Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Umsetzungshinweise zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste 2.1

Version 2.1 vom 15.12.2022

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	20.06.2018	Erstveröffentlichung
2.0	03.02.2022	Anpassung an MST-Version 2.0
2.1	15.12.2022	Anpassung an MST-Version v2.1

Tabelle 1: Versionsgeschichte der Umsetzungshinweise zum Mindeststandard zur Nutzung externer Cloud-Dienste

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Allgemeine Umsetzungshinweise

Das vorliegende Dokument unterstützt IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal bei der Interpretation und Umsetzung des Mindeststandards (MST) des Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Cloud-Dienste – Version 2.1 vom 15.12.2022[2].

Im ersten Kapitel dieses Dokumentes werden allgemeine Hinweise zur Umsetzung der Anforderungen des Mindeststandards gegeben. Dazu gehört die Erläuterung zentraler Begriffe sowie der Anwendungsbereiche dieses Mindeststandards. Nach Hinweisen zur Kategorisierung der mittels eines Cloud-Dienstes verarbeiteten Daten werden wesentliche Rahmendokumente für die Umsetzung dieses Mindeststandards beschrieben. Mit einem kurzen Überblick über den C5-Kriterienkatalog[3] endet das erste Kapitel.

Das zweite Kapitel dieses Dokumentes gibt Hinweise zur konkreten Umsetzung der Anforderungen des Mindeststandards und ist untergliedert nach den vier Phasen des Lebenszyklus einer Cloud-Nutzung. Dabei wird auch die Mitnutzung eines Cloud-Dienstes betrachtet, die zuvor in einem eigenen Mindeststandard behandelt wurde.[4]

1.1 Begriffsbestimmung und Abgrenzung

Für die korrekte Anwendung dieses 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. Der Mindeststandard nutzt die Definition für Cloud-Dienste des C5[5], die sich an die internationale Begriffsdefinition des ISO 17788 anlehnt.[6] Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen („Cloud-Dienste“) erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der in diesem Rahmen angebotenen Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen.

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern außerhalb der Verwaltung des Bundes erbracht werden.[7] Cloud-Dienste, die von IT-Dienstleistern des Bundes angeboten werden, 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] Analog „Informationssicherheitsbeauftragte (ISB)“

[2] MST NCD 2.1 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022a)

[3] Der Cloud Computing Compliance Criteria Catalogue – C5 (Kriterienkatalog Cloud Computing) liegt in zwei Ausgaben vor: der Ausgabe C5:2020 (Erscheinungsjahr 2020) und der Ausgabe C5:2016 (Erscheinungsjahr 2016). Sofern nicht anders angegeben, wird hier die Ausgabe C5:2020 referenziert.

[4] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

[5] Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)

[6] Der Standard „ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary“ (International Organization for Standardization (ISO), 2014) definiert Cloud Computing als Paradigma für die Ermöglichung über ein Netz auf ein skalierbaren und elastischen Pool von geteilten virtuellen oder physischen Ressourcen (Server, Plattform, Anwendung, Software, etc.) zuzugreifen und über ein Selbst-Service Portal zu bestellen und selbst zu administrieren. Ein Cloud-Service ist als über eine definierte Schnittstelle buchbare und über Cloud Computing angebotene Fähigkeiten („capabilities“) definiert. Cloud-Fähigkeiten werden nach Infrastruktur, Plattform und Anwendung unterschieden.

[7] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z. B. Bundescloud) fallen somit nicht unter diese Bestimmung.

1.2 Anwendungsbereiche

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 die Informationssicherheit eine zunehmend zentrale Rolle ein. Die Einforderung und Umsetzung von Sicherheitsanforderungen ist daher ein wichtiger Bestandteil bei der Inanspruchnahme von Cloud-Diensten.

Das BSI trägt diesem Bedarf Rechnung durch seinen aktuellen Mindeststandard zur Nutzung externer Cloud-Dienste 2.1 (s.o.), welcher aus den ursprünglichen Mindeststandards zur Nutzung[8] bzw. Mitnutzung[9] externer Cloud-Dienste hervorging. Der aktualisierte Mindeststandard umfasst somit zwei grundsätzliche Anwendungsbereiche: die Nutzung externer Cloud-Dienste sowie die Mitnutzung externer Cloud-Dienste.

1.2.1 Nutzung externer Cloud-Dienste

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

1.2.2 Mitnutzung externer Cloud-Dienste

Der zweite Anwendungsbereich stellt einen Sonderfall dar, in dem IT-Anwender einer Einrichtung externe Cloud-Dienste zwar in Anspruch nehmen, jedoch ohne dass zwischen der Einrichtung und dem Cloud-Anbieter ein Vertragsverhältnis darüber besteht. Damit ist die Einrichtung 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 Rahmenbedingungen haben beide Anwendungsbereiche auch Gemeinsamkeiten. Insofern gelten die in Kapitel 1 gemachten Aussagen für beide Anwendungsbereiche. Darauf aufbauend sind im weiteren Verlauf die Umsetzungshinweise zu den Sicherheitsanforderungen zur Nutzung (Kapitel 2.1 bis 0) und Mitnutzung (Kapitel 2.5) externer Cloud-Dienste aufgeführt.

1.2.3 Praxisbeispiele

Um die Differenzierung zwischen den beiden Anwendungsbereichen zu veranschaulichen, sind nachfolgend sechs unterschiedliche Praxisbeispiele aufgeführt. Dabei wird angegeben, in welchen Anwendungsbereich die Praxisbeispiele jeweils fallen bzw. ob der Mindeststandard überhaupt anzuwenden ist. Die jeweilige Begründung soll den Transfer in die Praxis erleichtern.

[8] MST CD 1.0 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017a)
[9] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

Beispiel	Begründung
Eine Einrichtung 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 Einrichtung u. a. Adressdaten von Außenkontakten.	Die Einrichtung 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 1.3).
Das IT-Referat einer Einrichtung 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.	Auftraggeber ist das IT-Referat und somit die Einrichtung. 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 1.3).

Tabelle 2: Anwendungsbereich: Nutzung externer Cloud-Dienste

Beispiel	Begründung
IT-Anwender eines Fachreferates sind eingeladen im Rahmen einer internationalen Arbeitsgruppe für den 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.	Auftraggeber des externen Cloud-Dienstes ist die europäische Institution. Die Einrichtung hat keinen Einfluss auf die Verträge und damit auch nicht auf Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Die Einrichtung 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 den vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2.5 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 Einrichtung 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 Einrichtung verarbeitet.	Auftraggeber ist der Lehrstuhl der internationalen Universität. Die Einrichtung hat keinen Einfluss auf die Verträge und damit auch nicht auf die Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Auch hier muss die Einrichtung 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 den vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2.5 des Mindeststandards. Danach erfolgt eine bewusste Entscheidung für oder gegen die Mitnutzung des externen Cloud-Dienstes.

Tabelle 3: Anwendungsbereich: Mitnutzung externer Cloud-Dienste

Beispiel	Begründung
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 Einrichtung als Auftragnehmer nutzt. Jedoch zielen beide Anwendungsbereiche insbesondere darauf ab, für die Verarbeitung von (dienstlichen) Daten entsprechende Sicherheitsanforderungen zu setzen. Eine Verarbeitung dieser besonders schützenswerten Daten (siehe Kapitel 1.3) erfolgt aber bei sogenannten Such- und Recherchediensten oder auch Webdiensten mit Registrierungszwang grundsätzlich nicht. Die Prüfung und Umsetzung der Sicherheitsanforderungen aus den beiden Anwendungsbereichen 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 dieses Mindeststandards.
Das IT-Referat einer Einrichtung bezieht für ein Webprojekt einen Cloud-Dienst über das Informationstechnikzentrum Bund (ITZBund). Über die Nutzung des Cloud-Dienstes wurde ein entsprechendes Service Level Agreement (SLA) abgeschlossen.	Zwar ist die Einrichtung hier in der Rolle des Auftraggebers, jedoch handelt es sich beim ITZBund nicht um ein Unternehmen aus der Wirtschaft. Cloud-Angebote der IT-Dienstleister des Bundes sind daher nicht externe Cloud-Dienste im Sinne des Mindeststandards zur Nutzung externer Cloud-Dienste (siehe Kapitel 1.1). Der Mindeststandard finden in diesen Fällen daher keine Anwendung.

Tabelle 4: Anwendungsbereich: Keine Nutzung/Mitnutzung eines externen Cloud-Dienstes im Sinne dieses Mindeststandards

1.3 Datenkategorisierung

Ein wesentlicher Punkt auch hinsichtlich einer Risikoanalyse – wie sie in den Anforderungen NCD.2.1.01 und NCD.2.1.03 gefordert wird – ist die Bestimmung bzw. Bewertung 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 schreibt der Mindeststandard eine Datenkategorisierung vor. 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:

Datenkategorie	Erläuterung
Datenkategorie 1: Privat- und Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß §§ 203 und 353b StGB	Hierunter fallen alle Daten, die durch das Strafgesetzbuch besonders geschützt sind. Daraus ergeben sich auch erhöhte Sicherheitsanforderungen an die Verarbeitung in einer externen Cloud. Hier reicht die Umsetzung der Basisanforderungen des C5[10] durch den Cloud-Anbieter allein in der Regel 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.
Datenkategorie 2: Personenbezogene Daten gemäß Artikel 4 Nummer 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 deshalb zu prüfen, welche optionalen weitergehenden Anforderungen des C5 der Cloud-Anbieter zusätzlich umzusetzen hat. Es wird empfohlen in diesem Zusammenhang die behördlichen Datenschutzbeauftragten einzubinden.
Datenkategorie 3: Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)[11]	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.
Datenkategorie 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. Dabei handelt es sich im Regelfall um Daten, für die eine Umsetzung der Basisanforderungen nach C5 ausreichend ist.

Tabelle 5: Anwendungsbereich: Keine Nutzung/Mitnutzung eines externen Cloud-Dienstes im Sinne dieses Mindeststandards

1.4 Rahmendokumente

Der Mindeststandard setzt die Erstellung verschiedener Rahmendokumente voraus. Diese sind auch Bestandteil der Vorgehensweise nach IT-Grundschutz. Konkret wird das Thema Cloud Computing im Baustein OPS.2.2 des IT-Grundschutz-Kompendiums[12] behandelt. Weitere hilfreiche Quellen für die Umsetzung des Mindeststandards sind die Umsetzungshinweise zu OPS.2.2 zum IT-Grundschutz-

[10] Cloud Computing Compliance Criteria Catalogue – C5:2020. Kriterienkatalog Cloud Computing (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)
[11] VSA (Bundesministerium des Innern und für Heimat (BMI), 2018)
[12] IT-Grundschutz-Kompendium 2022 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c)

Kompendium 2019[13], sowie die BSI-Veröffentlichung „Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende“[14]. Im Folgenden werden diese Quellen auszugsweise wiedergegeben. Über den IT-Grundschutz hinaus, stellt der Mindeststandard zusätzliche Anforderungen, welche in die genannten Rahmendokumente einfließen müssen (siehe Kapitel 2.1).

1.4.1 Strategie für die Cloud-Nutzung

Entscheidet sich eine Einrichtung für die Nutzung externer Cloud-Dienste, hat dies immer eine strategische Komponente, auch wenn der Umfang des Cloud-Dienstes gering ist. Letzteres kann dazu verleiten, die Konsequenzen dieses Outsourcings zu unterschätzen oder zu ignorieren, zumal es häufig der erste Fall von Outsourcing von IT-Dienstleistungen in einer Einrichtung ist. Im Rahmen der Erstellung einer Strategie für die Cloud-Nutzung sind wirtschaftliche, technische, organisatorische sowie sicherheitsrelevante Aspekte ausführlich zu betrachten.

Einbindung in die Institutionsstrategie

Der strategische Umgang der Einrichtung mit einer Cloud-Nutzung muss geregelt werden. Unter Berücksichtigung einer grundsätzlichen Entscheidung für die Nutzung von Cloud-Diensten ist zu ermitteln, in welchem Umfang klassische IT durch Cloud-Dienste abgelöst werden soll und welche Dienste dafür prinzipiell in Frage kommen.

Darüber hinaus ist festzulegen, welche Ziele die Einrichtung mit der Cloud-Nutzung erreichen möchte. Dies könnten beispielsweise sein: Kosteneinsparungen, flexiblerer Service, Ersatz bisheriger oder Einführung neuer Dienste.

Machbarkeitsstudie mit Zusammenstellung aller Rahmenbedingungen

Die Entscheidung zur Nutzung von Cloud-Diensten kann durch unterschiedliche externe Faktoren bedingt oder beeinflusst werden, wie

- rechtlichen Rahmenbedingungen (beispielsweise Vorgaben des Datenschutzes, von Aufsichtsbehörden oder von anderen Vertragspartnern),
- organisatorischen Rahmenbedingungen (beispielsweise Reife der Einrichtung hinsichtlich Organisation und IT) als auch
- technischen Anforderungen (beispielsweise Vorgaben bezüglich des benötigten Datennetzes, Leistungsfähigkeit der Internetanbindung, Verfügbarkeit der Datennetze und der IT-Systeme).

Die Ergebnisse dieser Untersuchung sind in einer Machbarkeitsstudie zu dokumentieren, welche die Eignung des untersuchten Cloud-Dienstes prüft.

Betriebswirtschaftliche Aspekte mit erster Kosten-Nutzen-Abschätzung

Da die Einführung von Cloud-Diensten oft der Kostenreduktion dient, steht die Relation von Kosten und Nutzen besonders im Fokus. Eine Kosten-Nutzen-Abschätzung gibt erste Hinweise auf die Wirtschaftlichkeit der Nutzung eines solchen Dienstes.

Neben den reinen Betriebskosten der Nutzung eines Cloud-Dienstes sind dabei auch die Kosten für die Migration, Schulung der Mitarbeitenden und des Administrationspersonals sowie gegebenenfalls für neue Hardware und den Ausbau der Netzkapazitäten zu berücksichtigen.

In die Kosten-Nutzen-Abschätzung sollte auch der strategische Wert der Ressourcen Know-how, Mitarbeitende, IT-Systeme und Anwendung eingehen. Durch die Nutzung eines Cloud-Dienstes könnten diese Ressourcen teilweise verloren gehen. Auf der Nutzenseite stehen beispielsweise Kostenersparnisse bei der Erneuerung obsoleter Hard- und Software, erhöhte Flexibilität der Leistungsfähigkeit der IT sowie

[13] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

[14] Sichere Nutzung von Cloud-Diensten (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016a)

möglicherweise Sicherheitsgewinne. Eine detailliertere Kosten-Nutzen-Analyse (siehe OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*) kann erfolgen, sobald der Cloud-Dienst genauer definiert ist und erste konkrete Angebote einzelner Cloud-Diensteanbieter vorliegen.

Auswahl der Dienste und des Bereitstellungsmodells

Anhand der zuvor genannten strategischen Überlegungen sollte festgehalten werden, welche konkreten Dienste zukünftig von einem Cloud-Diensteanbieter bezogen werden könnten. Die Entscheidung für ein geeignetes Bereitstellungsmodell (beispielsweis Private, Public oder Hybrid Cloud) erfolgt basierend auf den erhobenen Anforderungen. Dies wird auch als „Sourcing" bezeichnet.

Berücksichtigung von Sicherheitsaspekten von Anfang an

Bereits zu Beginn der Planungsmaßnahmen zur Cloud-Nutzung müssen grundlegende technische und organisatorische Sicherheitsaspekte ausreichend berücksichtigt werden. Insbesondere ist zu klären, ob und inwieweit das Cloud Computing in der Sicherheitsleitlinie behandelt wird. Folgender Cloud-Spezifika sollten sich die Verantwortlichen einer Einrichtung dabei bewusstmachen:

- Abhängig vom Cloud-Nutzungsmodell kann der Cloud-Dienstleister auf die Daten der beauftragenden Einrichtung zugreifen. Dies kann auch Daten mit erhöhtem Schutzbedarf betreffen.
- Zwischen der beauftragenden Einrichtung und dem Cloud-Dienstleister werden kontinuierlich Daten übertragen. Daraus erhöht sich das Gefahrenpotential, welches durch die Einrichtung zu ermitteln und zu bewerten ist.
- Mit der Einführung der Nutzung von Cloud-Diensten werden neue Prozesse und Arbeitsabläufe erforderlich. Diese müssen entworfen, eingeführt und umgesetzt werden. Die Folgen der dafür notwendigen Umstellungen müssen ermittelt und abgeschätzt werden.

Im Rahmen eines Einführungsvorhabens von Cloud-Diensten sollten alle Vor- und Nachteile mit Bezug zur Informationssicherheit durch die Einrichtung betrachtet, bewertet und dokumentiert werden.

Durchführung einer Risikoanalyse

Es muss seine Risikoanalyse nach BSI-Standard 200-3[15] durchgeführt werden. Weitere Informationen sind unter NCD.2.1.01, Buchstabe d) zu finden.

Erstellung einer Roadmap

Nach der Untersuchung strategischer und sicherheitsrelevanter Aspekte steht die Planung der Realisierung der gewünschten Cloud-Dienste im Fokus. Im Falle mehrerer Dienste hat sich die Erstellung einer Cloud-Roadmap bewährt. Dieser Fahrplan zur Einführung der Cloud-Dienste beschreibt anhand eines Phasenmodells den konkreten Roll-Out der Dienste. Ziel ist dabei die Erhöhung der Nutzendenakzeptanz bei gleichzeitiger Risikominimierung technischer Probleme bei der Umsetzung.

1.4.2 Sicherheitsrichtlinie für die Nutzung externer Cloud-Dienste

In einer Sicherheitsrichtlinie werden die Schutzziele und die allgemeinen Sicherheitsanforderungen einer Einrichtung formuliert. Sofern die Strategie für die Cloud-Nutzung bereits Sicherheitsvorgaben für die Nutzung externer Cloud-Dienste enthält, müssen diese in der Sicherheitsrichtlinie weiter ausgearbeitet werden. Dies dient auch als Entscheidungsgrundlage für die Auswahl geeigneter Cloud-Dienste und Diensteanbieter.

In diesem Zusammenhang müssen grundsätzlich alle Sicherheitsanforderungen betrachtet werden, die sich aus den organisatorischen, technischen und rechtlichen Rahmenbedingungen sowie den ermittelten Schnittstellen ergeben. Dies betrifft neben Sicherheitsanforderungen an die verwendete Technik inklusive der benötigten Kommunikationswege und -dienste beispielsweise auch Datenschutzaspekte. In der

[15] BSI-Standard 200-3 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017b)

Sicherheitsrichtlinie sollten außerdem auch organisatorische Aspekte, wie erforderliche Schulungsmaßnahmen für das Administrationspersonal und die Nutzenden, beachtet werden.

Weitere wesentliche Aspekte sind:

- Sicherheitsanforderungen an den Cloud-Dienstanbieter (beispielsweise die Einhaltung des Vier-Augen-Prinzips bei der Administration),
- Sicherheitsanforderungen in Abhängigkeit vom Bereitstellungsmodell (beispielsweise Zutritts- und Zugangsrechte für den Dienstleister beim Betrieb einer Private Cloud On-Premise),
- Sicherheitsanforderungen aus relevanten Gesetzen und Vorschriften (beispielsweise gesetzliche Bestimmungen bei international agierenden Dienstleistern).

1.4.3 Sicherheitskonzept für den externen Cloud-Dienst

Bei Verwendung von Cloud-Diensten muss für jeden verwendeten Cloud-Dienst ein Sicherheitskonzept basierend auf der IT-Grundschutz-Vorgehensweise erstellt werden. Grundlage des Dokumentes sind die Anforderungen, welche sich aus der Sicherheitsrichtlinie zur Cloud-Nutzung für einen konkreten Anwendungsfall ableiten lassen. Weiter werden die im Zusammenhang mit der Nutzung von Cloud-Diensten notwendigen Sicherheitsmaßnahmen im Sicherheitskonzept dokumentiert. Als Orientierung für die Erstellung des Sicherheitskonzeptes dienen dabei die Sicherheitsanforderungen an einen klassischen IT-Dienst.

In einem Sicherheitskonzept für die Cloud-Nutzung sollte darüber hinaus die durch die Nutzung von Cloud-Diensten entstehende besondere Gefährdungslage beschrieben werden. Insbesondere folgende Aspekte sollten dabei betrachtet werden:

- Ungeplante vorzeitige Vertragsbeendigung,
- mangelnde Portabilität von Daten (Software as a Service), Anwendungen (Platform as a Service) oder IT-Systemen (Infrastructure as a Service),
- generelle Abhängigkeit vom Cloud-Diensteanbieter mangels Wechselmöglichkeit (Vendor Lock-in),
- Gefährdung der Integrität von Informationen durch proprietäre Datenformate,
- gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Kunden (multi tenancy),
- Unkenntnis über den Speicherort der Informationen,
- hohe Mobilität der Informationen sowie
- unbefugter Zugriff auf Informationen beispielsweise durch Administrationspersonal des Cloud-Dienstanbieters oder andere Parteien.

Aus den erkannten spezifischen Gefährdungen für den jeweiligen Cloud-Dienst müssen konkrete Sicherheitsanforderungen abgeleitet werden. Deren Einhaltung sollte im Rahmen der Vertragsgestaltung mit dem Cloud-Dienstanbieter verbindlich vereinbart werden. Insbesondere die folgenden Punkte sollten dabei betrachtet werden:

- Vorgaben zur sicheren Administration des Cloud-Dienstes,
- Vorgaben zu Betriebsprozessen und Prozessen im Sicherheitsmanagement,
- Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen,
- Verschlüsselung der Informationen,
- Vergabe und Entzug von Berechtigungen sowie
- Durchführung von Datensicherungen, sowohl durch den Cloud-Diensteanbieter als auch durch die Einrichtung.

Das Sicherheitskonzept des Cloud-Diensteanbieter sollte regelmäßig durch unabhängige Dritte auf Aktualität sowie vollständige und korrekte Umsetzung überprüft werden.

1.5 Der C5-Kriterienkatalog des BSI

Ein wesentliches Dokument für diesen Mindeststandard ist der „Cloud Computing Compliance Criteria Catalogue – C5:2020“[16] des BSI (C5). Der C5 ist ein Kriterienkatalog und beschreibt Mindestanforderungen an die Informationssicherheit für Cloud-Dienste, die nicht unterschritten werden sollten. Ziel ist die transparente Darstellung der Informationssicherheit eines Cloud-Dienstes auf Basis einer standardisierten Prüfung. Diese kann von Kunden im Rahmen einer eigenen Risikoanalyse verwendet werden. Es obliegt also dem Kunden, das vorliegende Sicherheitsniveau in Relation zum eigenen Schutzbedarf zu bewerten. Der Kriterienkatalog wird von Cloud-Anbietern, Auditoren und Cloud-Kunden verwendet. Jede dieser Parteien hat eine Mitwirkungspflicht hinsichtlich der Informationssicherheit.

Cloud-Anbieter können die C5-Kriterien umsetzen, um die IT-Sicherheit ihrer Cloud-Dienste zu erhöhen und sich damit einen attraktiven Wettbewerbsvorteil zu verschaffen. Die Erfüllung der Kriterien kann beispielsweise durch Wirtschafts- oder andere geeignete Prüfer testiert und somit gegenüber Kunden nachgewiesen werden. Diese Prüfer werden in diesem Fall direkt vom Cloud-Anbieter beauftragt.

Die Verwendung von Cloud-Diensten bietet Chancen, birgt aber auch Risiken, sodass ein eigenes Risikomanagement durch jeden Kunden unerlässlich ist. Der Kunde ist auch in der Verantwortung zu prüfen, ob die Mindestkriterien für seinen konkreten Anwendungsfall durch weitergehende Kriterien ergänzt werden müssen. Verbleibende Restrisiken müssen durch den Kunden getragen und im Eintrittsfall verantwortet werden. Der C5 unterstützt den Kunden dabei, Transparenz hinsichtlich der Aufteilung sicherheitskritischer Aufgaben zwischen Cloud-Anbieter und -Kunden zu erhalten.

Die Kriterien des C5 sind untergliedert in 17 Bereiche, denen jeweils eine Zielsetzung zugewiesen ist, welche durch die Kriterien erreicht werden soll. Für einige C5-Kriterien bestehen korrespondierende Kriterien für Kunden, die aufzeigen sollen, wo potentiell Mitwirkungspflichten bestehen. Die Kunden müssen den Mitwirkungspflichten in ihrem Verantwortungsbereich nachkommen.

[16] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)

2 Umsetzungshinweise zu den Sicherheitsanforderungen

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 Planung, Beschaffung, Einsatz und Beendigung externer Cloud-Dienste 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 schon bekannt. Eine ganz zentrale Bedeutung bei der Bewertung externer Cloud-Dienste nimmt der C5-Kriterienkatalog zum Cloud Computing ein (siehe Kapitel 1.5). Er 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 daher, dass Einrichtungen bei einer Nutzung externer Cloud-Dienste 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 Einrichtung Transparenz über die Rahmenbedingungen. Durch diese Transparenz wird die Einrichtung erst in die Lage versetzt, ein Cloud-Angebot hinsichtlich ihrer eigenen Anforderungen an die Informationssicherheit beurteilen zu können. Der C5 folgt diesem Ansatz mit den sogenannten Rahmenbedingungen. Die 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.[17] 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.[18]

Der 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 Einrichtung genutzt werden sollen. Daneben bleibt die Verantwortung für die IT-Objekte, welche die Einrichtung im Rahmen ihrer IT-Grundschutz-Konzeption innehat, unberührt und wird durch die Nutzung externer Cloud-Dienste lediglich angepasst.

Nachfolgend sind die Sicherheitsanforderungen mit entsprechenden Umsetzungshinweisen gegliedert nach den Phasen Planung (Kapitel 2.1), Beschaffung (Kapitel 2.2), Einsatz (Kapitel 2.3) und Beendigung (Kapitel 2.4) dargestellt.

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

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

2.1 Planungsphase

Der Lebenszyklus der Nutzung eines Cloud-Dienstes beginnt mit der Planung der Nutzung und den dafür erforderlichen Vorarbeiten bzw. Überlegungen.

NCD.2.1.01 Strategie für die Cloud-Nutzung

a) Die Einrichtung MUSS eine Strategie für die Cloud-Nutzung nach OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung[19] erstellen.

b) Die Einrichtung MUSS in dieser Strategie für die Cloud-Nutzung festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu MUSS eine Richtlinie zur Risikoanalyse erstellt werden.[20]

c) Die Einrichtung MUSS prüfen, ob ein externer Cloud-Dienst grundsätzlich mit den in ihrer Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist.[21] Die Einrichtung DARF einen externen Cloud-Dienst NUR nutzen, wenn dieser die in der Strategie für die Cloud-Nutzung definierten Ziele, Chancen und Risiken angemessen unterstützt.

d) Die Einrichtung MUSS vor der Nutzung eines externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 b) festgelegten Richtlinie durchführen.

Zu a): Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie* wichtige Gesichtspunkte, welche in einer Strategie für die Cloud-Nutzung betrachtet und dokumentiert werden sollten.[22]

Zu b): Das Verfahren zur Erstellung einer Richtlinie wird im BSI-Standard 200-3 behandelt.

Zu d): Der Schutz der zu verarbeitenden Daten nimmt sowohl bei Nutzung, als auch bei Mitnutzung externer Cloud-Dienste 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 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.

NCD.2.1.02 Sicherheitsrichtlinie für externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung[23] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria

[19] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c), OPS.2.2 *Cloud-Nutzung*

[20] Siehe BSI-Standard 200-3, (BSI 2017b), S. 9f.

[21] Hinweis: OPS.2.2.A1 *Erstellung einer Strategie für die Cloud-Nutzung* sieht die Erstellung einer Strategie für die Cloud-Nutzung vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Strategie für die Cloud-Nutzung nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.

[22] Umsetzungshinweise IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

[23] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c), OPS.2.2 *Cloud-Nutzung*

Catalogue – C5 (Kriterienkatalog Cloud Computing) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[24]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung der Sicherheitsrichtlinie beteiligen und ebenfalls – sofern betroffen – die zuständigen Datenschutz- und Geheimschutzbeauftragten.

Zu a): Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* wichtige Aspekte, welche in die Sicherheitsrichtlinie für die Cloud-Nutzung eingehen sollten.[25]

Zu b): Die Basiskriterien nach dem C5 spiegeln aus Sicht des BSI das Niveau an Informationssicherheit wider, das ein Cloud-Dienst mindestens bieten muss, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen normalen Schutzbedarf haben. Die Basiskriterien bilden den Mindestumfang einer Prüfung nach dem C5 ab. Nichtsdestotrotz obliegt es den Cloud-Kunden, für ihren individuellen Anwendungsfall zu bewerten, inwiefern die Basiskriterien den Schutzbedarf ihrer Informationen angemessen reflektieren. Für Cloud-Kunden, deren Informationen einen höheren Schutzbedarf haben, können die Zusatzkriterien einen Ausgangs- bzw. Ansatzpunkt darstellen, um diese Bewertung vorzunehmen.[26]

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[27]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung des Sicherheitskonzeptes beteiligen und ebenfalls – sofern betroffen – die zuständigen Datenschutz- und Geheimschutzbeauftragten.

d) Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

– Kategorie 1 = Privat- und Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß Strafgesetzbuch (StGB) §§ 203 und 353b

– Kategorie 2 = personenbezogene Daten gemäß Datenschutzgrundverordnung (DSGVO) Art. 4 Nr. 1

[24] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)
[25] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)
[26] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), S. 15
[27] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

– Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[28]

– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

g) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen.

h) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten dienstlichen Daten dieser Kategorien die Geheim- und Datenschutzaspekte[29] sowie Anforderungen hinsichtlich Privat-, Dienst-, Betriebs- und Geschäftsgeheimnisse ermitteln und aus diesen ggf. entstehende, weitere Anforderungen ableiten.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln und bewerten.[30] Die Einrichtung MUSS die ermittelten Risiken gemäß den in der Strategie für die Cloud-Nutzung festgelegten Richtlinien zur Risikoanalyse bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß den in der Strategie für die Cloud-Nutzung genannten Richtlinien zur Risikoanalyse wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen)[31] unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

Zu a): Ein Sicherheitskonzept für Cloud-Dienste unterscheidet sich oft nur wenig von Sicherheitskonzepten für Informationsverbünde, die durch die Einrichtung selbst betrieben werden. Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* Besonderheiten, welche dabei berücksichtigt werden sollten.[32]

Zu d): Das Vorgehen zur Datenkategorisierung wurde bereits in Kapitel 1.3 ausführlich erläutert.

[28] VSA (Bundesministerium des Innern und für Heimat (BMI), 2018)

[29] Hinsichtlich der Datenschutzaspekte siehe insbesondere Orientierungshilfe – Cloud Computing (Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, 2014)

[30] Hinweis: Es gilt, zu bewerten, inwiefern die mit dem betrachteten Cloud-Dienst im beabsichtigten Anwendungsfall verbundenen rechtlichen, technischen und organisatorischen Risiken mit der Strategie für die Cloud-Nutzung vereinbar sind.

[31] 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. (Bundesministerium des Innern (BMI), 2014)

[32] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

2.2 Beschaffungsphase

Die Beschaffungsphase eines Cloud-Dienstes baut auf der Planungsphase und den darin erarbeiteten Strategien und Konzepten auf. Hinsichtlich der Beschaffung externer Cloud-Dienste sollte die Einrichtung insbesondere die einschlägigen „Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud)“[33] beachten und nutzen.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) erfüllt.[34]

b) Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5[35] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN mindestens

– die angemessene und wirksame Erfüllung der Basiskriterien nach C5[36],

– die aktuelle Dokumentation der Systembeschreibung[37],

– die Aktualität von vertraglich zugesicherten Zertifizierungen und Berichterstattungen sowie

– die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

[33] Vgl. EVB-IT Cloud, https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html

[34] Hinweis: Liegt ein C5-Prüfbericht vor, können diesem Informationen entnommen und der Bewertung zugrunde gelegt werden.

[35] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, die dabei unterstützt, einen C5-Prüfbericht systematisch auszuwerten. Diese Auswertung beinhaltet, die Sicherheitsmaßnahmen (Kontrollen) des Cloud-Diensteanbieters inklusive der zugehörigen Prüfergebnisse sowie der auf Cloud-Nutzerseite einzurichtenden Kontrollen aufzunehmen. In Verbindung mit den aufseiten der Einrichtung eingerichteten Kontrollen sowie weiterer, vom individuellen Anwendungsfall abhängenden Informationen lassen sich die mit der Nutzung des betrachteten Cloud-Dienstes verbundenen Risiken identifizieren und bewerten. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“ (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020b).

[36] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[37] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), Kapitel 3.4.3.2, S. 23f.) enthält der Bericht keine vom Cloud-Diensteanbieter angefertigte Systembeschreibung, sondern eine vom Prüfer im Rahmen der Prüfung angefertigte Systembeschreibung.

umfassen und KÖNNEN vom Cloud-Diensteanbieter durch die regelmäßige Bereitstellung einer aktuellen C5-Berichterstattung vom Typ2 erbracht werden.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten und eventuellen Unklarheiten und insbesondere darin ausgewiesene Abweichungen in geeigneter Form nachgehen. Hierbei MUSS die Einrichtung auch abwägen, ob und inwiefern ein Risiko entsteht und wie mit diesem umzugehen ist.

g) Insbesondere MÜSSEN Zertifikate, Prüfberichte und Nachweise den Zeitraum, in dem die Einrichtung den Cloud-Dienst nutzt, jeweils vollständig abdecken und DÜRFEN KEINE zeitlichen Lücken enthalten oder entstehen lassen. Dies MUSS die Einrichtung in ihre Sicherheitsanforderungen sowie demzufolge in die Leistungsbeschreibung aufnehmen.

h) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

i) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder akzeptieren, und MUSS dies entsprechend dokumentieren.

> *i) Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.*
>
> *ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.*

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

> *i) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.*
>
> *ii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revision oder Wirtschaftsprüfende) die Prüfrechte wahrnehmen können.*
>
> *iii) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.*
>
> *iv) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.*

Zu e): Die Basisanforderungen nach C5 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. Weiter soll sichergestellt werden, dass vertraglich zugesicherte Zertifizierungen und Berichterstattungen aktuell sind sowie Datensicherungskonzepte in der Praxis regelmäßig getestet und erprobt werden. Der C5 gibt hinsichtlich Prüfung und Berichterstattung entsprechende Regelungen vor (siehe C5, Kapitel 3.2 - 3.4). Der Prüfbericht muss der Einrichtung zugänglich gemacht werden, damit diese die Umsetzung prüfen kann. 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 f): Ist der Cloud-Anbieter vertraglich verpflichtet Nachweise zu erbringen (siehe Buchstabe d)), muss die Einrichtung festlegen, wie diese intern geprüft und ausgewertet werden können.

Zu g): Bei der Prüfung ist insbesondere darauf zu achten, dass die vorgelegten Nachweise den gesamten Cloud-Dienst und Nutzungszeitraum abdecken.

Zu h): 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.

Die hier thematisierten Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen werden von dem Cloud-Diensteanbieter selbst beauftragt. Im Gegensatz hierzu werden die Prüfungen unter j) von der Einrichtung selbst beauftragt oder durchgeführt.

Zu j): 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 Einrichtung insbesondere dann wahr, wenn Zweifel an der korrekten Umsetzung der vereinbarten Sicherheitsanforderungen bestehen. Mit der Prüfung kann die Einrichtung 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.

Kann der Cloud-Anbieter den geforderten Prüfbericht nach C5 oder gleichwertige Nachweise nicht vorlegen (siehe NCD.2.2.01, Buchstabe i), ii)), soll dies nicht zwingend zu einem Ausschluss des Anbieters führen. Daher wird hier die Möglichkeit geschaffen, die Prüfung durch die Einrichtung beauftragen zu lassen. Die dabei entstehenden Kosten sind in der Regel zumindest teilweise durch die Einrichtung selbst zu tragen.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter vollständig benennen lassen, welche seiner Unterauftragnehmer gemäß C5 als Subdienstleistungsunternehmen[38] anzusehen sind und auf welche Art und welchem Umfang er diese in die Bereitstellung des Cloud-Dienstes einbezieht.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass er der Einrichtung beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subdienstleistungsunternehmen, die in die Bereitstellung des Cloud-Dienstes involviert sind, unverzüglich schriftlich oder per E-Mail mitteilt.

[38] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), Kapitel 3.4.5, S. 25f.

i) Diese Mitteilung SOLLTE zeitlich vor Umsetzung der Änderung erfolgen.

ii) Der Cloud-Diensteanbieter MUSS der Einrichtung insbesondere mitteilen, wenn er bestehende Vertragsverhältnisse beendet oder neue Vertragsverhältnisse mit Subdienstleistungsunternehmen eingeht. Vertragsverhältnisse in diesem Sinne schließen alle mitgeltenden Dokumente und Regelungen, wie z. B. Leistungsscheine, Dienstgütevereinbarungen oder Allgemeine Geschäfts- und Einkaufsbedingungen ein.

c) Diese Mitteilungen KANN der Cloud-Diensteanbieter z. B. über Internetportale oder Push-Benachrichtigungen bereitstellen, wenn die Einrichtung diese Anforderungen als erfüllt ansieht.

d) Falls der Cloud-Diensteanbieter Subdienstleistungsunternehmen einbezieht oder anderweitig wesentliche Teile der Entwicklung oder Bereitstellung des Cloud-Dienstes an Unterauftragnehmer auslagert, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

– die Subdienstleistungsunternehmen und Unterauftragnehmer die zwischen der Einrichtung und dem Cloud-Diensteanbieter vertraglich festgelegten Vorgaben ebenfalls erfüllen und

– sich die Prüfrechte, die der Cloud-Diensteanbieter der Einrichtung zugesichert hat, auch auf die Subdienstleistungsunternehmen und Unterauftragnehmer des Cloud-Diensteanbieters beziehen.

Zu a): Liegt ein Prüfbericht nach C5 vor sind diese Informationen in der Systembeschreibung aufgeführt (siehe NCD.2.2.01, Buchstabe e)).

Zu b): Da Cloud-Angebote in der Regel flexibel gestaltet sind, können sich während der Vertragslaufzeit Änderungen bei der Einbindung von Unterauftragnehmern ergeben. Darüber ist die Einrichtung als Vertragspartner unverzüglich zu informieren.

Zu c): In der Regel bieten Cloud-Anbieter hierfür Informationsportale an. Es ist zu klären, wie die Einrichtung informiert wird. Insbesondere ob diese auch aktiv vom Cloud-Anbieter auf Änderungen hingewiesen wird (z. B. durch E-Mails).

Zu d): 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 NCD.2.2.01, Buchstabe j)) auch auf diese Unterauftragnehmer auszuweiten sind.

NCD.2.2.03 Gerichtsbarkeit

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie 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 C5:2020 vor, können diese Angaben der Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ 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:

- Deutschland,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat.

NCD.2.2.04 Lokation der Datenverarbeitung

a) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.

b) Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteanbieter mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.

Die Einrichtung 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,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat

genutzt werden.

Liegt ein Prüfbericht nach C5:2020 vor, können Angaben zu Datenlokationen des Cloud-Anbieters den Angaben zur Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden. Alternativ können dazu auch Informationen in den Verträgen oder Dienstegütevereinbarungen (Service Level Agreements) stehen.

NCD.2.2.05 Meldepflicht sicherheitsrelevanter Vorfälle

a) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.

ii) Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

Anmerkung: Der Titel der Anforderung enthält noch den Aspekt der Ermittlungsbefugnisse, da dieser in der Version 1.0 des Mindeststandards hier thematisiert wurde. Bei der Überarbeitung wurde der entsprechende Unterpunkt entfernt (einen Hinweis dazu befindet sich noch in Fußnote 23 des Mindeststandards), die Überschrift aber nicht angepasst. Dies wir bei der nächsten Aktualisierung des Mindeststandards korrigiert werden.

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

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

NCD.2.2.06 Beendigung des Vertragsverhältnisses

a) Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

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

NCD.2.2.07 Regelung der Datenrückgabe und Datenlöschung

a) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle).

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.

Zu a): Die Einrichtung 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.

Zu b): Für die Festlegung der Maßnahmen zur Datenlöschung und ggf. Datenmigration ist analog zu verfahren. Die hier festgelegten Regelungen sind für die Sicherheitsanforderungen NCD.2.4.01 und NCD.2.4.02 relevant (siehe Kapitel 2.4).

2.3 Einsatzphase

Die Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 Einbindung in das ISMS

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen für Cloud-Kunden[39] in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.

Zu a): Die Einrichtung 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 NCD.2.2.02) oder Meldungen von sicherheitsrelevanten Vorfällen (siehe NCD.2.2.05) in das ISMS der Einrichtung eingebunden werden können. Ziel sollte dabei sein, dass eine Verarbeitung der Informationen ohne Zeitverlust durch die zuständigen Verantwortlichen erfolgt.

NCD.2.3.02 Auswertung von Sicherheitsnachweisen

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[40]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

Zu a): Ist der Cloud-Anbieter vertraglich verpflichtet Nachweise zu erbringen (siehe NCD.2.2.01) muss die Einrichtung 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.

[39] Hinweis: Der C5 führt in Version 2020 mit den korrespondierenden Kriterien für Kunden bestimmte Mitwirkungspflichten des Cloud-Kunden ein. Der C5 hält Cloud-Diensteanbieter dazu an, diese Mitwirkungspflichten, abhängig von der Art des Cloud-Dienstes, zu definieren und in den C5-Prüfbericht als korrespondierende Kontrollen für Cloud-Kunden aufzunehmen. Es liegt im Verantwortungsbereich des Cloud-Kunden und damit der Einrichtung, den Mitwirkungspflichten entsprechende Kontrollen zu gestalten, einzurichten und durchzuführen. Dies ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Vgl. C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), S. 15.

[40] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“ (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020b).

Zu b): Sollten Unklarheiten nach Buchstabe a), ii) nicht auf andere Weise aufgeklärt werden können und die zugesicherten Prüf- und Kontrollrechte wahrgenommen werden, ist festzulegen, wie diese im konkreten Fall auszuüben sind.

NCD.2.3.03 Prüfung der Leistungsfähigkeit

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, vor dem Hintergrund der Nutzung des Cloud-Dienstes beurteilen.

b) Die Einrichtung MUSS ggf. auftretende Abweichungen bewerten und auf diese durch geeignete Anpassungen an der eigenen IT-Infrastruktur und Netzanbindung reagieren.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilen.[41]

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

NCD.2.3.04 Informationspflichten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

- einer Eingliederung des Cloud-Diensteanbieters in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihm,

- einem Austausch von Unterauftragnehmern oder Dritten (siehe hierzu auch NCD.2.2.02).

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

Zu b): Die Einrichtung muss festlegen, wie die Informationen des Cloud-Anbieters (z. B. zu den Anforderungen NCD.2.2.02 und NCD.2.2.05) innerhalb des eigenen ISMS weiterverarbeitet werden sollen.

NCD.2.3.05 Multi-Faktor-Authentisierung

a) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzern (Log-in) an, SOLLTE die Einrichtung diese nutzen.

b) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzern mit privilegierten Rechten (Log-in) wie bspw. zur Administration an, MUSS die Einrichtung diese nutzen.

[41] Hinweis: Viele Cloud-Diensteanbieter stellen für die Beurteilung ihrer Leistungsfähigkeit geeignete Information kontinuierlich (bspw. in Portalen oder auf Webseiten) bereit. Einrichtungen können basierend auf diesen sowie ggf. weiteren, selbst erhobenen Informationen die Leistungsfähigkeit von Cloud-Diensteanbietern kontinuierlich überwachen. Eine in geeigneter Weise durchgeführte kontinuierliche Überwachung kann die Basis für die geforderte, mindestens jährlich durchzuführende Bewertung der Leistungsfähigkeit eines Cloud-Diensteanbieters sein, aber sie nicht vollständig ersetzen.

2.4 Beendigungsphase

Im Falle der Beendigung der Nutzung eines Cloud-Dienstes, kommen die in der Betriebsphase geregelten Mechanismen zum Abschluss der Nutzungsphase zur Anwendung.

NCD.2.4.01 Datenrückgabe bei Beendigung

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

Einforderung und Umsetzung der festgelegten Regelungen zur Datenrückgabe. Die Regelungen ergeben sich aus dem jeweiligen Vertrag (siehe hierzu NCD.2.2.07).

NCD.2.4.02 Datenlöschung bei Beendigung

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.[42] Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern (z. B. Subdienstleistungsunternehmen) und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die durch den Cloud-Diensteanbieter bestätigte Datenlöschung dokumentieren.

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

2.5 Mitnutzung

Der Mindeststandard zur Nutzung externer Cloud-Dienste integriert in seiner nun vorliegenden Form auch den Mindeststandard des BSI zur Mitnutzung von externen Cloud-Diensten[43]. Die sogenannte Mitnutzung weicht von der Nutzung im Sinne dieses Mindeststandards ab, da zwischen der nutzenden Einrichtung und dem Cloud-Diensteanbieter für diese Dienstleistung kein eigenes Vertragsverhältnis besteht. Die dabei geltenden Sicherheitsanforderungen referenzieren die Anforderungen zur Nutzung externer Cloud-Dienste (Kapitel 2.1 bis 2.4), sofern dies geboten ist.

NCD.2.5.01 Mitnutzung externer Cloud-Dienste

a) Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) vereinbar ist.

b) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d bis i, umsetzen und einhalten.

c) Die Einrichtung MUSS ermitteln, an welchen Lokationen mit dem externen Cloud-Dienst dienstliche Daten verarbeitet werden. Dies schließt auch Datensicherungen sowie, sofern gegeben, Unterauftragnehmer und Subdienstleister des Cloud-Diensteanbieters ein.

[42] Hinweis: Neben Nutzdaten können auch Protokoll-/Transaktionsdaten zu löschen sein.
[43] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

i) Die Einrichtung MUSS bewerten, ob die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung sowie, sofern gegeben, weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) heranziehen.

d) Die Einrichtung MUSS ermitteln, welche Rechte an den dienstlichen Daten dem Cloud-Diensteanbieter oder Dritten durch das Akzeptieren der vom Cloud-Diensteanbieter vorgegebenen Allgemeinen Geschäftsbedingungen (AGB), Datenschutzerklärung oder sonstigen Nutzungsbedingungen eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit den eigenen Sicherheitsanforderungen, die sie in der Sicherheitsrichtlinie und dem eigenen Sicherheitskonzept definiert hat, vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

e) Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind. Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) abgleichen.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

f) Die Einrichtung MUSS erheben, wie und wann Daten durch den Cloud-Anbieter gelöscht werden (z.B. Löschfristen). Die Einrichtung MUSS dann bewerten, ob dies mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

g) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[44]

Zu c): Liegt ein Prüfbericht nach C5:2020 vor, können diese Angaben der Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

[44] Siehe MST MDM (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022b), S. 1ff.

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.

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.

Zu d): 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.

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.

Zu e): Es sollte 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.

Zu f): 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.

Zu f) i): 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.

Zu f) ii): 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 Risiken zu reduzieren oder zu vermeiden.

Literaturverzeichnis

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises. 2014. Orientierungshilfe – Cloud Computing, Version 2.0. [Online] Oktober 2014. [Zitat vom: 12. 01 2022.] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Orientierungshilfen/OHCloudComputing.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2016b. Anforderungskatalog Cloud Computing (C5). Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten. [Online] 2016b. [Zitat vom: 03. 02 2022.] https://www.bsi.bund.de/dok/452180.

—. 2017b. BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz. [Online] 2017b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/407502.

—. 2020a. Cloud Computing Compliance Criteria Catalogue – C5:2020. Kriterienkatalog Cloud Computing. [Online] 2020a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/452204.

—. 2022c. IT-Grundschutz-Kompendium, Edition 2022. [Online] 2022c. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/128568.

—. 2020b. Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5. [Online] 2020b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/14020574.

—. 2022b. Mindeststandard des BSI für Mobile Device Management (Version 2.0 vom 05.09.2022). [Online] 2022b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/453264.

—. 2018. Mindeststandard des BSI zur Mitnutzung von externen Cloud-Diensten (Version 1.0 vom 20.06.2018). [Online] 2018. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/397100.

—. 2017a. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste (Version 1.0 vom 24.04.2017). [Online] 2017a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/397130.

—. 2022a. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste (Version 2.1 vom xx.xx.2022). [Online] 2022a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/452272.

—. 2016a. Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende. [Online] 2016a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/128914.

—. 2019. Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019. [Online] 2019. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/407450.

Bundesministerium des Innern (BMI). 2014. 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. [Online] 2014. [Zitat vom: 12. 01 2022.] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html.

Bundesministerium des Innern und für Heimat (BMI). 2018. Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018. [Online] 2018. [Zitat vom: 12. 01 2022.] https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm.

International Organization for Standardization (ISO). 2014. International Standard ISO/IEC 17788:2014. *Information technology — Cloud computing — Overview and vocabulary.* [Online] 2014. [Zitat vom: 12. 01 2022.] https://www.iso.org/standard/60544.html.

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue
CRM	Customer Relationship Management
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
FAQ	Frequently Asked Questions
IEC	International Electrotechnical Commission
ISB	Informationssicherheitsbeauftragte
ISO	International Standards Organization
IT	Informationstechnik
ITZBund	Informationstechnikzentrum Bund
IT-GS	IT-Grundschutz
IT-SiBe	IT-Sicherheitsbeauftragte
MCD	Mitnutzung externer Cloud-Dienste
MDM	Mobile Device Management
MST	Mindeststandard
NCD	Nutzung externer Cloud-Dienste
RFC	Request for Comments
SLA	Service Level Agreement
StGB	Strafgesetzbuch
UMH	Umsetzungshinweise
VS	Verschlusssache
VSA	Verschlusssachenanweisung
z. B.	zum Beispiel