu (2): Kann der Cloud-Anbieter den geforderten Prüfbericht nach C5 oder gleichwertige Nachweise nicht vorlegen (siehe CD.04), soll dies nicht zwingend zu einem Ausschluss des Anbieters führen. Daher wird hier die Möglichkeit geschaffen, die Prüfung durch die Bundesbehörde beauftragen zu lassen.

CD.07: Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

*„Die Beteiligung von Unterauftragnehmern und anderen externen Dritten **(1)** müssen vom Cloud-Anbieter vollständig in Art und Umfang benannt werden. Beabsichtigte Änderungen **(2)** hierüber müssen unverzüglich schriftlich oder per E-Mail mitgeteilt werden. Diese Mitteilungen können auch über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).*

*Falls Unterauftragnehmer nicht nur unwesentliche Teile **(3)** zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, muss der Cloud-Anbieter zusichern,*

- *dass Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und*
- *dass zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen."*

Zu (1): Werden vom Cloud-Anbieter Unterauftragnehmer zur Erbringung von Leistungen eingesetzt, sind diese zu benennen. Liegt ein Prüfbericht nach C5 vor sind diese Informationen in der Systembeschreibung aufgeführt (siehe CD.01).

Zu (2): Da Cloud-Angebote in der Regel flexibel gestaltet sind, können sich während der Vertragslaufzeit Änderungen bei der Einbindung von Unterauftragnehmern ergeben. Darüber ist die Bundesbehörde als Vertragspartner unverzüglich zu informieren. In der Regel bieten Cloud-Anbieter hierfür Informationsportale an. Es ist zu klären, wie die Bundesbehörde informiert wird. Insbesondere ob diese auch aktiv vom Cloud-Anbieter auf Änderungen hingewiesen wird (z. B. durch E-Mails)

Zu (3): Wesentliche Teile des Cloud-Dienstes müssen bestimmt werden. Wesentlich sind Teilleistungen insbesondere dann, wenn ohne diese ein Anbieten des Cloud-Dienstes nicht möglich wäre (z. B. Rechenzentrumsbetrieb).Werden diese von Unterauftragnehmern wahrgenommen, müssen diese vom Cloud-Anbieter nicht nur benannt werden, sondern die vertraglich festgelegten Sicherheitsanforderungen erfüllen. Weiterhin ist zu prüfen, ob zugesicherte Prüfrechte (siehe CD.06) auch auf diese Unterauftragnehmer auszuweiten sind.

CD.08: Gerichtsbarkeit vertraglich zusichern

„Zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit und soweit rechtlich möglich, müssen Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren erfolgen. Es ist zu gewährleisten, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz keine Zeitverluste eintreten, zum Beispiel durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten, so dass die Stelle des Bundes handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann."

Vor dem Hintergrund des jeweiligen Anwendungsfalles ist zu prüfen, welche Bedeutung ein Gerichtsstand außerhalb von Deutschland hätte. Hierbei ist insbesondere zu bewerten, inwiefern Durchsetzungsrechte oder Eilrechtsschutz von Bedeutung sind. Gleiches gilt für das anzuwendende Recht.

Liegt ein Prüfbericht nach C5 vor, können diese Angaben dem Umfeldparameter "UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

Eine Bewertung des anwendbaren Rechts könnte aufgeteilt nach Regionen erfolgen:

- Deutsches Recht,
- Recht eines EU-Mitgliedstaates,
- Recht eines Nicht-EU-Mitgliedstaates

Kommt es zu einer gerichtlichen Auseinandersetzung nimmt der Gerichtsstand eine wichtige Rolle ein. Vor diesem Hintergrund könnte die Zuordnung des Gerichtsstandes nach Regionen erfolgen:

- "innerhalb Deutschlands",
- "innerhalb der EU",
- "außerhalb der EU"

CD.09: Lokation vertraglich zusichern

*„Sämtliche Lokationen **(1)**, an denen Daten verarbeitet werden, sind vertraglich festzulegen. Ob die Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen, ist auf Basis der Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) zu bewerten.“*

Zu (1): Die Bundesbehörde muss vor dem Hintergrund des Anwendungsfalles entscheiden, welche Lokationen für die Verarbeitung der Daten akzeptiert werden können. Dies bezieht Backup-Daten, Rechnungs- und Metadaten ein. Auch eine mögliche Verarbeitung von Daten durch Unterauftragnehmer ist zu berücksichtigen. Für die Bewertung können die Zonen

- "Deutschland",
- "innerhalb der EU" und
- "außerhalb der EU"

genutzt werden.

Liegt ein Prüfbericht nach C5 vor, können Angaben zu Datenlokationen des Cloud-Anbieters den Angaben zum Umfeldparameter "UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden. Alternativ können dazu auch Informationen in den Verträgen oder Dienstegütevereinbarungen (Service Level Agreement) stehen.

CD.10: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

*„Der Cloud-Anbieter muss zusichern, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse **(1)** gelangen. Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen.“*

Zu (1): Der Umgang mit Offenbarungspflichten und Ermittlungsbefugnissen ist für Bundesbehörden durch das Bundesministerium des Innern bereits geregelt. Siehe hierzu Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014. CD.10 nimmt Bezug darauf.

Liegt ein Prüfbericht nach C5 vor, können diese Informationen den Angaben zum Umfeldparameter "UP-03 Offenbarungs- und Ermittlungsbefugnisse" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

Eine Zuordnung könnte nach Regionen vorgenommen werden:

- Deutschland
- EU-Mitgliedsstaat
- Nicht EU-Mitgliedsstaat

CD.11: weitere rechtliche Vereinbarungen vertraglich zusichern

*„Pflichten des Cloud-Anbieters sicherheitsrelevante Vorfälle **(1)** (sowie ggf. andere Vorfälle) gegenüber der Stelle des Bundes zu melden, müssen vertraglich geregelt sein. Vertragsstrafen und Haftungsfragen **(2)** müssen in einem angemessen Verhältnis zum ermittelten Schutzbedarf stehen. Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Vertragsstrafen sollten im Regelfall 5% des Auftragsvolumens nicht unterschreiten."*

Zu (1): Sicherheitsrelevante Vorfälle gefährden im Regelfall die Informationssicherheit des Cloud-Dienstes und damit auch die Daten der Bundesbehörde. Um das Risiko für die eigenen Daten einschätzen zu können sind sicherheitsrelevante Vorfälle der Bundesbehörde gegenüber zu melden. Hierbei sollten Fristen und Meldewege vertraglich zugesichert werden.

Zu (2): Vertragsstrafen und Haftungsfragen sind durch entsprechende Regelungen festzulegen. Hierbei ist die Kritikalität des Cloud-Dienstes für die Bundesbehörde zu berücksichtigen (Risikoanalyse, Datenkategorisierung). Die Sicherheitsanforderung gibt weiterhin mit 5% des Auftragsvolumens eine Empfehlung ab.

CD.12: Beendigung des Vertragsverhältnisses regeln

*„Kündigungsfristen **(1)** müssen dem Einsatzszenario angemessen sein. Soweit rechtlich möglich, müssen kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Stelle des Bundes ausgeschlossen werden."*

Zu (1): Kündigungsfristen sind unter Beachtung des Anwendungsfalles und insbesondere unter Berücksichtigung der Ergebnisse aus Risikoanalyse und Datenkategorisierung zu vereinbaren. Daher sind diese durch die Bundesbehörde für den jeweiligen Anwendungsfall zu ermitteln und festzulegen. Dabei gilt: je "kritischer" ein Cloud-Dienst für die Bundesbehörde ist, desto länger sollten Kündigungsfristen seitens des Cloud-Anbieters ausgestaltet sein.

CD.13: Datenrückgabe und Datenlöschung beim Cloud-Anbieter vertraglich zusichern

„Die Rückgabe der Daten muss geregelt werden (Format, Datenträger, Protokolle usw.). Maßnahmen zur Datenlöschung müssen dem ermittelten Schutzbedarf entsprechen."

Die Bundesbehörde muss Regelungen zur Datenrückgabe festlegen. Dies beinhaltet u.a. Format, Datenträger, Protokolle und die Dokumentation der Übergabe muss definiert werden. Hierbei sind insbesondere die Ergebnisse der Datenkategorisierung zu berücksichtigen, so dass eine Datenrückgabe nicht unbedingt zwingend sein muss. Für die Festlegung der Maßnahmen zur Datenlöschung und ggf. Datenmigration ist analog zu verfahren. Die hier festgelegten Regelungen sind für die Sicherheitsanforderungen CD.19 und CD.20 relevant (siehe Kapitel 2.3).

2.2 Sicherheitsanforderungen "Einsatzphase"

CD.14: ISMS einbinden

„Die Stelle des Bundes muss den externen Cloud-Dienst in ihr eigenes ISMS einbinden. Sind durch die externe Cloud-Nutzung bei der Stelle des Bundes eigene Maßnahmen erforderlich, müssen diese umgesetzt werden."

Die Bundesbehörde hat zu prüfen und festzulegen, wie der externe Cloud-Dienst in das eigene ISMS eingebunden werden kann. Schnittstellen sind zu identifizieren und zu dokumentieren. Insbesondere ist zu prüfen, wie Mitteilungen des Cloud-Anbieters über Änderungen bei Unterauftragnehmern (siehe CD.07) oder Meldungen von sicherheitsrelevanten Vorfällen (siehe CD.11) in das ISMS der Bundesbehörde eingebunden werden können. Ziel sollte dabei sein, dass eine Verarbeitung der Informationen ohne Zeitverlust durch die zuständigen Verantwortlichen erfolgt.

CD.15: Sicherheitsnachweise prüfen

„Die Stelle des Bundes muss die Sicherheitsnachweise und sonstige Berichte des Cloud-Anbieters auswerten. Diese dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. Ergeben sich aus der Auswertung Unklarheiten, muss diesen nachgegangen werden. Sofern erforderlich, sind die zugesicherten Prüf- und Kontrollrechte wahrzunehmen."

