Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter

Stand 27.09.2010

ENTWURF

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

Inhaltsverzeichnis

0 Definition Cloud Computing

0.1 Was ist Cloud Computing?

Cloud Computing ist ein IT-Angebot, das es ermöglicht, eine oder mehrere IT-Dienstleistungen wie Rechenleistung, Hintergrundspeicher, Entwicklungsumgebungen, Anwendungssoftware oder sogar komplette Arbeitsumgebungen

- jederzeit,
- netzbasiert,
- schnell und dem tatsächlichen Bedarf angepasst
- sowie nach tatsächlicher Nutzung abrechenbar

zu beziehen.

0.2 Was unterscheidet eine Public Cloud von einer Private Cloud?

- In einer **Public Cloud** können die angebotenen Services von jedermann genutzt werden.
- Von einer **Private Cloud** spricht man, wenn sowohl die Services als auch die Infrastruktur einer Institution unterstehen und von ihr exklusiv genutzt werden.
- Werden aus einer Private Cloud heraus, Dienste einer Public Cloud genutzt, so spricht man von einer **Hybrid Cloud**.

0.3 Welche verschiedenen Services werden im Cloud Computing angeboten?

Grundsätzlich unterscheidet man drei verschiedene Kategorien von Cloud Services:

1. **Infrastructure-as-a-Service (IaaS)**
   Vereinfacht gesagt, werden bei IaaS Hardwarekomponenten (Infrastructure) als ein Service angeboten, wie z. B. Speicherplatz, CPU, Netze.
2. **Platform-as-a-Service (PaaS)**
   Ein PaaS-Provider stellt Software-Entwicklern eine Laufzeit und ggf. Entwicklungsumgebung zur Verfügung, die genutzt werden kann, um Applikationen auf der Plattform zu entwickeln und auszuführen. Vorteilhaft in diesem Zusammenhang ist die Tatsache, dass viele Funktionalitäten wie beispielsweise Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe von der Plattform bereitgestellt werden.
3. **Software-as-a-Service (SaaS)**
   Sämtliche Angebote von Programmen, die den Kriterien des Cloud Computing entsprechen

fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt und als Beispiele seien das Kontaktdatenmanagement, Finanzbuchhaltung oder Kollaborationsanwendungen genannt.

0.4 Was unterscheidet Cloud Computing von klassischem IT-Outsourcing?

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Das Auslagern von Geschäfts- und Produktionsprozessen ist ein etablierter Bestandteil heutiger Organisationsstrategien.

Die Nutzung von Cloud Services gleicht in vielem dem klassischen Outsourcing, aber es kommen noch einige Unterschiede hinzu, die zu berücksichtigen sind.

- Cloud Services sind dynamisch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. So können Cloud-basierte Angebote rascher an den tatsächlichen Bedarf angepasst werden.
- Die Steuerung der in Anspruch genommenen Cloud-Dienste erfolgt in der Regel mittels einer Webschnittstelle durch den Cloud-Nutzer selbst. So kann der Nutzer automatisiert die genutzten Dienste auf seine Bedürfnisse zuschneiden.
- Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte, die ggf. in In- und Ausland sind, zu verteilen.
- Aus wirtschaftlichen Gründen teilen sich in einer Public Cloud mehrere Nutzer eine gemeinsame Infrastruktur. Bei IaaS beispielsweise kann es also vorkommen, dass sich mehrere virtuelle Maschinen eine physische CPU teilen müssen.

0.5 Geltungsbereich der BSI-Mindestanforderungen

- Betrachtet wird die Cloud-basierte Verarbeitung von Informationen, deren Vertraulichkeitsbedarf einen normalen bis hohen Schutzbedarf entspricht (z. B. firmenvertrauliche Informationen, schützenswerte personenbezogene Daten). Informationen mit einer Einstufung als Verschlusssache werden nicht betrachtet. Die Kategorisierung der Daten bzgl. ihres Schutzbedarfs folgt den Hinweisen des BSI-Standards 100-2.
- Der Verfügbarkeitsanspruch der in Anspruch genommenen Dienstleistungen liegt im normalen bis hohen Bedarfsbereich.
- Die aufgeführten Anforderungen werden drei Kategorien zugeordnet:
    - Die **Kategorie B** (=Basisanforderung) umfasst die Basisanforderungen, die an jeden Cloud-Anbieter gestellt werden.

    - Die **Kategorie Vt+** (=Vertraulichkeit hoch) umfasst zusätzliche Anforderungen, die vom Cloud-Anbieter realisiert werden müssen, wenn Daten mit einem Vertraulichkeitsbedarf hoch verarbeitet werden sollen.
    - Die **Kategorie Vf+** (=Verfügbarkeit hoch) umfasst zusätzliche Anforderungen, die vom Cloud-Anbieter realisiert werden müssen, wenn Dienstleistungen mit einem Verfügbarkeitsbedarf hoch in Anspruch genommen werden sollen.
- Die Anforderungen gelten für IaaS, PaaS und SaaS soweit nicht anders vermerkt.
- Aufgrund der Dynamik der Cloud-Entwicklung ist eine periodische Überprüfung der nachfolgend dargestellten Mindestanforderungen (ggf. mit Aufnahme zusätzlicher Anforderungen) notwendig.

1 Sicherheitsmanagement beim Anbieter

Für eine reibungslose Bereitstellung und Nutzung von Cloud-Diensten sind die internen Prozesse zur Umsetzung der Sicherheit in der Cloud unverzichtbar. Daher müssen Betreiber von Cloud-Computing-Plattformen ein wirksames ISMS (Information Security Management System) wie beispielsweise nach ISO 27001 oder bevorzugt IT-Grundschutz auf Basis von ISO 27001 umsetzen.

Sicherheitsmanagement beim Anbieter	B	Vt+	Vf+
Definiertes Vorgehensmodell aller IT-Prozesse (z. B. nach ITIL, COBIT)	✓		
Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. BSI-Standard 100-2 (IT-Grundschutz), ISO 27001)	✓		
Erstellung eines IT-Sicherheitskonzeptes für die Cloud	✓		

2 Sicherheitsarchitektur

Jeder Cloud-Anbieter muss eine durchgängige Sicherheitsarchitektur (infrastrukturelle und technische Aspekte, Systemkomponenten) konzipieren und implementieren, um seine Ressourcen (Gebäude, Netze, Systeme, Anwendungen, Daten, etc.) sowie die Anwendungen und Daten seiner Kunden zu schützen.

Cloud-Computing-Plattformen müssen mandantenfähig (multi-tenancy) sein und eine verlässliche Trennung der Mandanten gewährleisten. Dies gilt gleichermaßen sowohl für Private Clouds (z. B. Trennung der Daten der Finanzbuchhaltung von denen der Personalabteilung) als auch für Public Clouds (da hier sich unbekannte Nutzer den selben Service nutzen) und stellt einen Schlüsselaspekt der Cloud-Sicherheit dar.

Rechenzentrumsicherheit	B	Vt+	Vf+
Redundante Auslegung aller wichtigen Versorgungs-Komponenten (Strom, Klimatisierung der RZ, Internetanbindung, etc.)	✓		
24/7 Überwachung des Zugangs, inkl. Videoüberwachungssysteme, Brandmelder, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.	✓		
Kontrollierte Zugangskontrolle für das Rechenzentrum	✓		
Zwei redundante Rechenzentren, die mindestens so weit von einander entfernt sind, dass eine Katastrophe (z. B. Explosion, Feuer) in einem Rechenzentrum, das andere nicht beeinträchtigt.			✓

Netzsicherheit	B	Vt+	Vf+
Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, SPAM-Schutz, etc.)	✓		
Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, etc.)	✓		
DDoS-Mitigation (Abwehr von DDoS-Angriffen)	✓		
Fernadministration durch einen sicheren Kommunikationskanal (SSH, SSL, IPSec, VPN, etc.)	✓		
Gewährleistung der hohen Verfügbarkeit bei den Verbindungen zwischen den Rechenzentren der Cloud und zum Nutzer; physisch und logisch redundante Anbindung der Cloud-Standorte und der Nutzer			✓

Host- und Servervirtualisierung	B	Vt+	Vf+
Technische Maßnahmen zum Schutz des Hosts (Host-based Intrusion Detection System, Host Firewalls, regelmäßige Integritätsüberprüfungen, etc.) und des Hypervisors	✓		
Sichere Default-Konfiguration des Hosts (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)	✓		
Veröffentlichte Benutzer-Richtlinien zur Absicherung von virtuellen Maschinen (nur IaaS)	✓		
Möglichkeit kundeneigene Images für virtuelle Maschinen einzusetzen und qualitätsgesicherte Images zur Verfügung stellen (nur IaaS)	✓		
Multifaktor-Authentisierung für den Zugriff auf die Virtuelle Maschine (nur IaaS)		✓	✓
Soweit einsetzbar und verfügbar: Einsatz zertifizierter Hypervisoren (Common Criteria mind. EAL 4)		✓	✓

Anwendungs- und Plattformsicherheit	B	Vt+	Vf+
Sicherheit muss Bestandteil des Software Development Life Cycle-Prozesses sein (Reviews, Automatisierte Tests, Vulnerability Tests, etc.)	✓		
Sichere Isolierung und Kapselung der Anwendungen	✓		
Richtlinien für Kunden zur Erstellung von sicheren Anwendungen (nur PaaS)	✓		

Ressourcen- und Patchmanagement	B	Vt+	Vf+
Konfigurationsmanagement	✓		
Sichere Provisionierung und Deprovisionierung von Ressourcen	✓		
Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service Packs) sowie Release Management	✓		
Sicherstellung der Patchverträglichkeit auf Testssystem vor Einspielen in Wirkbetrieb	✓		

Datenspeicherung, Speichervirtualisierung und Datensicherheit	B	Vt+	Vf+
Datensicherheit im Lebenszyklus der Daten definieren und umsetzen	✓		
Sichere Isolierung der Kundendaten (virtuelle Speicherbereiche, Tagging, etc.)	✓		
Regelmäßige Datensicherung und Möglichkeit der Datenwiederherstellung (außer nach Löschung) muss gesichert sein (z. B. redundante Replikate, evtl. auch Kundentests)	✓		
Datenarchivierung nach einschlägigen Gesetzen bzw. Bestimmungen	✓		
Daten bei deren Vernichtung komplett und unwiderruflich löschen (sicheres Löschen)	✓		
Option der verschlüsselten Speicherung sensitiver Daten unter vollständiger Schlüsselkontrolle des Kunden (nur IaaS)		✓	

Verschlüsselung und Schlüsselmanagement	B	Vt+	Vf+
Verschlüsselte Kommunikation zwischen Cloud-Anbieter und Cloud-Nutzer (TLS/SSL)	✓		
Verschlüsselte Kommunikation zwischen Cloud-Computing-Standorten	✓		
Verschlüsselte Kommunikation mit dritten Cloud-Service-Anbietern, falls diese für das eigene Angebot notwendig sind.	✓		

Verschlüsselung und Schlüsselmanagement	B	Vt+	Vf+
Best-Practices der Schlüsselverwaltung umsetzen, z. B.: • Administratoren sollten keinen Zugriff auf die Schlüssel haben • Verschlüsselungsschlüssel sollten niemals in Klartext offengelegt werden • Zugang zu Schlüsselverwaltungsfunktionen sollten eine separate Authentisierung erfordern • Schutz der im Speicher zwischengespeicherten Schlüssel • Sichere Archivierung von Schlüsseln • Sichere Replizierung von Schlüsseln		✓	

3 ID- und Rechtemanagement

Die Identitätsverwaltung ist wichtiger Bestandteil der Zugangskontrolle in Cloud-Computing-Systemen und muss von jeder Cloud-Plattform unterstützt werden. Das ID-Management kann auch bei einem Drittanbeiter (z. B. basierend auf SAML) angesiedelt sein. Es sollte eine Zweifaktor-Authentifizierung für Cloud-Nutzer angeboten werden. Intern muss der Cloud-Anbieter ebenfalls eine starke Authentisierung seiner Mitarbeiter nutzen.

Das Rechtemanagement muss gewährleisten, dass jede Rolle nur die Daten (auch Metadaten) sehen darf, die zur Erfüllung der Aufgabe notwendig sind. Das gilt auch für Administratoren.

ID- und Rechtemanagement	B	Vt+	Vf+
Sichere Identifikation der Cloud-Nutzer und Mitarbeiter des Cloud-Anbieters	✓		
Starke Authentisierung (z. B. Zweifaktor-Authentisierung) für Administratoren des Cloud-Anbieters	✓		
Zugriffskontrolllisten für Cloud-Nutzer und Mitarbeiter des Cloud-Anbieters	✓		
Regelmäßige Kontrolle und Aktualisierung der Zugriffskontrolllisten	✓		
Least Privilege Model (Nutzer bzw. Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen)	✓		
Vier-Augen-Prinzip für kritische Administrationstätigkeiten		✓	✓
Starke Authentisierung (z. B. Zweifaktor-Authentisierung) für Cloud-Nutzer		✓	✓
Angebot verschiedener Authentisierungsverfahren		✓	✓

4 Monitoring und Security-Incident Management

Der Cloud-Anbieter muss ein wirksames Monitoring implementieren und dem Cloud-Nutzer aussagekräftige Monitoringdaten zur Verfügung stellen.

Monitoring und Incident Management	B	Vt+	Vf+
24/7 Überwachung der Cloud (z. B. Verfügbarkeit der Services bzw. von Ressourcen)	✓		
Einbindung in die CERT-Strukturen und in das nationale IT-Krisenmanagement	✓		
Anbieter stellt sicher, dass 24/7 auf Angriffe, die aus der Cloud heraus durchgeführt werden, reagiert werden kann	✓		
Anbieter stellt sicher, dass interne Angriffe von Cloud-Nutzern auf andere Cloud-Nutzer erkannt werden	✓		
Logdatenerfassung und Auswertung (z. B. Systemstatus, fehlgeschlagene Authentisierungsversuche, etc.)	✓		
24/7-erreichbares, handlungsfähiges Cloud-Management und Trouble-Shooting	✓		
Verfügbarkeit der Services überwachen und messen und Messergebnisse den Kunden zur Verfügung stellen	✓		

5 Notfallmanagement

Um auf Ausnahmesituationen wie Notfälle vorbereitet zu sein, muss ein Cloud-Anbieter über ein entsprechendes Notfallmanagement, basierend auf etablierten Standards wie beispielsweise BS 25999 oder BSI-Standard 100-4, verfügen. Dazu gehört es, organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln, umzusetzen und zu üben, die eine rasche Reaktion auf Notfälle und die Fortsetzung zumindest der wichtigsten Geschäftsprozesse ermöglichen.

Notfallmanagement	B	Vt+	Vf+
Der Cloud-Anbieter muss ein Notfallmanagement implementieren	✓		
Regelmäßige Übungen (z. B. Ausfall eines Cloud-Computing-Standorts)	✓		
Nachweis eines implementierten Notfallmanagements (beispielsweise auf Basis von BS 25999 oder BSI-Standard 100-4)			✓

6 Sicherheitsprüfung und -nachweis

Der Cloud-Anbieter muss regelmäßig den IT-Sicherheitszustand überprüfen lassen und entsprechende Prüfnachweise den Cloud-Nutzern zur Verfügung stellen.

Sicherheitsprüfung und -nachweis	B	Vt+	Vf+
Der Cloud-Anbieter muss dem Cloud-Nutzer regelmäßig berichten über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, über Sicherheitsvorfälle, über die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests. Auch im Falle einer drohenden Insolvenz ist der Cloud-Nutzer zu unterrichten.	✓		
Regelmäßige Penetrationstests	✓		
Regelmäßige Penetrationstests bei Subunternehmen	✓		
Regelmäßige und unabhängige Sicherheitsrevisionen		✓	✓
Regelmäßige und unabhängige Sicherheitsrevisionen bei Subunternehmern		✓	✓

7 Anforderungen an das Personal

Der Cloud-Anbieter muss sicherstellen, dass sein Personal vertrauenswürdig, geschult und auf definierte Regeln verpflichtet ist.

Anforderungen an das Personal	B	Vt+	Vf+
Vertrauenswürdiges Personal	✓		
Ausbildung der Mitarbeiter des Cloud-Anbieters (Regelmäßige Schulung)	✓		
Sensibilisierung der Mitarbeiter des Cloud-Anbieters für Informationssicherheit und Datenschutz	✓		
Verpflichtung der Mitarbeiter auf Datenschutz, Sicherheitsmaßnahmen, Vertraulichkeit der Kundendaten	✓		

8 Transparenz

Der Cloud-Anbieter muss offen legen, an welchen Standorten die Daten und Anwendungen gespeichert und verarbeitet werden und wie dort der Zugriff durch Dritte geregelt ist. Auch wenn der Cloud-Anbieter Teile der Datenverarbeitung bzw. -speicherung von Subunternehmen ausführen lässt, müssen diese Informationen dem Cloud-Nutzer vorgelegt werden. Bei Änderungen zu obigen Punkten ist der Cloud-Nutzer zu unterrichten und es sind ihm ggf. alternative Lösungen anzubieten.

Transparenz	B	Vt+	Vf+
Offenlegung der Standorte des Cloud-Anbieters (Land, Region)	✓		
Offenlegung der Subunternehmer des Cloud-Anbieters	✓		
Transparenz, welche Eingriffe der Cloud-Anbieter in Daten und Verfahren der Kunden vornehmen darf	✓		
Regelmäßige Unterrichtung über Änderungen (z. B. neue oder abgekündigte Funktionen, neue Subunternehmer, andere Punkte, die für das SLA relevant sind)	✓		
Transparenz, welche Software durch den Cloud-Anbieter auf Seiten des Kunden installiert wird sowie über die daraus resultierenden Sicherheitserfordernisse /-risiken	✓		
Transparenz über staatliche Eingriffs- und Einsichtrechte, über gerichtlich festlegbare Einsichtrechte Dritter und über Prüfpflichten zu gespeicherten Daten durch den Cloud-Anbieter an allen potenziellen Standorten		✓	✓
Darlegung der Rechts- und Besitzverhältnisse des Cloud-Anbieters sowie der Entscheidungsbefugnisse		✓	✓
Erlaubnisvorbehalt des Kunden vor Eingriffen auf seinen Client gegenüber dem Cloud-Anbieter		✓	✓

9 Organisatorische Anforderungen

Sicherheitsleistungen müssen zwischen dem Cloud-Anbieter und dem Cloud-Nutzer vertraglich vereinbart werden, vorzugsweise in einem Security-SLA oder an hervorgehobener Stelle im SLA. Es muss Einsicht in die sicherheitsrelevanten Bestimmungen von Verträgen/SLAs mit den Subunternehmern gewährt werden. Auch für eine potenzielle Insolvenz des Cloud-Anbieters muss der Zugriff auf die Daten/Anwendungen des Cloud-Nutzers gesichert sein.

Organisatorische Anforderungen	B	Vt+	Vf+
Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben	✓		
Einsicht in Security-SLA bzw. SLA von Subunternehmern	✓		
Rahmenbedingungen zur Gültigkeit des SLAs aufführen (z. B. keine Verpflichtung zur Leistungserbringung aufgrund Höherer Gewalt)	✓		
Sicherstellung des Betriebs oder der Bereitstellung der Daten im Falle einer Insolvenz des Cloud-Anbieters		✓	✓

10 Kontrollmöglichkeiten für Nutzer

Den Cloud-Nutzern muss es möglich sein, Audits beim Cloud-Provider durchzuführen. Hierfür kann der Cloud-Anbieter Schnittstellen zur Verfügung stellen. Sofern dies nicht möglich ist, muss der Cloud-Anbieter dem Nutzer äquivalente, durch Dritte erstellte Auditberichte vorlegen.

Der Cloud-Nutzer muss überprüfen können, ob der Cloud-Anbieter das vereinbarte SLA einhält und so auch die Abrechnung nachvollziehen können.

Kontrollmöglichkeiten für Nutzer	B	Vt+	Vf+
Kunden sollen die Möglichkeit haben die Einhaltung der SLAs zu überwachen, indem beispielsweise die Qualität der angebotenen Services überwacht wird	✓		
Durchführung eines Audits beim Cloud-Anbieter durch den Cloud-Nutzer		✓	✓
Möglichkeit des Kunden, in Abstimmung mit dem Anbieter, Penetrationstests durchzuführen		✓	✓

11 Portabilität von Daten und Anwendungen

Cloud-Dienste müssen so gestaltet sein, dass der Cloud-Nutzer seine Daten jederzeit aus der Cloud wieder exportieren kann (kein vendor lock-in). Hierzu müssen die Daten in einem anbieterunabhängigen Format gespeichert sein oder in ein solches umgewandelt werden können. Das gleiche gilt für den Import von Daten.

Ziel muss es sein, ganze Anwendungen von einem Cloud-Anbieter zu einem anderen verschieben zu können, ohne dass der Nutzer sie neu entwickeln muss.

Portabilität von Daten und Anwendungen	B	Vt+	Vf+
Import und Export der Daten in einem geeigneten Format	✓		
Anwendungen müssen plattformunabhängig sein (nur SaaS)	✓		

12 Interoperabilität

Die Interoperabilität von Cloud-Computing-Plattformen definiert die Fähigkeit, unabhängige Cloud-Computing-Plattformen zusammenarbeiten zu lassen, ohne dass gesonderte Absprachen zwischen den Plattformen notwendig sind.

Um die Interoperabilität zu gewährleisten, müssen Anbieter von Cloud-Computing-Diensten standardisierte oder offen gelegte Schnittstellen (API, Protokolle) verwenden.

Interoperabilität	B	Vt+	Vf+
Standardisierte oder offen gelegte Schnittstellen (API und Protokolle)	✓		

13 Datenschutz/Compliance

Wenn in der Cloud personenbezogene Daten verarbeitet oder gespeichert werden, muss der Schutz personenbezogener Daten gemäß den Bestimmungen des BDSG gewährleistet sein.

Zudem sind vom Cloud-Anbieter die vom Cloud-Nutzer geforderten sonstigen rechtlichen Bestimmungen einzuhalten (compliance). Der Cloud-Anbieter muss hier die technischen Voraussetzungen geschaffen haben.

Datenschutz/Compliance	B	Vt+	Vf+
Gewährleistung des Datenschutzes nach deutschem Recht	✓		
Datenschutzrichtlinien und -gesetze, denen der Cloud-Nutzer unterliegt, müssen eingehalten werden	✓		
Speicherung und Verarbeitung der personenbezogenen Daten nur innerhalb der Mitgliedsstaaten der EU oder eines Vertragsstaats des EWR	✓		
Keine Einbindung von Unterauftragnehmern, die eine Verarbeitung der personenbezogenen Daten nur innerhalb der oben genannten Staaten nicht gewährleisten können	✓		
Kontrollrechte des Cloud-Nutzers zur datenschutzkonformen Verarbeitung der personenbezogenen Daten	✓		
Gesetzliche Bestimmungen des Cloud-Nutzers müssen durch den Anbieter eingehalten werden. Die relevanten Bestimmungen teilt der Cloud-Nutzer dem Anbieter mit.	✓		

14 Cloud-Zertifizierung

Der Cloud-Anbieter soll sein Sicherheitsniveau nachweisen können. Sobald anerkannte Zertifizierungen für Cloud-Anbieter verfügbar sind, sollten diese nachgewiesen werden.

Cloud-Zertifizierung	B	Vt+	Vf+
„Nachweis“ der Einhaltung von cloud-spezifischen Standards und Mindestanforderungen (vorliegende Mindestanforderungen des BSI), sobald solche etabliert sind (Selbstaussage)	✓		
Nachweis ausreichender Informationssicherheit (Zertifizierung)		✓	✓

15 Zusatzforderungen an Public-Cloud-Anbieter für die Bundesverwaltung

Nutzt die Bundesverwaltung einen Cloud-Anbieter, so muss dieser weitere Forderung erfüllen.

Zusatzforderungen an Public-Cloud-Anbieter für die Bundesverwaltung	B	Vt+	Vf+
Vertrag mit Gerichtsstandort Deutschland und deutsches Recht	✓		
IS-Revisionsrecht für das BSI stellvertretend für die Bundesverwaltung	✓		
Zusammenarbeit mit dem BSI-CERT und dem IT-Krisenreaktionszentrum im BSI	✓		
Berechtigung des BSI zur Durchführung von Penetrationstests in der Cloud	✓		

Einschränkungen

Die Nutzung einer Public Cloud bedeutet für den Nutzer eingeschränkte Kontrollmöglichkeiten gegenüber einem Betrieb unter eigener Hoheit. Sollen Informationen/Prozesse mit einer sehr hohen Vertraulichkeit (z. B. VS-eingestufte Daten) und/oder einer sehr hohen Verfügbarkeit (z. B. kritische Geschäftsprozesse, IT-Anwendungen in Kritischen Infrastrukturen) in einer Public Cloud verarbeitet bzw. ausgeführt werden, so hat der Dateneigner kritisch abzuwägen, ob er die Nutzung einer Public Cloud für diese hochschutzbedürftigen Daten/Prozesse verantworten kann.