Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Mitnutzung von externen Cloud-Diensten

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 20.06.2018

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

Inhaltsverzeichnis

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs.1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[3] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Analog „Informationssicherheitsbeauftragte (ISB)“
[2] Zur standardisierten Vorgehensweise siehe https://www.bsi.bund.de/mindeststandards
[3] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Behörde“ verwendet.

1 Beschreibung

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. Angeboten werden insbesondere Infrastrukturen, Plattformen und Software, jedoch umfasst die Spannbreite das vollständige Spektrum der Informationstechnik.[4]

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.

Dieser Mindeststandard grenzt zwischen Nutzung und Mitnutzung von externen Cloud-Diensten ab. Beauftragt eine Behörde einen externen Cloud-Dienst selbst oder gemeinsam mit anderen wird von einer Nutzung ausgegangen, wobei zwischen Cloud-Anbieter und nutzender Behörde ein Vertragsverhältnis besteht. Dieser Anwendungsfall ist mit dem Mindeststandard des BSI zur Nutzung externer Cloud-Dienste bereits geregelt.[5] Nehmen hingegen ein oder mehrere IT-Anwender einer Behörde einen externen Cloud-Dienst in Anspruch, ohne dass zwischen mitnutzender Behörde und Cloud-Anbieter ein Vertragsverhältnis besteht, wird von einer Mitnutzung ausgegangen. Für diesen Anwendungsfall setzen die in Kapitel 2 beschriebenen Bewertungskriterien und Sicherheitsanforderungen ein definiertes Sicherheitsniveau, das aus Sicht des BSI nicht unterschritten werden darf.

Der Mindeststandard setzt in seiner Methodik die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[6] Er gilt für alle Schutzbedarfskategorien. Im Rahmen des Informationssicherheitsmanagements ist somit zu bewerten, ob die Mitnutzung des externen Cloud-Dienstes die eigenen Sicherheitsanforderungen erfüllt. Ziel ist es, dass die mitnutzende Behörde abhängig vom Schutzbedarf der zu verarbeitenden Daten anhand der in Kapitel 2.1 formulierten Bewertungskriterien bewusste Entscheidungen für oder gegen eine Mitnutzung trifft.

Kommt die mitnutzende Behörde zu dem Ergebnis, dass der externe Cloud-Dienst künftig in Anspruch genommen werden kann, sind seitens der IT-Anwender der mitnutzenden Behörde mindestens die Sicherheitsanforderungen aus Kapitel 2.2 zu beachten.

[4] Siehe hierzu auch die entsprechenden Konkretisierungen unter https://www.bsi.bund.de/cloud.
[5] Vgl. BSI (2017a), S. 1 ff.
[6] Vgl. BSI (2017d), S. 1 ff.

2 Sicherheitsanforderungen

Nachfolgende Vorgaben adressieren die Mitnutzung von externen Cloud-Diensten (siehe Kapitel 1). Diese sind nach der Auffassung des BSI einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden.

2.1 Bewertung externer Cloud-Dienste

Im Rahmen des Informationssicherheitsmanagements ist vor Mitnutzung zusätzlich zur Schutzbedarfsfeststellung aus dem IT-Grundschutz eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen. Diese sind zwingend erforderlich, da eine Entscheidung über die künftige Mitnutzung des externen Cloud-Dienstes im Wesentlichen auf diesen Ergebnissen basiert. Im Rahmen der Risikoanalyse und Datenkategorisierung sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragten zu beteiligen.[7]

In der Risikoanalyse und Datenkategorisierung sind zusätzlich zum Schutzbedarf, Geheim- und Datenschutzaspekte[8] sowie Personen- und Dienstgeheimnisse zu ermitteln. Die Daten sind im Rahmen der Datenkategorisierung den nachfolgenden Kategorien zuzuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO[9]
- Kategorie 3 = Verschlusssachen gemäß dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (SÜG)
- 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 nachvollziehbar zu dokumentieren. Regelungen aus den allgemeinen Verwaltungsvorschriften zum materiellen und organisatorischen Schutz von Verschlusssachen (§ 35 SÜG) und den Datenschutzgesetzen bleiben vom Mindeststandard unberührt.
Die Verantwortung für die Gewährleistung der Informationssicherheit trägt die Leitung einer Behörde als Teil der allgemeinen Leitungsverantwortung.[10] Somit entscheidet die jeweilige Hausleitung über die letztendliche Mitnutzung von externen Cloud-Diensten. Werden im Rahmen der Mitnutzung ausnahmslos Daten der Kategorie 4 verarbeitet[11], kann die Hausleitung die Entscheidung über eine Inanspruchnahme auch dem IT-SiBe übertragen.
Die Risikoanalyse ist insbesondere vor dem Hintergrund aktueller Veröffentlichungen des BSI zu Cloud-Sicherheit vorzunehmen.[12] Die ermittelten Risiken für die Daten müssen betrachtet und bewertet werden. Auch auf Seiten der mitnutzenden Behörde können zusätzliche Maßnahmen erforderlich sein, um den ermittelten Risiken entgegenzuwirken.
Für die Bewertung im Rahmen des Informationssicherheitsmanagements (siehe Kapitel 1) werden Informationen über den Cloud-Anbieter und externen Cloud-Dienst benötigt. Die nachfolgenden Bewertungskriterien geben vor, welche Informationen von der mitnutzenden Behörde hierfür heranzuziehen sind und wie eine anschließende Bewertung zu erfolgen hat.

[7] Im Rahmen des § 8 Abs.1 BSIG berät und unterstützt das BSI auf Anfrage.
[8] Hinsichtlich Datenschutzaspekte siehe insbesondere AKTM (2014), S. 1 ff.
[9] Ab dem 25.05.2018 ist die DSGVO anzuwenden.
[10] Vgl. BMI (2017), S. 8.
[11] „Verarbeiten von Daten“ i. S. d. Mindeststandards ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten.
[12] Siehe hierzu insbesondere BSI (2016), „Anforderungskatalog Cloud Computing des BSI“ (Cloud Computing Compliance Controls Catalogue, kurz C5).

Da die mitnutzende Behörde nicht selbst Auftraggeber ist, muss zunächst geklärt werden, wer mit dem externen Cloud-Anbieter ein Vertragsverhältnis eingegangen ist. Von dem Auftraggeber[13] oder aus anderen verlässlichen Quellen sind dem IT-SiBe Informationen zum Vertrag und zur Sicherheitskonzeption der Cloud-Nutzung vorzulegen.
Können einzelne Informationen nicht bezogen werden, ist dies zu dokumentieren und unter Berücksichtigung der Ergebnisse aus der Datenkategorisierung entsprechend zu bewerten.
Auf dieser Basis hat der IT-SiBe der mitsnutzenden Behörde die nachfolgenden Bewertungen durchzuführen.[14]

MCD.2.1.01: Anwendbares Recht, Gerichtsstand

Es ist zu ermitteln, unter welchem Recht die Vereinbarung zwischen der nutzenden Institution und dem Cloud-Anbieter unterliegt und unter welchem Gerichtsstand sie steht. Es ist zu bewerten, ob Vereinbarungen, die nicht deutschem Recht folgen und keinen deutschen Gerichtsstand vorsehen, von der mitnutzenden Behörde unter Berücksichtigung der Ergebnisse der Datenkategorisierung und Risikoanalyse akzeptiert werden können. Dies ist grundsätzlich gegeben, wenn ausschließlich Daten der Kategorie 4 verarbeitet werden sollen.

MCD.2.1.02: Offenbarungspflichten und Ermittlungsbefugnisse

Es ist zu ermitteln, ob und unter welchen fremdstaatlichen Offenbarungspflichten und Ermittlungsbefugnissen der Cloud-Anbieter steht. Es ist zu bewerten, ob Risiken durch mögliche Informationsabflüsse dieser Art akzeptiert werden können. Diese sind im Regelfall nicht zu akzeptieren, wenn Daten der Kategorie 3 verarbeitet werden sollen.

MCD.2.1.03: Datenlokationen

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

MCD.2.1.04: Nutzung und Weitergabe von Daten an Dritte

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

MCD.2.1.05: Verfügbarkeit der Daten

Es ist zu ermitteln, welche verbindlichen Zusagen hinsichtlich der Verfügbarkeit des Cloud-Dienstes existieren. Es ist zu bewerten, ob aus Sicht der mitnutzenden Behörde die zugesicherte Verfügbarkeit ausreichend ist. Für die Bewertung können insbesondere die Regelungen zur Anwendung des HV-Benchmark kompakt[15] herangezogen werden.
Die Verfügbarkeit von Daten ist auch von der eigenen IT-Infrastruktur abhängig. Die Behörde muss daher mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performanz der Netzanbindung und -verbindungen, überprüfen und ggf. anpassen.

MCD.2.1.06: Verschlüsselung der Datenübertragung

Es ist zu ermitteln, ob die Daten über einen sicheren Kanal übertragen werden. Hierfür muss die Stärke der Schlüssel (Schlüssellänge und -verfahren) den IT-Sicherheitsrichtlinien der mitnutzenden Behörde

[13] Hinweis: Handelt es sich bei dem Auftraggeber um eine Behörde, so findet dort der Mindeststandard zur Nutzung externer Cloud-Dienste Anwendung.
[14] Für die Bewertung können andere Fachbereiche der Behörde hinzugezogen werden (z. B. Datenschutzbeauftragte, Justiziariat, u. a.).
[15] Vgl. BSI (2018), S. 1 ff.

entsprechen. Liegt dem sicheren Kanal eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls[16] genügen. Wird eine VPN-Verbindung genutzt, muss diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der mitnutzenden Behörde entsprechen.

MCD.2.1.07: Verschlüsselung der Daten

Es ist zu ermitteln, wie die Daten vom Cloud-Anbieter verschlüsselt gespeichert werden. Es ist zu bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung und Risikoanalyse vereinbar sind.[17] Ist die vom Cloud-Anbieter eingesetzte Verschlüsselung nicht geeignet, ist zu prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

MCD.2.1.08: Erforderliche Softwareinstallationen

Es ist zu ermitteln, ob für die Mitnutzung auf Arbeitsplatzcomputern oder mobilen Endgeräten der IT-Anwender zusätzliche Softwareinstallationen erforderlich sind. Es ist zu bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitsrichtlinie der mitnutzenden Behörde vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.
Ist ein Zugriff über mobile Endgeräte geplant, sind diese zentral zu verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[18]

MCD.2.1.09: Berechtigungsvergabe

Es ist zu ermitteln, wie die Berechtigungsvergabe erfolgt. In diesem Zusammenhang ist insbesondere zu bewerten, ob die Berechtigungsvergabe dem Berechtigungskonzept der mitnutzenden Behörde genügt.

MCD.2.1.10: Kündigungsfristen

Es ist zu ermitteln, welche Kündigungsfristen Auftraggeber und Cloud-Anbieter vereinbart haben. Es ist zu bewerten, ob die vereinbarten Kündigungsfristen mit dem Einsatzszenario der mitnutzenden Behörde vereinbar sind. Kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte von Leistungen sind stets kritisch zu hinterfragen.

MCD.2.1.11: Datenrückgabe und Datenlöschung

Es ist zu ermitteln, welche Vereinbarungen zwischen Auftraggeber und Cloud-Anbieter zur Datenrückgabe und -löschung existieren und ob diese auch für die mitnutzende Behörde gelten. Lock-In-Effekte sind zu vermeiden, daher ist zu prüfen, ob der externe Cloud-Anbieter einen Datenexport in einem marktgängigen Datenformat anbietet.
Es ist zu bewerten, ob die Rechte und Maßnahmen zur Datenrückgabe und -löschung mit den Ergebnissen der Datenkategorisierung und Risikoanalyse sowie den gesetzlichen Anforderungen vereinbar sind.

MCD.2.1.12: Informationsaustausch

Die mitnutzende Behörde informiert das BSI über die Mitnutzung von externen Cloud-Diensten jährlich zum Stichtag 31. Januar. Diese Informationen umfassen auch Beendigung und Wechsel. Hierfür ist das dafür vorgesehene Formblatt zu verwenden.[19]

2.2 Sichere Mitnutzung externer Cloud-Dienste

Nachfolgende Sicherheitsanforderungen regeln eine sichere Mitnutzung des externen Cloud-Dienstes durch IT-Anwender der mitnutzenden Behörde.

[16] Vgl. BSI (2014), S. 1.
[17] Die eingesetzte Verschlüsselung sollte der Basisanforderung „KRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung" gem. BSI (2016), S. 63 entsprechen.
[18] Vgl. BSI (2017b), S. 1 ff.
[19] Das Formblatt wird auf den Webseiten des BSI zur Verfügung gestellt.

MCD.2.2.01: Mindestanforderung an Kennwörter

Für den Kennwortgebrauch sind die verbindlichen Regeln der mitnutzenden Behörde zu beachten.[20] Unter Berücksichtigung der Ergebnisse aus Datenkategorisierung und Risikoanalyse muss für die Authentisierung am externen Cloud-Dienst ausreichend starke Kennwörter (oder alternative Verfahren, die mindestens ein vergleichbares Sicherheitsniveau gewährleisten) genutzt werden. Diese müssen insbesondere gegenüber Brute-Force-Angriffen hinreichend stark sein.

MCD.2.2.02: Umgang mit Benutzernamen und Kennwörtern

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

MCD.2.2.03: Mitteilungen bei Änderungen

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

[20] Siehe BSI (2017c), S. 142 - „ORP.4.A8 - Regelung des Passwortgebrauchs“.

Literaturverzeichnis

AKTM (2014) 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 (2017) Bundesministerium des Innern, Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung, Berlin 2017

BSI (2014) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden – Version 1.0 vom 21.11.2014

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, Bonn

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Abs.1 S.1 BSIG – Version 1.0 vom 24.04.2017

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management nach § 8 Abs.1 S.1 BSIG – Version 1.0 vom 11.05.2017

BSI (2017c) Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, Final Draft, Bonn 2017

BSI (2017d) Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, Bonn 2017

BSI (2018) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0 nach § 8 Abs.1 S.1 BSIG – Version 1.1 vom 19.06.2018

Abkürzungsverzeichnis

AKTM	Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises
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)
DSGVO	Datenschutz-Grundverordnung
IT-SiBe	IT-Sicherheitsbeauftragter
ISB	Informationssicherheitsbeauftragter
SSL	Secure Sockets Layer (engl.)
StGB	Strafgesetzbuch
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz)
TLS	Transport Layer Security (engl.)
VPN	Virtual Private Network