Ist der Cloud-Anbieter vertraglich verpflichtet Nachweise zu erbringen (siehe CD.04 und CD.05) muss die Bundesbehörde festlegen, wie diese intern geprüft und ausgewertet werden können. Bei der Prüfung ist insbesondere darauf zu achten, dass die vorgelegten Nachweise den gesamten Cloud-Dienst und Nutzungszeitraum abdecken. Weiterhin ist festzulegen, wie zugesicherte Prüf- und Kontrollrechte wahrgenommen werden können.

CD.16: Leistungsfähigkeit prüfen

„Die Stelle des Bundes muss mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, überprüfen und ggf. anpassen."

Die Netzwerkanbindung an den Cloud-Dienst nimmt vor allem für die Verfügbarkeit eine zentrale Rolle ein. Die Bundesbehörde muss daher ihre eigene Infrastruktur hinsichtlich der benötigten Leistungsfähigkeit überprüfen (z. B. SLA für externe Netzanbindung, eingesetzte Firewalls, Anbindung der Arbeitsplatzrechner usw.)

CD.17: Informationspflichten nachhalten

„Die Stelle des Bundes muss nachhalten, dass der Cloud-Anbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

- *einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,*
- *einem Austausch von Unterauftragnehmern oder Dritten.*

Darüber hinaus dokumentiert die Stelle des Bundes Meldungen des Cloud-Anbieters über relevante Störungen und Cyber-Angriffe."

Die Bundesbehörde muss festlegen, wie die Informationen des Cloud-Anbieters (z. B. zu den Anforderungen CD.07 "Änderungen bei Unterauftragnehmern; CD.11 "Meldung sicherheitsrelevanter Vorfälle) innerhalb des eigenen ISMS weiterverarbeitet werden sollen und wie in diesem Zusammenhang ein Monitoring erfolgen kann.

CD.18: Informationsaustausch

„Die Stelle des Bundes informiert das BSI über die eigene Nutzung externer Cloud-Dienste jährlich zum Stichtag 31. Januar. Diese Informationen umfassen auch Beendigung und Wechsel von externen Cloud-Diensten."

Zum Informationsaustausch siehe Hinweise in Kapitel 1.3.

2.3 Sicherheitsanforderungen "Beendigungsphase"

CD.19: Datenrückgabe durchführen

„Alle Daten müssen vom Cloud-Anbieter in der vereinbarten Form zurück an die Stelle des Bundes übergeben werden. Die Übergabe muss dokumentiert werden."

Einforderung und Umsetzung der festgelegten Regelungen zur Datenrückgabe. Die Regelungen ergeben sich aus dem jeweiligen Vertrag (siehe hierzu CD.13).

CD.20: Datenlöschung bestätigen

„Der Cloud-Anbieter muss die Löschung aller Daten der Stelle des Bundes, einschließlich vorhandener Datensicherungen, bestätigen. Dies muss auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen. Die Datenlöschung muss dokumentiert sein."

Wurde die Löschung aller Daten nach Vertragsende vereinbart, hat sich die Bundesbehörde die tatsächliche Löschung dann vom Cloud-Anbieter schriftlich bestätigen zu lassen.

3 Umsetzungshinweise zur Mitnutzung externer Cloud-Dienste

Im Anwendungsbereich der Mitnutzung greifen IT-Anwender einer Behörde auf einen externen Cloud-Dienst zu, ohne dass die Behörde ein Vertragsverhältnis mit dem Anbieter eingegangen ist. Diese Fälle waren bisher nicht durch Mindeststandards geregelt. Daher hat das BSI einen entsprechenden Mindeststandard nach § 8 Abs. 1 BSIG über die Mitnutzung externer Cloud-Dienste veröffentlicht (siehe Kapitel 1).

Vor jeder Mitnutzung ist eine Risikoanalyse und Datenkategorisierung durchzuführen. Sie liefern entscheidende Informationen, um die spätere Bewertung des externen Cloud-Dienstes durchführen zu können. Sie sind daher zwingend. Informationen dazu sind in Kapitel 1.2 aufgeführt.

Auf Basis dieser kann die Umsetzung der Sicherheitsanforderungen beginnen. Am Ende steht immer eine bewusste Entscheidung der Bundesbehörde für oder gegen die Mitnutzung des externen Cloud-Dienstes.

3.1 Sicherheitsanforderungen "Bewertung externer Cloud-Dienste"

Im ersten Regelungsbereich (MCD.2.1.01 bis MCD.2.1.12) nimmt die Informationsbeschaffung und -bewertung über den externen Cloud-Dienst eine zentrale Rolle ein. Anhand der Informationen soll der IT-SiBe letztendlich in die Lage versetzt werden, eine zuverlässige Bewertung hinsichtlich der Informationssicherheit des externen Cloud-Dienstes vorzunehmen. Hierbei ist es das primäre Ziel, eine bewusste Entscheidung darüber zu treffen, ob der externe Cloud-Dienst den Sicherheitsbedürfnissen des jeweiligen Anwendungsfalles genügt. Die Hausleitung entscheidet auf dieser Grundlage, ob dieser Cloud-Dienst künftig mitgenutzt werden soll oder nicht.

Die nachfolgenden Sicherheitsanforderungen folgen diesem Ansatz und bestehen daher jeweils aus zwei Teilen. Der erste Teil stellt dar, welche Informationen zu ermitteln sind (z. B. Gerichtsstand, Datenlokationen usw.). Im zweiten Teil sind diese ermittelten Informationen zu bewerten.

Für den Bewertungsteil geben die Sicherheitsanforderungen keine „harten“ Ausschlusskriterien vor. Dies erfolgt vor dem Hintergrund des großen Anwendungsbereiches der Mitnutzung. So könnte beispielsweise eine Datenverarbeitung über mehrere Kontinente hinweg akzeptiert werden, wenn lediglich „offene Daten“ verarbeitet werden sollen. Die Bewertung könnte aber zu einem anderen Ergebnis führen, wenn stattdessen auch Daten der Kategorie 3 verarbeitet werden sollen. Daher hier eine auf den Anwendungsfall bezogene Bewertung erforderlich. Diese sollte durch den zuständigen IT-SiBe erfolgen. Dieser kann bei Bedarf entsprechende Unterstützung heranziehen (z. B. hauseigene Justiziariat, Fachreferate, Datenschutzbeauftragte, Geheimschutzbeauftragte, IT-Referat usw.). Auch das BSI steht für beratende Unterstützung zur Verfügung.

Es muss in diesem Zusammenhang häufig entschieden werden, wie mit möglichen verbleibenden Risiken umgegangen werden soll. Hierfür schlägt der BSI-Standard 200-3: Risikomanagement eine entsprechende Vorgehensweise vor. Letztendlich müssen die für den Anwendungsfall geeigneten Risikobehandlungs-optionen (z. B. Vermeidung, Reduzierung, Akzeptanz) ausgewählt werden.

Externe Cloud-Dienste könnten auch dann mitgenutzt werden, wenn Risiken durch zusätzliche technische oder organisatorische Maßnahmen ausreichend reduziert, vermieden oder akzeptiert werden. IT-Anwender sind dann entsprechend zu sensibilisieren und über die ggf. nur eingeschränkte Mitnutzung zu informieren.

Als Beispiel für eine organisatorische Maßnahme könnte das Festlegen bestimmter Daten dienen, die im Anwendungsfall verarbeitet werden dürfen. So könnte den IT-Anwendern ausschließlich eine Verarbeitung von Daten der Kategorie 4 gestattet werden (siehe Kapitel 1.2). Als technische Maßnahme könnte eine Mitnutzung nur über gesonderte Stand-Alone-PCs erfolgen, die keine Anbindung an das interne Hausnetz haben.

Die Entscheidung, ob der externe Cloud-Dienst künftig mitgenutzt werden soll oder nicht, hat die jeweilige Hausleitung zu treffen.[5] Die Entscheidungsbefugnis kann delegiert werden. So kann bei einer ausschließlichen Verarbeitung von Daten der Kategorie 4 auch der zuständige IT-Sicherheitsbeauftragte die Entscheidung treffen, wenn er von der Hausleitung dazu ermächtig wurde. In jedem Fall werden hierfür Informationen benötigt, die eine sachgerechte Entscheidung ermöglichen. Die Sicherheitsanforderungen sorgen dafür, dass diese Informationen strukturiert abgefragt und bewertet werden.

Nachfolgend werden Umsetzungshinweise für die Sicherheitsanforderungen aus Kapitel 2.1 des Mindeststandards zur Mitnutzung externer Cloud-Dienste gegeben.

MCD.2.1.01: Anwendbares Recht, Gerichtsstand

„Es ist zu ermitteln, unter welchem Recht die Vereinbarung zwischen der nutzenden Institution und dem Cloud-Anbieter unterliegt und unter welchem Gerichtsstand sie steht."

Das anwendbare Recht sowie der Gerichtsstand können bei der nutzenden Institution (Auftraggeber) erfragt werden. Eventuell sind entsprechende Allgemeine Geschäftsbedingungen des Cloud-Anbieters auch online einsehbar. Können diese Informationen nicht ermittelt werden, ist dies zu vermerken und entsprechend zu bewerten.

Liegt ein Prüfbericht nach C5 vor, können diese Angaben dem Umfeldparameter "UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

„Es ist zu bewerten, ob Vereinbarungen, die nicht deutschem Recht folgen und keinen deutschen Gerichtsstand vorsehen, von der mitnutzenden Behörde unter Berücksichtigung der Ergebnisse der Datenkategorisierung und Risikoanalyse akzeptiert werden können. Dies ist grundsätzlich gegeben, wenn ausschließlich Daten der Kategorie 4 verarbeitet werden sollen."

Vor dem Hintergrund des jeweiligen Anwendungsfalles ist zu prüfen, welche Bedeutung ein Gerichtsstand außerhalb von Deutschland hätte. Hierbei ist insbesondere zu bewerten, inwiefern Durchsetzungsrechte oder Eilrechtsschutz von Bedeutung sind. Gleiches gilt für das anzuwendende Recht. Eine Bewertung des anwendbaren Rechts könnte aufgeteilt nach Regionen erfolgen:

- Deutsches Recht,
- Recht eines EU-Mitgliedstaates,
- Recht eines Nicht-EU-Mitgliedstaates
- unbekannt

Kann das anwendbare Recht nicht ermittelt werden, ist hierfür die Option "unbekannt" auszuwählen. Dies führt im Regelfall zu einem Ausschluss, da die Bundesbehörde wissen muss, welches Recht gilt und welche gesetzlichen Rechte und Pflichten sie treffen und wie diese ggf. durchgesetzt werden können. Kommt es zu einer gerichtlichen Auseinandersetzung nimmt der Gerichtsstand eine wichtige Rolle ein. Vor diesem Hintergrund könnte die Zuordnung des Gerichtsstandes nach Regionen erfolgen:

- "innerhalb Deutschlands",
- "innerhalb der EU",
- "außerhalb der EU" oder
- "unbekannt".

MCD.2.1.02: Offenbarungspflichten und Ermittlungsbefugnisse

„Es ist zu ermitteln, ob und unter welchen fremdstaatlichen Offenbarungspflichten und Ermittlungsbefugnissen der Cloud-Anbieter steht."

Liegt ein Prüfbericht nach C5 vor, können diese Informationen den Angaben zum Umfeldparameter "UP-03 Offenbarungs- und Ermittlungsbefugnisse" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden. Alternativ können auch entsprechende Transparenzberichte herangezogen werden. In der Regel sollte dazu der Auftraggeber des externen Cloud-Dienstes befragt werden. Können diese Informationen nicht ermittelt werden, ist dies zu vermerken und entsprechend zu bewerten.

[5] Siehe hierzu auch BSI-Standard 200-3: Risikomanagement, S. 34

„Es ist zu bewerten, ob Risiken durch mögliche Informationsabflüsse dieser Art akzeptiert werden können. Diese sind im Regelfall nicht zu akzeptieren, wenn Daten der Kategorie 3 verarbeitet werden sollen."

Der Umgang mit Offenbarungspflichten und Ermittlungsbefugnissen ist für Bundesbehörden durch das Bundesministerium des Innern bereits geregelt. Siehe hierzu Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014.

Eine Zuordnung könnte nach Regionen vorgenommen werden:

- Deutschland
- EU-Mitgliedsstaat
- Nicht EU-Mitgliedsstaat
- Unbekannt.

MCD.2.1.03: Datenlokationen

„Es ist zu ermitteln, an welchen Lokationen Daten verarbeitet werden."

Liegt ein Prüfbericht nach C5 vor, können diese Angaben dem Umfeldparameter "UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung" entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

Alternativ können dazu auch Informationen in den Verträgen oder Dienstgütevereinbarungen (Service Level Agreement) stehen. Hierzu sollte der Auftraggeber des externen Cloud-Dienstes kontaktiert werden. Können diese Informationen nicht ermittelt werden, ist dies zu vermerken und entsprechend zu bewerten.

Eine Zuordnung der Datenlokationen nach Regionen könnte wie folgt vorgenommen werden:

- Deutschland
- EU-Mitgliedsstaat
- Nicht EU-Mitgliedsstaat
- unbekannt

„Es ist zu bewerten, ob aus Sicht der mitnutzenden Behörde die Daten an den zugesicherten Lokationen verarbeitet werden dürfen. Hierfür sind insbesondere die Ergebnisse der Datenkategorisierung heranzuziehen."

Wie einleitend beschrieben sind die Risikobehandlungsoptionen immer auf den Anwendungsfall bezogen auszuwählen. So kann eine Datenverarbeitung ausschließlich von Daten der Kategorie 4 durchaus vertretbar sein.

MCD.2.1.04: Nutzung und Weitergabe von Daten an Dritte

„Es ist zu ermitteln, welche Rechte dem Cloud-Anbieter oder Dritten an den bzw. mit dem Umgang der Daten eingeräumt werden."

Die hier eingeräumten Rechte sind insbesondere von Bedeutung, wenn Daten der Kategorie 1 bis 3 verarbeitet werden sollen. Aber auch bei einer ausschließlichen Verarbeitung von Daten der Kategorie 4 ist hier eine kritische Bewertung notwendig.

„Es ist zu bewerten, ob die Vereinbarungen und Bedingungen des Cloud-Anbieters mit den IT-Sicherheitsrichtlinien der mitnutzenden Behörde vereinbar sind. Hierzu sind insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Anbieters auszuwerten. Rechte, aufgrund derer Daten an Dritte zu kommerziellen Zwecken verkauft oder selbst durch den Cloud-Anbieter außerhalb der konkreten, vorgesehenen Leistungserbringung genutzt werden können, sind im Regelfall nicht zu akzeptieren."

Für die Bewertung der Nutzung und Weitergabe von Daten an Dritte könnte folgende Unterteilung genutzt werden:

- keine Rechte für die Nutzung und Weitergabe von Daten an Dritte
- Rechte, die eine Weitergabe und Verarbeitung durch Unterauftragnehmer ermöglichen
- Rechte, die einen Verkauf der Daten an Dritte zu kommerziellen Zwecken ermöglichen

- Rechte, die eine Nutzung der Daten außerhalb der konkreten vorgesehenen Leistungserbringung ermöglichen
- unbekannt.

MCD.2.1.05: Verfügbarkeit der Daten

„Es ist zu ermitteln, welche verbindlichen Zusagen hinsichtlich der Verfügbarkeit des Cloud-Dienstes existieren."

Zusagen für die Verfügbarkeit des externen Cloud-Dienstes sind zu ermitteln und aus Sicht der IT-Anwender (Anwendungsfall) einzuordnen:

- konkrete Zusagen zur Verfügbarkeit, diese sind dem Anwendungsfall angemessen
- konkrete Zusagen zur Verfügbarkeit, diese sind dem Anwendungsfall nicht angemessen
- keine konkrete Zusagen
- Zusagen sind nicht bekannt

„Es ist zu bewerten, ob aus Sicht der mitnutzenden Behörde die zugesicherte Verfügbarkeit ausreichend ist. Für die Bewertung können insbesondere die Regelungen zur Anwendung des HV-Benchmark kompakt herangezogen werden. Die Verfügbarkeit von Daten ist auch von der eigenen IT-Infrastruktur abhängig. Die Behörde muss daher mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performanz der Netzanbindung und -verbindungen, überprüfen und ggf. anpassen."

Der HV-Benchmark kompakt hilft bei der Bewertung von Rechenzentren in Bezug auf die IT-Sicherheit. In diesem Zusammenhang sei auch auf den Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt verwiesen. Das im HV-Benchmark vorgestellte Verfahren kann dazu genutzt werden, das eigene Rechenzentrum hinsichtlich der Anforderungen an die Verfügbarkeit zu überprüfen.

MCD.2.1.06: Verschlüsselung der Datenübertragung

„Es ist zu ermitteln, ob die Daten über einen sicheren Kanal übertragen werden."

Eine sichere Verschlüsselung bei der Übertragung der Daten zwischen der Bundesbehörde und dem externen Cloud-Dienst ist ein wesentlicher Bestandteil einer sicheren Nutzung.

Daher ist hierzu ermitteln ob und mit welcher Technologie die Verschlüsselung erfolgt. Das Ergebnis kann entsprechend eingeordnet werden:

- Verschlüsselung der Datenübertragung mit folgendem Protokoll (z. B. TLS 1.2)
- keine Verschlüsselung der Datenübertragung
- unbekannt ob und welche Technik zur Verschlüsselung eingesetzt wird

Liegt ein Prüfbericht nach C5 vor, können diese Angaben der Umsetzung zur Basisanforderung "KRY-02-Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)" entnommen werden.

„Hierfür muss die Stärke der Schlüssel (Schlüssellänge und -verfahren) den IT-Sicherheitsrichtlinien der mitnutzenden Behörde entsprechen. Liegt dem sicheren Kanal eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls genügen. Wird eine VPN-Verbindung genutzt, muss diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der mitnutzenden Behörde entsprechen."

Für die Bewertung wird insbesondere auf die Regelungen zum Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls verwiesen. Wenn zur Verschlüsselung der Daten TLS verwendet wird, hat diese auf Basis von TLS 1.2 in Kombination mit Perfect Forward Secrecy zu erfolgen. Für eine erste Überprüfung von HTTPS-Verbindungen stehen im Internet bereits verschiedene Dienste zur Verfügung.

MCD.2.1.07: Verschlüsselung der Daten

„Es ist zu ermitteln, wie die Daten vom Cloud-Anbieter verschlüsselt gespeichert werden."

Neben der Verschlüsselung des Transportweges (siehe MCD.2.1.08) sollte auch eine Verschlüsselung der Daten im Cloud-Dienst erfolgen. Hierfür muss der Cloud-Anbieter Verfahren und technische Maßnahmen zur Verschlüsselung bei der Speicherung etablieren. Ausnahmen können für Daten akzeptiert werden, wenn diese für die Erbringung des Cloud-Dienstes funktionsbedingt nicht verschlüsselt sein können.

Daher ist hierzu ermitteln ob und mit welcher Technologie eine Verschlüsselung erfolgt. Das Ergebnis kann entsprechend eingeordnet werden:

- Verschlüsselung der Daten erfolgt auf Basis von:
- keine Verschlüsselung der Daten
- unbekannt ob und welche Technik zur Verschlüsselung eingesetzt wird

„Es ist zu bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung und Risikoanalyse vereinbar sind (Die eingesetzte Verschlüsselung sollte der Basisanforderung „KRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung" des C5 entsprechen). Ist die vom Cloud-Anbieter eingesetzte Verschlüsselung nicht geeignet, ist zu prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können."

Liegt ein Prüfbericht nach C5 vor, können diese Angaben der Umsetzung zur Basisanforderung "KRY-03-Verschlüsselung von sensiblen Daten bei der Speicherung" entnommen werden.

MCD.2.1.08: Erforderliche Softwareinstallationen

„Es ist zu ermitteln, ob für die Mitnutzung auf Arbeitsplatzcomputern oder mobilen Endgeräten der IT-Anwender zusätzliche Softwareinstallationen erforderlich sind."

Ist für die Mitnutzung die Installation von Software auf den Arbeitsplatzrechner erforderlich, können dadurch weitere Risiken entstehen. Daher sind hierzu entsprechende Informationen zu ermitteln. Das Ergebnis kann dann entsprechend eingeordnet werden:

- Softwareinstallation ist erforderlich: Name der Anwendung
- Softwareinstallation ist optional: Name der Anwendung
- Softwareinstallation nicht erforderlich
- unbekannt

„Es ist zu bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitsrichtlinie der mitnutzenden Behörde vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

In diesem Zusammenhang ist zu überprüfen, welche Berechtigungen die Software benötigt. (z. B. lokale Administrationsrechte) Hier sollte insbesondere hinterfragt werden, ob diese mit den sonstigen behördeninternen Regelungen vereinbar sind.

Ist ein Zugriff über mobile Endgeräte geplant, sind diese zentral zu verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten."

Weiterhin ist zu ermitteln, ob ein Zugriff über mobile Endgeräte möglich ist. Auch hier kann das Ergebnis entsprechend zugeordnet werden:

- Nutzung mobiler Endgeräte erforderlich
- Nutzung mobile Endgeräte nicht erforderlich
- unbekannt

Ist eine Mitnutzung auch über mobile Endgeräte möglich, muss dieses Szenario entsprechend bewertet werden. Hier sind verschiedene technische (Zugriff nur über verwaltete Geräte) oder organisatorische Maßnahmen (z. B. Verbot des Zugriffs über private Geräte) möglich, um die Risiken zu reduzieren oder zu vermeiden.

MCD.2.1.09: Berechtigungsvergabe

„Es ist zu ermitteln, wie die Berechtigungsvergabe erfolgt."

Für die Bewertung ist es notwendig zu ermitteln, wie im externen Cloud-Dienst die Berechtigungsvergabe organisiert ist. Das Ergebnis kann dann entsprechend eingeordnet werden:

- durch Gruppenadministrator der nutzenden Institution
- durch Systemadministratoren des Cloud-Anbieters
- Sonstiges:
- unbekannt

Liegt ein Prüfbericht nach C5 vor, können diese Angaben der Umsetzung zur Basisanforderung "IDM-03-Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen" entnommen werden.

„In diesem Zusammenhang ist insbesondere zu bewerten, ob die Berechtigungsvergabe dem Berechtigungskonzept der mitnutzenden Behörde genügt."

Die Berechtigungsvergabe und das Rollenkonzept sollten mit den behördeninternen Anforderungen abgeglichen werden. Abweichungen sind entsprechend zu bewerten.

MCD.2.1.10: Kündigungsfristen

„Es ist zu ermitteln, welche Kündigungsfristen Auftraggeber und Cloud-Anbieter vereinbart haben."

Kündigungsfristen sind unter Beachtung des Anwendungsfalles und insbesondere unter Berücksichtigung der Ergebnisse aus Risikoanalyse und Datenkategorisierung zu betrachten. Daher sind diese durch die Bundesbehörde für den jeweiligen Anwendungsfall zu ermitteln und zu bewerten. Dabei gilt - je "kritischer" ein Cloud-Dienst für die Bundesbehörde ist, desto länger sollten Kündigungsfristen Seitens des Cloud-Anbieters ausgestaltet sein.

Weiterhin ist zu ermitteln, ob (kurzfristige) einseitige Kündigungs- oder Zurückbehaltungsrechte für den Anwendungsfall relevant sein können:

- einseitige Kündigungs- oder Zurückbehaltungsrechte werden dem Cloud-Anbieter eingeräumt
- einseitige Kündigungs- oder Zurückbehaltungsrechte werden dem Cloud-Anbieter nicht eingeräumt
- unbekannt

„Es ist zu bewerten, ob die vereinbarten Kündigungsfristen mit dem Einsatzszenario der mitnutzenden Behörde vereinbar sind. Kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte von Leistungen sind stets kritisch zu hinterfragen."

Sehr kurze Kündigungsfristen können negative Auswirkungen haben. Diese sind daher zu bewerten.

MCD.2.1.11: Datenrückgabe und Datenlöschung

„Es ist zu ermitteln, welche Vereinbarungen zwischen Auftraggeber und Cloud-Anbieter zur Datenrückgabe und -löschung existieren und ob diese auch für die mitnutzende Behörde gelten. Lock-In-Effekte sind zu vermeiden, daher ist zu prüfen, ob der externe Cloud-Anbieter einen Datenexport in einem marktgängigen Datenformat anbietet."

Je nach Anwendungsfall können fehlende Vereinbarungen zur Datenrückgabe und Datenlöschung für die Bundesbehörde zusätzliche Risiken darstellen. Daher sind die Vereinbarungen zu ermitteln und für die nachfolgende Bewertung entsprechend einzuordnen:

- Rückgabe und Löschung der Daten ist vertraglich zugesichert
- Rückgabe und Löschung der Daten ist vertraglich nicht zugesicherte
- Rückgabe und Löschung der Daten ist für den Anwendungsfall nicht relevant.

„Es ist zu bewerten, ob die Rechte und Maßnahmen zur Datenrückgabe und -löschung mit den Ergebnissen der Datenkategorisierung und Risikoanalyse sowie den gesetzlichen Anforderungen vereinbar sind."

Die Bundesbehörde muss Regelungen zur Datenrückgabe kennen. Dies beinhaltet u.a. Format, Datenträger, Protokolle und die Dokumentation der Übergabe muss definiert werden. Hierbei sind insbesondere die Ergebnisse der Datenkategorisierung zu berücksichtigen, so dass eine Datenrückgabe nicht unbedingt zwingend sein muss. Für die Festlegung der Maßnahmen zur Datenlöschung und ggf. Datenmigration wird analog verfahren.

MCD.2.1.12: Informationsaustausch

„Die mitnutzende Behörde informiert das BSI über die Mitnutzung von externen Cloud-Diensten jährlich zum Stichtag 31. Januar. Diese Informationen umfassen auch Beendigung und Wechsel. Hierfür ist das dafür vorgesehene Formblatt zu verwenden."

Zum Informationsaustausch siehe Hinweise in Kapitel 1.3.

3.2 Sicherheitsanforderungen „Sichere Mitnutzung externer Cloud-Dienste"

Im zweiten Regelungsbereich sind Sicherheitsanforderungen an die konkrete Mitnutzung. Diese sind daher von den jeweiligen IT-Anwendern zu beachten und umzusetzen. Der IT-SiBe unterstützt hierbei entsprechend.

MCD.2.2.01: Mindestanforderung an Kennwörter

„Für den Kennwortgebrauch sind die verbindlichen Regeln der mitnutzenden Behörde zu beachten. Unter Berücksichtigung der Ergebnisse aus Datenkategorisierung und Risikoanalyse muss für die Authentisierung am externen Cloud-Dienst ausreichend starke Kennwörter (oder alternative Verfahren, die mindestens ein vergleichbares Sicherheitsniveau gewährleisten) genutzt werden. Diese müssen insbesondere gegenüber Brute-Force-Angriffen hinreichend stark sein."

Die Stärke des verwendeten Kennworts trägt maßgeblich zur sicheren Mitnutzung bei. Es sollte daher mindestens die Anforderungen der IT-Sicherheitsrichtlinie der mitnutzenden Bundesbehörde erfüllen.

Generelle Hinweise zum Kennwortgebrauch sind auch im IT-Grundschutz-Kompendium zu finden („ORP.4.A8 - Regelung des Passwortgebrauchs").

MCD.2.2.02: Umgang mit Benutzernamen und Kennwörtern

„Benutzername und Kennwort sind zu schützen. Kennwörter dürfen nur dem jeweiligen IT-Anwender bekannt sein. Auch auf mobilen Endgeräten sind Benutzername und Kennwort nicht ungeschützt zu speichern. Werden Benutzernamen und Kennwörter von mehreren IT-Anwendern genutzt (sog. Account Sharing), ist hierfür die Genehmigung des zuständigen IT-SiBe einzuholen. Grundsätzlich ist Account Sharing zu vermeiden und nur in begründeten Einzelfällen möglich."

Werden Benutzernamen und / oder Kennwörtern unberechtigten Dritten bekannt, können dadurch Risiken für den gesamten Cloud-Dienst entstehen. Daher sind diese besonders zu schützen.

MCD.2.2.03: Mitteilungen bei Änderungen

„Werden Änderungen oder beabsichtigte Änderungen am externen Cloud-Dienst den IT-Anwendern bekannt, sind diese unverzüglich dem zuständigen IT-SiBe mitzuteilen."

Die Entscheidung für die Mitnutzung des externen Cloud-Dienstes basiert maßgeblich auf der Bewertung der vorliegenden Informationen (siehe MCD.2.1.01 bis MCD 2.1.11). Änderungen können die Bewertungen verändern und damit auch die Grundlage der Mitnutzung entziehen. Daher sind die IT-Anwender dahingehen zu sensibilisieren, bei bekannt werden von Änderungen diese dem IT-SiBe mitzuteilen.