Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 24.04.2017

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

Inhaltsverzeichnis

Vorwort

§ 8 Absatz 1 BSIG regelt die Befugnis des Bundesamtes für Sicherheit in der Informationstechnik (BSI), allgemeine Mindeststandards für die Sicherheit der Informationstechnik für Stellen des Bundes festzulegen. Mindeststandards können nach der Gesetzesbegründung etwa die IT-Grundschutz-Kataloge oder auch Prüfkriterien sein. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen.

Mindeststandards sind Vorgaben des BSI für die Stellen des Bundes. Allerdings kann das Bundesministerium des Innern (BMI) im Benehmen mit dem IT-Rat die dort formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes mit Ausnahme der in § 8 Absatz 1 Satz 4 BSIG[1] genannten als verbindlich erklären.

Über die Stellen des Bundes hinaus sind Mindeststandards nach § 8 Absatz 1 BSIG auch in der öffentlichen Verwaltung der Länder und Kommunen für den Einsatz von Informationstechnik und zur Sicherung kritischer Infrastrukturen von grundsätzlicher Bedeutung. Ziele, Anforderungen und Empfehlungen von Mindeststandards können dazu genutzt werden, eigene Sicherheitsanforderungen anzupassen oder zu überprüfen, auch bei der Erstellung von Leistungsbeschreibungen im Rahmen eigener Vergabeverfahren. Anbieter von Informationstechnik und IT-Dienstleister können Mindeststandards dazu nutzen, ihre angebotenen Produkte sicherer zu machen.

1 Dies sind Bundesgerichte, der Bundestag, Bundesrat, Bundespräsident und Bundesrechnungshof.

1 Beschreibung

Dieser Mindeststandard definiert Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. Diese Anforderungen sind einzuhalten, um ein Mindestmaß an Informationssicherheit beim Nutzen derartiger Dienste zu gewährleisten. Er richtet sich hinsichtlich seiner Umsetzung an IT-Verantwortliche, IT-Sicherheitsbeauftragte[2] und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen. Anbieter von Cloud-Diensten und andere interessierte Personen können diesen Mindeststandard zur Erhöhung der Informationssicherheit oder zum Abgleich ihrer Angebote heranziehen.

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. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[3]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden. Als Nutzung ist insbesondere die Beauftragung eines externen Cloud-Dienstes durch eine Stelle des Bundes selbst oder gemeinsam mit Anderen zu verstehen.

Dieser Mindeststandard setzt die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[4] Er gilt für alle Schutzbedarfskategorien.

2 Bzw. Informationssicherheitsbeauftragte
3 BSI (2017), https://www.bsi.bund.de/cloud
4 Vgl. BSI (2008), S.49f.

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Beschaffungs- (Kapitel 2.1), die Einsatz- (Kapitel 2.2) sowie die Beendigungsphase (Kapitel 2.3) von externen Cloud-Diensten. Diese sind einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden. Vor der Nutzung externer Cloud-Dienste ist zusätzlich zur Schutzbedarfsfeststellung aus dem IT-Grundschutz eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen.

In der Datenkategorisierung sind zusätzlich zum Schutzbedarf Geheim- und Datenschutzaspekte[5] sowie Personen- und Dienstgeheimnisse zu ermitteln.

Im Rahmen der Datenkategorisierung sind die Daten den nachfolgenden Kategorien zuzuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

Daten können den Kategorien 1, 2 oder 3 gleichzeitig angehören. Die Kategorisierung der Daten ist zu dokumentieren.

Die Risikoanalyse ist insbesondere vor dem Hintergrund aktueller Veröffentlichungen des BSI zu Cloud-Sicherheit vorzunehmen.[6] Die ermittelten Risiken für die Daten müssen betrachtet und bewertet werden. Auch auf Seiten der Stelle des Bundes können je nach Nutzungsszenario in allen Phasen der Cloud-Nutzung zusätzliche Maßnahmen erforderlich sein. Im Rahmen dieser Risikoanalyse sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen zu beteiligen.

2.1 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Anbieters.

2.1.1 Auswahl Cloud-Anbieter

Im Rahmen des Beschaffungsprozesses muss vom Bieter die Vorlage von Systembeschreibungen[7], Zertifizierungen sowie Prüfberichten und anderen Nachweisen gefordert werden. Bei einer vorliegenden Testierung nach C5[8] können die nachfolgend genannten Informationen aus der im Prüfbericht enthaltenen Systembeschreibung entnommen werden.

CD.01: Systembeschreibung und weitergehende Informationen fordern

Die Vorlage der Systembeschreibung des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. Sie muss die Vorgaben nach C5 erfüllen und ist insbesondere auf Mitwirkungspflichten 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 festzulegen.

5 Hinsichtlich Datenschutzaspekte siehe insbesondere AKTM (2011), S.1ff.
6 Siehe hierzu insbesondere „Anforderungskatalog Cloud Computing des BSI“ (Cloud Computing Compliance Controls Catalogue, kurz C5).
7 Beschreibung des Cloud-Dienste betreffenden internen Kontrollsystems (Systembeschreibung).
8 Vgl. BSI (2016), S.1ff.

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 und Risikoanalyse entsprechend berücksichtigt werden.

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.

2.1.2 Vertragliche Regelungen

Vertragliche Regelungen nehmen bei der sicheren Nutzung von externen Cloud-Diensten eine zentrale Rolle ein. Daher benennen und konkretisieren die aufgeführten Mindestanforderungen zu regelnde Vertragsbestandteile aus Sicht der Informationssicherheit. Die Erfüllung der nachfolgenden Mindestanforderungen ist im Rahmen der Leistungsbeschreibung möglichst als Ausschlusskriterium zu fordern.

CD.04: Sicherheitsnachweise vertraglich zusichern

Der Cloud-Anbieter muss regelmäßig Sicherheitsnachweise über

- die angemessene und wirksame Umsetzung der Basisanforderungen nach C5,
- die aktuelle Dokumentation der Systembeschreibung,
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

vorlegen.

Diese Sicherheitsnachweise sollten durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise 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.

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.

CD.06: Recht auf Prüfungen und Kontrollen vertraglich zusichern

Grundsätzlich müssen der Stelle des Bundes eigene Prüfrechte 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 nach C5 vorlegen kann, muss die Stelle des Bundes dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

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

Die Beteiligung von Unterauftragnehmern und anderen externen Dritten müssen vom Cloud-Anbieter vollständig in Art und Umfang benannt werden. Beabsichtigte Änderungen 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 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.

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.

CD.09: Lokation vertraglich zusichern

Sämtliche Lokationen, 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.

CD.10: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

Der Cloud-Anbieter muss zusichern, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse 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.[9]

CD.11: weitere rechtliche Vereinbarungen vertraglich zusichern

Pflichten des Cloud-Anbieters sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Stelle des Bundes zu melden, müssen vertraglich geregelt sein. Vertragsstrafen und Haftungsfragen 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.

CD.12: Beendigung des Vertragsverhältnisses regeln

Kündigungsfristen 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.

9 Vgl. BMI (2014), S.1

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.

2.2 Einsatzphase

Mindestanforderungen an den Cloud-Betrieb werden insbesondere durch die vertragliche Zusicherung der angemessenen und wirksamen Umsetzung des C5 (siehe Kapitel 2.1) aufgestellt. Sie adressieren primär den jeweiligen Cloud-Anbieter und gewährleisten damit einen sicheren Betrieb während der Vertragslaufzeit. Mindestanforderungen an den Einsatz von Cloud-Diensten regeln hingegen, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden können. Hierfür müssen Sicherheitsnachweise eingefordert und Informationspflichten des Cloud-Anbieters nachgehalten werden. Dies soll gewährleisten, dass die Stelle des Bundes die Risiken für ihre Informationssicherheit durch eigene Prüfungen, Auswertungen von Prüfberichten und sonstige vertraglich zur Verfügung gestellte Informationen des Cloud-Anbieters im Rahmen ihres Informationssicherheits-Management-Systems (ISMS) steuern kann.

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.

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.

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.

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.

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.[10]

10 für den standardisierten und vereinfachten Austausch siehe https:// www.bsi.bund.de

2.3 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die ordnungsgemäße Abwicklung des Vertragsverhältnisses. Dies ist in der Regel nur möglich, wenn bereits bei Vertragsschluss alle relevanten Themen zum Vertragsende geregelt wurden. Daher umfasst bereits die Beschaffungsphase (Kapitel 2.1) entsprechende Mindestanforderungen zu diesem Bereich.

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.

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.

Literaturverzeichnis

AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, 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

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, Version 2.0, Bonn 2008

BSI (2016) Bundesamt für Sicherheit in der Informationstechnik: Anforderungskatalog Cloud Computing – Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten, Version 1.0 – Stand Februar 2016

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik; Cloud Computing Grundlagen; https://www.bsi.bund.de/cloud, abgerufen am 10.03.2107

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C5	Anforderungskatalog Cloud Computing des BSI (engl. Titel: Cloud Computing Compliance Controls Catalog)
ISMS	Informationssicherheits-Management-System
StGB	Strafgesetzbuch
VSA	Verschlusssachen gem. allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen