Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Mitnutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Entwurf Beta 0.50 vom 13.09.2017

Änderungshistorie

Version	Datum	Name	Beschreibung
0.10	02.06.2017	Zobel	Rohentwurf auf Basis des Interviews mit B34
0.20	24.07.2017	Grete / Zobel	Freigabe durch B34 zur hausinternen Abstimmung
0.30	08.08.2017	Zobel	Änderungen der hausinternen Abstimmung sichtbar eingearbeitet
0.33	24.08.2017	Grete / Zobel	Bewertung und Einarbeitung der Ergebnisse aus hausinterner Abstimmung
0.41	07.09.2017	Zobel	Alpha-Entwurf zum Konsultationsverfahren der Ressorts

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.

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.[1] 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[2] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Zur standardisierten Vorgehensweise siehe BSI (2017), https://www.bsi.bund.de/mindeststandards
[2] 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.[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.

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[4] bereits geregelt. 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 Sicherheitsanforderungen ein definiertes Sicherheitsniveau, das aus Sicht des BSI nicht unterschritten werden darf. Der Mindeststandard richtet sich an IT-Verantwortliche, IT-Sicherheitsbeauftragte[5] und IT-Anwender.

Der für die mitnutzende Behörde zuständige IT-Sicherheitsbeauftragte hat vor der Mitnutzung zu überprüfen, ob der externe Cloud-Dienst die eigenen Sicherheitsanforderungen erfüllt. Hierfür setzt der Mindeststandard in Kapitel 2.1 entsprechende Mindestanforderungen. Kommt die mitnutzende Behörde zu dem Ergebnis, dass der externe Cloud-Dienst künftig in Anspruch genommen werden kann, haben die IT-Anwender der mitnutzenden Behörde die Mindestanforderungen aus Kapitel 2.2 einzuhalten.

Der Mindeststandard setzt in seiner Methodik die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[6] Er gilt für alle Schutzbedarfskategorien.

[3] Vgl. BSI (2017a), https://www.bsi.bund.de/cloud
[4] Vgl. BSI (2017b), S.1ff.
[5] Analog „Informationssicherheitsbeauftragte“
[6] Vgl. BSI (2008), S.49f.

2 Sicherheitsanforderungen

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

2.1 Bewertung externer Cloud-Dienste

Vor der Mitnutzung ist 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 sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragten zu beteiligen.

In der Datenkategorisierung sind zusätzlich zum Schutzbedarf, Geheim- und Datenschutzaspekte[7] sowie Personen- und Dienstgeheimnisse zu ermitteln. Die Daten sind daher 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 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.

Über die Inanspruchnahme von externen Cloud-Diensten entscheidet die jeweilige Hausleitung der mitnutzenden Institution. Werden lediglich Daten der Kategorie 4 verarbeitet[8], kann die Hausleitung die Entscheidung über eine Inanspruchnahme auch dem IT-Sicherheitsbeauftragten übertragen.

Die Risikoanalyse ist insbesondere vor dem Hintergrund aktueller Veröffentlichungen des BSI zu Cloud-Sicherheit vorzunehmen.[9] 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 weitere Bewertung werden Informationen über den Cloud-Anbieter und externen Cloud-Dienst benötigt. Die nachfolgenden Mindestanforderungen geben vor, welche Informationen von der mitnutzenden Behörde zu ermitteln sind und wie eine anschließende Bewertung zu erfolgen hat.

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 oder aus anderen verlässlichen Quellen sind durch den IT-Sicherheitsbeauftragten Informationen zum Vertrag und zur Sicherheitskonzeption der Cloud-Nutzung zu beschaffen.

Auf dieser Basis hat der IT-Sicherheitsbeauftragte der mitnutzenden Behörde die nachfolgenden Sicherheitsanforderungen zu beachten.

[7] Hinsichtlich Datenschutzaspekte siehe insbesondere AKTM (2011), S.1ff.

[8] „Verarbeiten von Daten“ i. S. d. Mindeststandards ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten

[9] Siehe hierzu insbesondere BSI (2016), „Anforderungskatalog Cloud Computing des BSI“ (Cloud Computing Compliance Controls Catalogue, kurz C5)

MCD.01: Gerichtsbarkeit

Es ist zu ermitteln, unter welchem Gerichtsstand die Vereinbarung zwischen der nutzenden Institution und dem Cloud-Anbieter steht. Es ist zu bewerten, ob Vereinbarungen, die nicht deutschem Recht folgen, keinen deutschen Gerichtsstand und kein obligatorisch vorab zu betreibendes Streitschlichtungsverfahren 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.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 grundsätzlich nicht zu akzeptieren, wenn Daten der Kategorien 1, 2 oder 3 verarbeitet werden sollen.

MCD.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.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, vertraglich vorgesehenen Leistungserbringung genutzt werden können, sind grundsätzlich nicht zu akzeptieren.

MCD.05: Verfügbarkeit der Daten

Es ist zu ermitteln, welche vertraglichen 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 3.0[10] herangezogen werden.

MCD.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 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[11] genügen. Wird eine VPN-Verbindung genutzt, muss diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der mitnutzenden Behörde entsprechen.

MCD.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.[12] 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.

[10] Vgl. BSI (2017c), S.1

[11] Vgl. BSI (2015), S.1

[12] Die eingesetzte Verschlüsselung sollte der Basisanforderung „KRY-03 "Verschlüsselung von sensiblen Daten bei der Speicherung" gem. BSI (2016), S.63 entsprechen.

MCD.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.[13]

MCD.09: 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.10: 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. Es ist zu bewerten, ob diese Rechte und Maßnahmen zur Datenrückgabe und -löschung mit den Ergebnissen der Datenkategorisierung und Risikoanalyse sowie den gesetzlichen Anforderungen vereinbar sind.

MCD.11: 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.[14]

2.2 Sichere Mitnutzung von externen Cloud-Diensten

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

MCD.12: Mindestanforderung an Passwörter

Für den Zugriff auf externe Cloud-Dienste haben Passwörter folgende Mindestvorgaben zu erfüllen:[15]

1. Das Passwort setzt sich aus mindestens acht Zeichen zusammen.
2. Das Passwort setzt sich aus einer Kombination von Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern zusammen. Hierbei sind mindestens zwei Anforderungen umzusetzen.
3. Steht eine Zwei-Faktor-Authentifizierung zur Verfügung, ist diese zu nutzen.
4. Das Kennwort wird vom IT-Anwender weder bereits noch in Zukunft für andere Dienste oder Logins verwendet.

MCD13: Umgang mit Benutzernamen und Passwörtern

Benutzername und Passwort sind zu schützen und dürfen nur dem jeweiligen IT-Anwender bekannt sein. Auch auf mobilen Endgeräten sind Benutzername und Passwort nicht ungeschützt zu speichern.

Werden Benutzernamen und Passwörter von mehreren IT-Anwendern genutzt (sog. Account Sharing), ist hierfür die Genehmigung des zuständigen IT-Sicherheitsbeauftragten einzuholen. Grundsätzlich ist Account Sharing zu vermeiden und nur in begründeten Einzelfällen möglich.

[13] Vgl. BSI (2017b), S.1ff

[14] Das Formblatt wird auf den Webseiten des BSI zur Verfügung gestellt.

[15] Diese Vorgaben sind als Mindestanforderungen zu verstehen, die nicht zu unterschreiten sind. Generelle Hinweise siehe auch BSI (2016a), S. 1520f. - M.211 „Regelung des Passwortgebrauchs“.
Bei der Verwendung von Einmal-Passwörtern kann von diesen Vorgaben abgewichen werden.

MCD14: Mitteilungen bei Änderungen

Werden Änderungen der Mitnutzung bekannt, sind diese unverzüglich dem zuständigen IT-Sicherheitsbeauftragten mitzuteilen. Dies gilt auch bei Beendigung der Mitnutzung.

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

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

BSI (2015) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden 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 (2016a) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, 15. Ergänzungslieferung – 2016, Bonn

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik; Mindeststandards – Standardisierte Vorgehensweise; https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Standardisierte_Vorgehensweise/Standardisierte_Vorgehensweise_node.html, abgerufen am 20.07.2017

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik; Cloud Computing Grundlagen; https://www.bsi.bund.de/cloud, abgerufen am 20.07.2107

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

BSI (2017c) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 3.0 nach § 8 Abs. 1 S. 1 BSIG – Version 1.0 vom 26.05.2017

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)
MDM	Mobile Device Management
SSL	Secure Sockets Layer (engl.)
StGB	Strafgesetzbuch
TLS	Transport Layer Security (engl.)
VPN	Virtual Private Network
VSA	Verschlusssachen gem. allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen