Bundesamt
für Sicherheit in der
Informationstechnik

Kriterienkatalog Cloud Computing

C5:2020

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6666

E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/C5/

1 Vorwort des Präsidenten

Der C5-Anforderungskatalog des BSI hat sich in den letzten Jahren zu einer Speerspitze entwickelt, die die Cyber-Sicherheit in einem der wichtigsten Felder der Digitalisierung vorantreibt und unterstützt: dem Cloud Computing. Für den Erfolg der Digitalisierung ist es von großer Bedeutung, dass Cloud-Dienste nachweislich ein allgemein akzeptiertes Sicherheitsniveau aufweisen.

Als ich zu Beginn meiner Amtszeit im BSI 2016 als einen der ersten Vorgänge die Verabschiedung des ersten C5-Anforderungskatalogs verantwortete, fiel mir auf, dass das BSI hier einen neuen Weg ging. Das BSI hat Sicherheitsziele definiert, aber offengelassen, wie diese erreicht werden. Nicht das BSI führt C5-Audits durch, sondern Wirtschaftsprüfer, deren vorhandenes Prüfportfolio mit dem C5 um Cloud-Sicherheitsaspekte erweitert wird. In unterschiedlichsten Cloud-Architekturen sind konkrete Einzelmaßnahmen schwierig zu standardisieren, aber man kann sich auf gemeinsame Sicherheitsziele einigen, die ihren Weg in den C5 gefunden haben. Entsprechende Audits können nicht oder nur schwer von einer nationalen Behörde allein durchgeführt werden. Cloud-Dienste werden meistens global erbracht, daher erfolgt die Prüfung durch international verlässliche Partner.

Die internationale Erfolgsgeschichte des C5 zeigt, dass die damaligen Entscheidungen richtig waren. Viele nationale und internationale, kleine und große Cloud-Anbieter haben inzwischen ein C5-Testat erhalten, und auch außerhalb des öffentlichen Sektors fragen viele Cloud-Kunden die Testate nach, um die Sicherheit des eingesetzten Cloud-Dienstes zu bewerten. In regulierten Bereichen wie etwa bei Banken und Versicherungen werden C5-Testate als Nachweise eingesetzt und akzeptiert. Das BSI hat sich damit als Gestalter der Informationssicherheit in der Digitalisierung im Cloud-Bereich eine wichtige Rolle erarbeitet, die weltweit akzeptiert und geschätzt wird.

Als das BSI zu Beginn 2019 ankündigte, den C5 zu überarbeiten und dafür die Erfahrungen der Cloud-Anbieter, Kunden und Prüfer erfragte, war die Resonanz sehr groß. Viele unterschiedliche Gruppen, Verbände und sogar im Wettbewerb stehende Anbieter und Prüfer wirkten an gemeinsamen Workshops unter Leitung des BSI mit, teilten ihre Erfahrungen und machten konstruktive Vorschläge zur Verbesserung des C5. Ihnen allen möchte ich auf diesem Wege meinen Dank aussprechen!

Das Ergebnis kann sich sehen lassen. Neben unzähligen Aktualisierungen und Verbesserungen möchte ich folgende besonders hervorheben:

1. Der neue C5 setzt die allgemeinen Anforderungen des EU Cybersecurity Acts (EUCA) um. Die europäische Verordnung beschreibt Anforderungen an IT-Produkte und -Dienste, die nach einem EUCA-konformen Verfahren zertifiziert sind. Diese Anforderungen sind in den C5:2020 eingeflossen und in der neuen Domäne Produktsicherheit zusammengefasst.
2. Bei der sicheren Nutzung von Cloud-Diensten spielt die Schnittstelle zwischen Cloud-Anbieter und Cloud-Nutzer eine wichtige Rolle. Der C5:2020 führt „korrespondierende Kriterien“ ein, die der Cloud-Kunde an der Schnittstelle zum Cloud-Dienst zu erfüllen hat, um seinen Teil an der gemeinsamen Verantwortung für die Sicherheit wahrzunehmen.

Damit wird die Rolle des C5 als starkes Fundament für Cloud-Sicherheit für Anbieter, Kunden und Prüfer weiter ausgebaut. Er dient damit auch zukünftig als gutes Beispiel, wie Informationssicherheit in der Digitalisierung gestaltet werden kann.

Inhaltsverzeichnis

1 Vorwort des Präsidenten ... 3
2 Einleitung ... 6
2.1 Vorbemerkungen ... 6
2.2 Begriffsbestimmungen ... 7
3 Aufbau und inhaltliche Gliederung der Kriterien ... 9
3.1 Aufbau ... 9
3.2 Inhaltliche Gliederung der C5-Kriterien ... 10
3.3 Zugrundeliegende Standards und Publikationen ... 11
4 Nachweis der Konformität durch eine unabhängige Prüfung ... 13
4.1 Einführung ... 13
4.2 Anzuwendende Prüfungsstandards ... 13
4.3 Verbindung zu anderen Prüfungen ... 14
4.4 Ergänzende Anforderungen des BSI ... 15
4.5 Umgang mit Aktualisierungen des Kriterienkataloges ... 22
5 Angaben zu den Rahmenbedingungen des Cloud-Dienstes ... 24
6 Basiskriterien, Zusatzkriterien und ergänzende Informationen ... 28
6.1 Organisation der Informationssicherheit (OIS) ... 28
6.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP) ... 33
6.3 Personal (HR) ... 36
6.4 Asset Management (AM) ... 40
6.5 Physische Sicherheit (PS) ... 45
6.6 Regelbetrieb (OPS) ... 52
6.7 Identitäts- und Berechtigungsmanagement (IDM) ... 67
6.8 Kryptographie und Schlüsselmanagement (CRY) ... 74
6.9 Kommunikationssicherheit (COS) ... 77
6.10 Portabilität und Interoperabilität (PI) ... 82
6.11 Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) ... 85
6.12 Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) ... 91
6.13 Umgang mit Sicherheitsvorfällen (SIM) ... 96
6.14 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) ... 100
6.15 Compliance (COM) ... 104
6.16 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ) ... 107
6.17 Produktsicherheit (PSS) ... 109

2 Einleitung

2.1 Vorbemerkungen

Das BSI gestaltet als die Cyber-Sicherheitsbehörde des Bundes die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Informationssicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung, denn diese kann nur gelingen, wenn Anwender Vertrauen in (neue) Technologien entwickeln und diese zu ihrem Nutzen sicher einsetzen können.

Die Nutzung von Cloud Computing hat in den letzten Jahren stetig zugenommen und ist zu einem etablierten Standard für das Service- und Liefermodell von IT-Dienstleistungen avanciert. Cloud Computing basiert auf einem hohen Maß an Standardisierung der Hardware und Software sowie der darauf aufbauenden Dienstleistungen, deren Details dem Kunden im Regelfall nicht näher bekannt sind. Demzufolge ist ein besonders hohes Maß an Vertrauen in den Cloud-Dienstleister erforderlich, das zunächst einmal hergestellt werden muss.

In 2016 hat das BSI diesen Kriterienkatalog mit Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten veröffentlicht, um dieses Vertrauen herzustellen. Die Kriterien waren aus etablierten Standards zur Informationssicherheit abgeleitet und ermöglichten eine Prüfung durch Wirtschaftsprüfer nach internationalen Prüfungsstandards. Die inhaltlichen Kriterien wurden beispielsweise aus ISO/IEC 27001 sowie der Cloud Controls Matrix der Cloud Security Alliance.

Mit dieser ersten inhaltlichen Überarbeitung des Kriterienkatalogs möchte das BSI der Entwicklung in diesem Umfeld Rechnung tragen. Hierzu ist das BSI auch mit Cloud-Anbietern, Nutzern, Prüfern und Regulatoren in Dialog getreten, um deren Anregungen aufzunehmen. Die folgenden Aspekte stellen die wesentlichen Veränderungen im Vergleich zur vorherigen Version dieses Kriterienkatalogs dar:

- Aktualisierung der Kriterien hinsichtlich neuer Konzepte, z. B. „DevOps“, also dem Zusammenwachsen von Entwicklung und Betrieb von IT-Systemen;
- Erweiterung der Kriterien zur Bereitstellung der Cloud-Dienste um Produkt-spezifische Aspekte der Informationssicherheit, diese sind aus dem European Cybersecurity Act abgeleitet;
- Erweiterung der Kriterien zur Bereitstellung der Cloud-Dienste um Aspekte, die den Umgang des Cloud-Anbieters mit Ermittlungsanfragen staatlicher Stellen betreffen;
- Aufnahme korrespondierender Kriterien für Cloud-Kunden, diese dienen dazu, aufzuzeigen, an welchen Stellen Cloud-Kunden eigene Maßnahmen entwickeln müssen, um die Sicherheit des Cloud-Dienstes zu gewährleisten;
- Aufnahme ergänzender Hinweise und Informationen zum besseren Verständnis der Kriterien sowie zu deren kontinuierlicher Prüfung;
- Ergänzung des bisherigen Prüfungsverfahrens, der Prüfung einer Erklärung zum IT-System, um die Möglichkeit einer direkten IT-Prüfung.

Der Name wurde von Anforderungskatalog zu Kriterienkatalog geändert. Damit wurde der Tatsache Rechnung getragen, dass die bisherigen Anforderungen aus dem C5 in den seltensten Fällen 1:1 in ein dienstleistungsbezogenes internes Kontrollsystem beim Cloud-Anbieter überführt wurden. Stattdessen wurden die Kontrollen des dienstleistungsbezogenen internen Kontrollsystems dahingehend geprüft, ob sie das Niveau der C5-Anforderungen erreichen. Damit dienten sie bereits als Kriterien für ein Kontrollsystem, was nun durch die Umbenennung verdeutlicht wird. Auch der englische Name wurde auf Cloud Computing Compliance Criteria Catalogue geändert; die Abkürzung C5 wurde daher beibehalten.

Hinsichtlich Aufbau und Inhalt dieses Kriterienkatalogs wird auf den Abschnitt 3 dieses Dokuments verwiesen. Hinweise zum Nachweis der Konformität mit diesem Kriterienkatalog sind Gegenstand des Abschnitts 4. Die Kriterien für eine unabhängige Prüfung sind in den Abschnitten 5 und 6 zu finden.

Die Kriterien in diesem Kriterienkatalog sind für zu prüfende Zeiträume anzuwenden, die am oder nach dem 15. Februar 2021 enden. Eine frühere Anwendung dieser Kriterien ist zulässig.

2.2 Begriffsbestimmungen

Für Zwecke dieses Kriterienkatalogs gelten die folgenden Begriffsbestimmungen, die sich an Definitionen aus dem IT-Grundschutz-Kompendium des BSI sowie des internationalen Standards ISO/IEC 17788:2014 (Information technology – Cloud computing – Overview and vocabulary) ableiten:

Assets: Dieser Begriff wird in diesem Kriterienkatalog synonym zu dem Begriff „Systemkomponenten“ (siehe weiter unten) verwendet.

Authentizität: Eigenschaft von Informationen, dass Änderungen einem Verursacher eindeutig zuzuordnen sind.

Cloud-Anbieter: Natürliche oder juristische Person, die einen Cloud-Dienst bereitstellt.

Cloud Computing: Ansatz für das dynamische und 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.

Cloud-Dienst: Im Rahmen von Cloud Computing angebotenen Dienstleistung der Informationstechnik. Dies beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud-Kunde: Natürliche oder juristische Person, die mit dem Cloud-Anbieter zum Zwecke der Nutzung des Cloud-Dienstes in einer Geschäftsbeziehung steht.

Hardware-Objekte: Physische und virtuelle Infrastruktur-Ressourcen (z. B. Server, Speichersysteme, Netzkomponenten), sowie Endgeräte, soweit der Cloud-Anbieter in einer Risikobewertung festgestellt hat, dass diese bei Verlust oder unautorisierten Zugriffen die Informationssicherheit des Cloud-Dienstes gefährden könnten (z. B. Mobilgeräte, die als Security-Token zur Authentifizierung genutzt werden).

Integrität: Eigenschaft von Informationen, dass diese vollständig und richtig (korrekt, unversehrt) und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind.

Informationssicherheit: Schutz der im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Informationen der Kunden des Cloud-Anbieters hinsichtlich der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

Schutzbedarf: Für die Kunden des Cloud-Anbieters ausreichendes und angemessenes Niveau der Informationssicherheit hinsichtlich der im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Informationen.

Systemkomponenten: Die für die Informationssicherheit des Cloud-Dienstes während der Erstellung, Verarbeitung, Speicherung, Übertragung, Löschung oder Zerstörung von Informationen benötigten Objekte im Verantwortungsbereich des Cloud-Anbieters, z. B. Firewalls, Loadbalancer, Webserver, Anwendungsserver und Datenbankserver.

Verfügbarkeit: Eigenschaft von Informationen, Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen, dass sie stets wie vorgesehen genutzt werden können.

Vertraulichkeit: Eigenschaft von Informationen, dass sie ausschließlich befugten Personen, Einheiten und Prozessen in der zulässigen Weise verfügbar gemacht werden.

Weiter gelten die folgenden Begriffsbestimmungen, die aus dem International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information", ISAE 3402 „Assurance Reports on Controls at a Service Organization" sowie den damit im Einklang stehenden Prüfungsstandards (PS) 860 und 951 n.F. des Instituts der Wirtschaftsprüfer (IDW) abgeleitet wurden.

C5-Kriterien: Die zur Beurteilung der Informationssicherheit des Cloud-Dienstes anzuwendenden und in diesem Kriterienkatalog definierten Maßstäbe dieses Kriterienkatalogs (vgl. Abschnitt 6).

Dienstleistungsbezogenes internes Kontrollsystem: Die von den gesetzlichen Vertretern (Management) des Cloud-Anbieters angewendeten Grundsätze, Verfahren und Maßnahmen, die auf die organisatorische und technische Umsetzung der Entscheidungen des Managements zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit, zur Informationssicherheit des Cloud-Dienstes sowie zur Einhaltung der für den Cloud-Anbieter maßgeblichen rechtlichen und sonstigen Vorschriften gerichtet sind.

Direkte Prüfung: Ein Prüfungsauftrag, bei dem der Wirtschaftsprüfer den durch die Auftragsvereinbarung abgegrenzten Cloud-Dienst als Prüfungsobjekt anhand der C5-Kriterien prüft und die daraus resultierenden Sachverhaltsinformationen als Teil seiner Berichterstattung darstellt.

Erklärung der gesetzlichen Vertreter zum Cloud-Dienst: Angaben der gesetzlichen Vertreter des Cloud-Anbieters über die Beschreibung des dienstleistungsbezogenen internen Kontrollsystems zur Bereitstellung des Cloud-Dienstes sowie über die Angemessenheit und, sofern einschlägig, die Wirksamkeit der Kontrollen zum Erfüllen der C5-Kriterien in schriftlicher Form.

Kontrolle: Prozessintegrierte oder prozessunabhängige Maßnahme, um die Wahrscheinlichkeit für das Auftreten von Ereignissen zu vermindern bzw. aufgetretene Ereignisse aufzudecken, um die Informationssicherheit des Cloud-Dienstes aufrecht zu erhalten.

Prüfung einer Erklärung: Ein Prüfungsauftrag, bei dem der Wirtschaftsprüfer prüft, ob die Erklärung der gesetzlichen Vertreter zum Cloud-Dienst frei von wesentlichen Fehlern ist.

Wesentliche Fehler: Mängel in der Erklärung der gesetzlichen Vertreter, z. B.:

- Angaben lassen nicht erkennen, dass Kontrollen nicht angemessen, nicht implementiert oder nicht wirksam sind, um mit hinreichender Sicherheit die C5-Kriterien zu erfüllen;
- Angaben sind falsch oder fehlen, die einzeln oder in Summe für die Kunden des Cloud-Anbieters relevant sein können, um die Informationssicherheit des Cloud-Dienstes zu beurteilen;
- Angaben umfassen unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen, die eine Irreführung der Kunden des Cloud-Anbieters zur Folge haben können.

3 Aufbau und inhaltliche Gliederung der Kriterien

3.1 Aufbau

Dieser Kriterienkatalog enthält Kriterien zur Informationssicherheit von Cloud-Diensten. Diese gliedern sich in 17 Bereiche, denen jeweils eine Zielsetzung zugewiesen ist, die durch die Kriterien erreicht werden soll (vgl. Abschnitt 3.2).

Die Kriterien gliedern sich in Basiskriterien und Zusatzkriterien (C5-Kriterien).

Die Basiskriterien 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 diesem Kriterienkatalog 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. Cloud-Anbieter können die Zusatzkriterien zusätzlich zu den Basiskriterien in eine Prüfung aufnehmen, um Kunden mit einem höheren Schutzbedarf anzusprechen.

Neben Basis- und Zusatzkriterien sowie ergänzenden Informationen zu den Kriterien enthält Kapitel 6 die folgenden Elemente:

- Hinweise zur kontinuierlichen Prüfung:
  Die C5-Kriterien wurden um Hinweise ergänzt, wie Cloud-Anbieter durch Automatisieren ihrer Verfahren und Maßnahmen erste Schritte zu einer kontinuierlichen Überwachung, bis hin zu einer Prüfung durch unabhängige Dritte einleiten können. Dies soll Cloud-Anbietern ermöglichen, Abschätzungen zur generellen Umsetzbarkeit sowie Aufwandsschätzungen einer kontinuierlichen Prüfung durch unabhängige Dritte vorzunehmen.

- Korrespondierende Kriterien für Kunden:
  Die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes obliegt nicht alleine dem Cloud-Anbieter. Auch die Kunden müssen den Mitwirkungspflichten in ihrem Verantwortungsbereich nachkommen. Bei Cloud-Diensten für Infrastruktur sind Kunden typischerweise selbst dafür verantwortlich, z. B. Sicherheitsaktualisierungen für das von Ihnen genutzte Betriebssystem einzuspielen, wohingegen diese Verantwortung bei der Nutzung eines Cloud-Dienstes für eine Software typischerweise beim Cloud-Anbieter liegt.
  Für ausgewählte C5-Kriterien sind korrespondierende Kriterien für Kunden angegeben, die aufzeigen sollen, wo potentiell Mitwirkungspflichten bestehen. Es handelt sich dabei allerdings um keine abschließende und für alle Cloud-Dienste allgemein gültige Aufstellung. Vielmehr werden folgende Ziele verfolgt:
  - Cloud-Anbieter soll dies beim Erstellen der Systembeschreibung unterstützen, jene C5-Kriterien zu identifizieren, bei denen typischerweise korrespondierende Kontrollen auf Seiten der Kunden vorausgesetzt werden, die zusammen mit den Kontrollen des Cloud-Anbieters eingerichtet sein müssen, um die C5-Kriterien zu erfüllen (vgl. Abschnitt 4.4.4.1);
  - Prüfer soll dies bei der Prüfung der Systembeschreibung dabei unterstützen, die Angemessenheit der Angaben zu den korrespondierenden Kontrollen zu beurteilen;
  - Kunden soll dies unterstützen die Angaben zu den korrespondierenden Kontrollen in der Systembeschreibung besser zu verstehen und entsprechende Kontrollen einzurichten.

Vertrauen in die Informationssicherheit eines Cloud-Dienstes kann durch detaillierte Angaben über die beim Cloud-Anbieter eingerichteten Kontrollen hergestellt werden. Neben Transparenz hinsichtlich der C5-Kriterien (vgl. Abschnitt 3.2), sind auch die Angaben zu den Rahmenbedingungen des Cloud-Dienstes zu beachten (z. B. Gerichtsstandort des Cloud-Anbieters oder vertragliche Vereinbarungen zur Verfügbarkeit und Störungsbeseitigung). Diese müssen aus Sicht des BSI den potentiellen Kunden eines Cloud-Dienstes bekannt sein, um dessen Eignung für ihren jeweiligen Anwendungsfall beurteilen zu können.

3.2 Inhaltliche Gliederung der C5-Kriterien

Die C5-Kriterien gliedern sich in 17 Bereiche, die sich an der Darstellung der Maßnahmenziele aus ISO/IEC 27001:2013 Anhang A orientieren (vgl. Tabelle 1).

Nr.	Bereich (Kennung)	Zielsetzung
1	Organisation der Informationssicherheit (OIS)	Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation
2	Sicherheitsrichtlinien und Arbeitsanweisungen (SP)	Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen
3	Personal (HR)	Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden
4	Asset Management (AM)	Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenes Schutzniveau über deren gesamten Lebenszyklus sicherstellen
5	Physische Sicherheit (PS)	Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs
6	Regelbetrieb (OPS)	Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern
7	Identitäts- und Berechtigungs-management (IDM)	Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (in der Regel privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen
8	Kryptographie und Schlüsselmanagement (CRY)	Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information
9	Kommunikationssicherheit (COS)	Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen
10	Portabilität und Interoperabilität (PI)	Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen

		zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen
11	Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)	Sicherstellen der Informationssicherheit im Entwicklungszyklus von Systemkomponenten des Cloud-Dienstes
12	Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)	Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Subdienstleister) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen
13	Umgang mit Sicherheitsvorfällen (SIM)	Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen
14	Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)	Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement
15	Compliance (COM)	Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung
16	Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)	Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten
17	Produktsicherheit (PSS)	Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden

Tabelle 1: Bereiche des Kriterienkatalogs mit zugewiesenen Zielsetzungen

3.3 Zugrundeliegende Standards und Publikationen

Die C5-Kriterien leiten sich aus Anforderungen ab, die aus national und international etablierten Standards und Publikationen entnommen wurden. Der Detaillierungsgrad geht dabei meist über diese Standards und Publikationen hinaus, um ein hohes Niveau an Transparenz über die Grundsätze, Verfahren und Maßnahmen der Cloud-Anbieter zu erreichen.

In diesen Kriterienkatalog sind Anforderungen aus den folgenden Standards und Publikationen eingeflossen:

- DIN EN ISO/IEC 27001:2017 – Informationssicherheitsmanagementsysteme – Anforderungen
- DIN ISO/IEC 27002:2016 – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Maßnahmen
- ISO/IEC 27017:2015 –Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- BSI – IT-Grundschutz-Kompendium 2. Edition 2019
- CSA (Cloud Security Alliance, eine Non-Profit-Organisation zur Verbreitung von Sicherheitsstandards im Cloud Computing) – Cloud Controls Matrix 3.0.1 (CSA CCM)
- AICPA (American Institute of Certified Public Accountants, amerikanischer Berufsverband der Wirtschaftsprüfer) – Trust Services Criteria 2017 (TSC)
- ANSSI (Agence nationale de la sécurité des systèmes d'information, französische Behörde für die Sicherheit von Informationssystemen) – Prestataires de services d'informatique en nuage v. 3.1 (SecNumCloud)
- IDW (Institut der Wirtschaftsprüfer, die Interessenvertretung der wirtschaftsprüfenden Berufsstände in Deutschland) RS FAIT 5 – Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing“, Stand vom 04.November 2015

Cloud-Anbietern, die sich bei der Gestaltung ihrer Grundsätze, Verfahren und Maßnahmen bereits an einem oder mehreren dieser Standards und Publikationen orientieren, können diese den C5-Kriterien zuordnen, um die Erfüllung zu beurteilen.

Die Zuordnung wird durch Referenztabellen unterstützt, die das BSI auf seiner Webseite bereitstellt (https://www.bsi.bund.de/C5). Die Referenztabellen sind als Hilfsmittel zu verstehen. Unabhängig von den darin enthaltenen Angaben ist stets im Einzelfall zu beurteilen, ob die eingerichteten Grundsätze, Verfahren und Maßnahmen geeignet sind, die C5-Kriterien zu erfüllen (vgl. Abschnitt 4.4.6).

4 Nachweis der Konformität durch eine unabhängige Prüfung

4.1 Einführung

Die in diesem Kriterienkatalog dargelegten C5-Kriterien können sowohl von Cloud-Anbietern als auch von Cloud-Kunden herangezogen werden. Während Cloud-Anbieter sich beim Gestalten ihrer Grundsätze, Verfahren und Maßnahmen an den C5-Kriterien ausrichten können, werden Cloud-Kunden den Anspruch haben, zu verifizieren, ob der Cloud-Anbieter diese Kriterien erfüllt. Eine Selbstauskunft für jeden einzelnen Kunden wäre für Cloud-Anbieter jedoch nicht effizient und für Kunden zu wenig verbindlich. Zudem wäre eine einheitliche Auskunftstiefe – wenn ein Kunde mehrere Anbieter anfragt – nicht gegeben, so dass ein Kunde die Auskünfte verschiedener Anbieter nur schwer vergleichen könnte. Eine auf einheitlichen Kriterien basierende Beurteilung des Cloud-Anbieters durch einen unabhängigen und sachverständigen Wirtschaftsprüfer, der nach verbindlichen Vorgaben Berichterstattungen gegenüber dem Auftraggeber erstellt, die zur Weitergabe an bestehende und potenzielle Kunden geeignet sind, ist nach Auffassung des BSI eine wirtschaftliche und sinnvolle Lösung.

Daher legt das BSI nachfolgend seine Auffassung dar, welche Anforderungen an einen Nachweis der Konformität sowie der Berichterstattung gegenüber dem Cloud-Anbieter und deren Kunden bestehen.

Der Kunde des Cloud-Anbieters sollte die Einhaltung der Kriterien aus diesem Kriterienkatalog als einen wesentlichen Bestandteil seiner Beauftragung ansehen und dies auch mit dem Anbieter vereinbaren. Dies gilt insbesondere für den Fall, wenn die Zusatzkriterien durch den Cloud-Anbieter erfüllt werden sollen. Ferner sollte der potenzielle Cloud-Kunde seine Entscheidung nicht nur auf eine vorhandene, aktuelle Berichterstattung nach diesem Kriterienkatalog gründen (unabhängig, ob diese sich auf die Basis- oder Zusatzkriterien bezieht), sondern sollte sich die Berichterstattung des Wirtschaftsprüfers vom Cloud-Anbieter regelmäßig vorlegen lassen und diesen für seinen Anwendungsfall bewerten.

Das BSI ist an keinem Teil der Prüfung oder Berichterstattung beteiligt. Die Prüfungsdurchführung durch den Wirtschaftsprüfer erfolgt weisungsunabhängig vom BSI. Der Wirtschaftsprüfer erbringt seine Tätigkeit gegenüber dem Cloud-Anbieter, nicht gegenüber dem Kunden des Anbieters.

4.2 Anzuwendende Prüfungsstandards

Bei den Anforderungen zum Nachweis der Konformität wurde, wie bei der inhaltlichen Ausgestaltung der C5-Kriterien selbst, auf national und international etablierte Standards zurückgegriffen.

Im Einzelnen sind dies der International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ bzw. der mit diesem in Einklang stehende deutsche Prüfungsstandard (PS) 860 „IT-Prüfung außerhalb der Abschlussprüfung“ des Instituts der Wirtschaftsprüfer (IDW) oder andere nationale Äquivalente zum ISAE 3000 (Revised). Einer dieser Prüfungsstandards oder ein damit in Einklang stehendes nationales Pendant soll von Prüfern als Grundlage zur Prüfungsplanung, Prüfungsdurchführung und Berichterstattung herangezogen werden.

Für Einzelfragen der Prüfungsdurchführung und Berichterstattung sollen weitere Prüfungsstandards hinzugezogen werden: Zu nennen sind ISAE 3402 „Assurance Reports on Controls at a Service Organization“ bzw. der mit diesem in Einklang stehende deutsche IDW PS 951 n.F. „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen”) oder andere nationale Äquivalente zum ISAE 3402. Von

diesen Standards wurden die Anforderungen an die Inhalte der Systembeschreibung abgeleitet, die Bestandteil der Berichterstattung sind (vgl. Abschnitt 4.4.4.1).

Darüber hinaus wurden die Prüfungsstandards AT-C section 105 „Concepts Common to All Attestation Engagements“ und AT-C section 205 „Examination Engagements“ der AICPA, des amerikanischen Berufsverbands der Wirtschaftsprüfer herangezogen. Diese Standards ergänzen ISAE 3402 und IDW PS 951 n.F. insbesondere um Anforderungen an das Berücksichtigen von Subdienstleistungsunternehmen.

4.3 Verbindung zu anderen Prüfungen

Die C5-Kriterien sind von etablierten Standards und Publikationen abgeleitet (vgl. Abschnitt 3.3). Sofern diese beim Cloud-Anbieter bereits als Referenz genutzt werden, wird dieser bereits entsprechende Grundsätze, Verfahren und Maßnahmen in seinem Betriebsablauf berücksichtigt haben.

Diese Grundsätze, Verfahren und Maßnahmen bilden typischerweise auch die Grundlage für weitere Prüfungen, die der Cloud-Anbieter ggf. auch bereits durch Wirtschaftsprüfer durchführen lässt. Zu nennen sind in diesem Zusammenhang insbesondere Prüfungen nach ISAE 3402, IDW PS 951 n.F. oder den US-Regelungen für SOC 1 oder SOC 2. In diesen Fällen bietet es sich an, diese Prüfungen organisatorisch und zeitlich mit einer Prüfung nach diesem Kriterienkatalog zu kombinieren. Hierdurch werden Wirtschaftsprüfer und Cloud-Anbieter in die Lage versetzt, Aufzeichnungen parallel sowohl für eine Berichterstattung nach z. B. ISAE 3402 und/oder SOC 2 als auch für die Berichterstattung nach diesem Kriterienkatalog zu nutzen.

Sofern der Cloud-Anbieter darüber hinaus Zertifikate (z. B. nach ISO/IEC 27001, ISO 22301) anstrebt, bietet es sich ebenfalls an, die entsprechenden Prüfungen, soweit möglich, zu kombinieren. Die in einem separaten Begleitdokument zu diesem Kriterienkatalog definierte Referenztabelle kann dazu herangezogen werden.

Beim Bewerten der Abdeckung von C5-Kriterien durch Ergebnisse, die in anderen Prüfungen erzielt wurden, ist die Art der Prüfung besonders zu berücksichtigen und gegen die für eine C5-Prüfung erforderliche „hinreichende Sicherheit“ für die „Prüfung einer Erklärung“ oder eine „direkte Prüfung“ abzugleichen (vgl. Abschnitt 4.4.1). Bei einem solchen Vorgehen müssen beispielsweise Ergebnisse aus einer ISO-Zertifizierung anders bewertet werden als solche, die mit einer Prüfung nach ISAE 3000 erzielt wurden.

In den Referenztabellen sind die C5-Kriterien den in anderen Standards definierten Kriterien zugeordnet. Hierbei ist zu berücksichtigen, dass eine Zuordnung zunächst nur die thematische Verwandtschaft der Kriterien widerspiegelt. Zudem ist angegeben, inwiefern die C5-Kriterien aus Sicht des BSI das von den zugeordneten, anderen Kriterien artikulierte Niveau an Informationssicherheit abbilden.

Die Tabellen sind lediglich als Hilfsmittel anzusehen, um in einer ersten Annäherung zu verstehen, inwiefern sich die C5-Kriterien mit den in anderen Standards definierten Kriterien überschneiden. Von den in den Referenztabellen angegebenen Zuordnungen kann jedoch nicht vollständig auf die tatsächliche Abdeckung der C5-Kriterien durch bei einem Cloud-Anbieter eingerichtete Grundsätze, Verfahren und Maßnahmen geschlossen werden. Dies gilt auch dann, wenn diese eingerichteten Grundsätze, Verfahren und Maßnahmen bereits einer Prüfung gemäß eines oder mehrerer in der Referenztabelle enthaltener Standards unterzogen wurden. Aus Sicht des BSI ist stets individuell und spezifisch zu ermitteln, inwiefern die von einem Cloud-Anbieter eingerichteten Grundsätze, Verfahren und Maßnahmen die C5-Kriterien tatsächlich abdecken.

Der bloße Verweis auf die in anderen Standards definierten Kriterien, denen die C5-Kriterien in den Referenztabellen zugeordnet sind, ist daher nicht ausreichend.

Die sonstigen Möglichkeiten des Wirtschaftsprüfers, im Rahmen seiner Eigenverantwortlichkeit ggf. auch Ergebnisse Dritter zu verwenden, bleiben hiervon unberührt.

4.4 Ergänzende Anforderungen des BSI

Nachfolgend wird die Anwendung der oben genannten Prüfungsstandards spezifiziert.

4.4.1 Prüfungsauftrag

Der Nachweis der Konformität hat grundsätzlich unter Anwendung des Prüfungsstandards ISAE 3000 (Revised) zu erfolgen.

Der Prüfungsstandard ISAE 3000 (Revised) unterscheidet Prüfungsaufträge mit einer hinreichenden Sicherheit („reasonable assurance“) von Prüfungsaufträgen mit einer begrenzten Sicherheit („limited assurance“). Prüfungen zum Nachweis der Konformität mit diesem Kriterienkatalog haben nach Auffassung des BSI mit hinreichender Sicherheit („reasonable assurance“) zu erfolgen.

Ferner wird zwischen der Prüfung einer Erklärung („attestation engagement“) und einer direkten Prüfung („direct engagement“) unterschieden. Grundsätzlich eignen sich beide Prüfungsarten für die Beurteilung des Nachweises der Konformität mit diesem Kriterienkatalog.

Zudem können Prüfungen in der Form einer Angemessenheitsprüfung oder einer Wirksamkeitsprüfung durchgeführt werden. Nach Auffassung des BSI ist eine Wirksamkeitsprüfung erforderlich, um eine angemessene Aussagekraft hinsichtlich der Eignung des dienstleistungsbezogenen internen Kontrollsystems zu erzielen. Nur auf Grundlage von Wirksamkeitsprüfungen kann mit hinreichender Sicherheit beurteilt werden, ob das dienstleistungsbezogene interne Kontrollsystem geeignet ist, den in diesem Kriterienkatalog definierten C5-Kriterien zu entsprechen. Prüfungen der Angemessenheit des dienstleistungsbezogenen internen Kontrollsystems sollten nur im Falle der Erstprüfung eines Cloud-Dienstes nach diesem Kriterienkatalog erfolgen und keinesfalls mehrmals hintereinander in Betracht gezogen werden.

4.4.2 Anzuwendende Kriterien

4.4.2.1 Kriterien zur Informationssicherheit des Cloud-Dienstes

Die Basiskriterien 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 diesem Kriterienkatalog 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. Cloud-Anbieter können die Zusatzkriterien zusätzlich zu den Basiskriterien in eine Prüfung aufnehmen, um Kunden mit einem höheren Schutzbedarf anzusprechen.

Soweit einzelne Basis- oder Zusatzkriterien aufgrund der Art und Ausgestaltung des bereitgestellten Cloud-Dienstes oder der Grundsätze, Verfahren und Maßnahmen des Cloud-Anbieters nicht anwendbar sind, ist dies vom Cloud-Anbieter in der Systembeschreibung darzulegen. Der Wirtschaftsprüfer hat basierend auf den vom Cloud-Anbieter übergebenen Informationen zu beurteilen, ob und inwiefern tatsächlich eine Nichtanwendbarkeit der C5-Kriterien vorliegt oder C5-Kriterien nicht bzw. nur teilweise erfüllt sind.

Die anwendbaren C5-Kriterien sind in der Berichterstattung im Abschnitt zur Darstellung der C5-Kriterien, Kontrollen, Prüfungshandlungen und Prüfungsergebnisse anzugeben.

4.4.2.2 Weitere Kriterien zur Transparenz und Berichterstattung

Weitere Kriterien stellen die Angaben zu den Rahmenbedingungen des Cloud-Dienstes (vgl. Abschnitt 5) sowie die Anforderungen an die Systembeschreibung und die Erklärung der gesetzlichen Vertreter (vgl. Abschnitt 4.4.4.1; dort ist auch die Handhabung der Rahmenbedingungen bei einer direkten Prüfung geregelt) dar. Diese dienen der Information der Kunden über die Informationssicherheit des Cloud-Dienstes, um dessen Eignung für ihren Anwendungsfall zu beurteilen. Sie sollen außerdem ein vergleichbares Niveau in der Berichterstattung sicherstellen, um Kunden einen Vergleich mehrerer Cloud-Anbieter bzw. Cloud-Dienste, für die ein C5-Bericht ausgestellt wurde, zu erleichtern.

4.4.3 Gegenstand und Ziel der Prüfung

4.4.3.1 Prüfung einer Erklärung

Gegenstand der Prüfung ist die vom Cloud-Anbieter erstellte Systembeschreibung des dienstleistungsbezogenen internen Kontrollsystems zur Bereitstellung des Cloud-Dienstes in Bezug auf die C5-Kriterien (Systembeschreibung). Die Prüfung erfolgt auf Grundlage einer Erklärung der gesetzlichen Vertreter des Cloud-Anbieters über die Angemessenheit der Kontrollen zum Erfüllen der anwendbaren C5-Kriterien zum zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) und, sofern beauftragt, die Wirksamkeit der Kontrollen während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2).

Ziel der Prüfung ist es, dem Wirtschaftsprüfer eine Aussage mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die Systembeschreibung des Cloud-Anbieters die tatsächliche Ausgestaltung und Einrichtung des dienstleistungsbezogenen internen Kontrollsystems zum zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) bzw. während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2) sachgerecht darstellt und die Mindestinhalte gemäß Abschnitt 4.4.4.1 dieses Kriterienkatalogs enthalten sind,
- die in der Systembeschreibung dargestellten Kontrollen zu dem zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) bzw. während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2) angemessen ausgestaltet und eingerichtet sind, um die anwendbaren C5-Kriterien zu erfüllen und
- sofern beauftragt, die in der Systembeschreibung dargestellten Kontrollen (Berichterstattung vom Typ 2) während des zu prüfenden Zeitraums wirksam sind.

Aus Sicht des BSI können Cloud-Anbieter, die bereits über eine Systembeschreibung verfügen, diese in Prüfungen gemäß diesem Kriterienkatalog erneut nutzen. Eine bereits vorhandene Systembeschreibung, welche die Anforderungen eines anderen Standards erfüllt, ist jedoch gegebenenfalls an diesen Kriterienkatalog anzupassen.

4.4.3.2 Direkte Prüfung

Bei einer direkten Prüfung erfolgt die Erhebung der vom Cloud-Anbieter für den Cloud-Dienst angewendeten Grundsätze, Verfahren und Maßnahmen durch den Wirtschaftsprüfer.

Anders als bei der Prüfung einer Erklärung liegt vom Cloud-Anbieter keine Systembeschreibung vor. Die Erhebung der für die Prüfung relevanten Teile des dienstleistungsbezogenen internen Kontrollsystems erfolgt daher während der Prüfungsdurchführung. Dies erfordert vom Wirtschaftsprüfer typischerweise Befragungen sachkundiger Auskunftspersonen des Cloud-Anbieters sowie die Durchsicht relevanter Aufzeichnungen und Dokumente.

Ziel der Prüfung ist es, dem Wirtschaftsprüfer eine Aussage mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die vom Cloud-Anbieter angewandten Grundsätze, Verfahren und Maßnahmen des zu prüfenden Cloud-Dienstes angemessen ausgestaltet und eingerichtet sind, um die anwendbaren C5-Kriterien zu erfüllen und
- sofern beauftragt, die angewandten Grundsätze, Verfahren und Maßnahmen während des zu prüfenden Zeitraums wirksam sind.

Die direkte Prüfung ist aus Sicht des BSI insbesondere für Cloud-Anbieter geeignet, die ihr dienstleistungsbezogenes internes Kontrollsystem noch nicht vollständig bzw. noch nicht ausreichend detailliert in einer Systembeschreibung dokumentiert haben.

4.4.4 Anforderungen an die Systembeschreibung und die Erklärung der gesetzlichen Vertreter

4.4.4.1 Systembeschreibung

Bei der Prüfung einer Erklärung hat die Systembeschreibung des Cloud-Anbieters insbesondere die folgenden Mindestinhalte zu umfassen, damit Kunden eine hinreichende Transparenz über die Informationssicherheit des Cloud-Dienstes erhalten:

- Name, Art und Umfang der bereitgestellten Cloud-Dienste;
- Beschreibung der Systemkomponenten für die Bereitstellung des Cloud-Dienstes;
- Angaben zu den Rahmenbedingungen des Cloud-Dienstes gemäß den Kriterien in Abschnitt 6 dieses Kriterienkatalogs, die es potentiellen Kunden des Cloud-Dienstes ermöglichen, dessen Eignung für ihren Anwendungsfall zu beurteilen;
- anwendbare C5-Kriterien;
- Grundsätze, Verfahren und Maßnahmen, einschließlich der dafür eingerichteten Kontrollen, zur Bereitstellung (Entwicklung und Betrieb) der Cloud-Dienste in Bezug auf die anwendbaren C5-Kriterien;
- Umgang mit bedeutsamen Vorkommnissen, die Ausnahmen vom Regelbetrieb darstellen, wie beispielsweise Sicherheitsvorfälle oder der Ausfall von Systemkomponenten;
- die der bei Ausgestaltung der Grundsätze, Verfahren und Maßnahmen vom Cloud-Anbieter unterstellten korrespondierenden Kontrollen bei den Kunden des Cloud-Dienstes;
- an Subdienstleistungsunternehmen vergebene oder ausgelagerte Funktionen in Bezug auf die anwendbaren C5-Kriterien, einschließlich Angaben zu Art und Umfang der Auslagerung, Lokationen der Verarbeitung und Speicherung von Daten, Komplexität und Einzigartigkeit der bezogenen Leistungen und die daraus resultierende Abhängigkeit des Cloud-Anbieters sowie zur Verfügbarkeit einer Berichterstattung nach diesem Kriterienkatalog.

Bei der Prüfung der Wirksamkeit (Berichterstattung vom Typ 2) ist die Systembeschreibung um folgende Mindestinhalte zu ergänzen:

- wesentlichen Änderungen an den Grundsätzen, Verfahren und Maßnahmen, einschließlich der dafür eingerichteten Kontrollen, zur Bereitstellung (Entwicklung und Betrieb) der Cloud-Dienste in Bezug auf die anwendbaren C5-Kriterien, die während des zu prüfenden Zeitraums durchgeführt wurden;

- Auftreten von und Umgang mit bedeutsamen Vorkommnissen im zu prüfenden Zeitraum, die Ausnahmen vom Regelbetrieb darstellten, im Verantwortungsbereich des Cloud-Anbieters lagen und die dazu führten, dass
  - die vertraglichen Vereinbarungen zur Verfügbarkeit des Cloud-Dienstes nicht erfüllt wurden oder
  - unautorisierte Dritte Zugriff auf die im Cloud-Dienst gespeicherten Daten der Cloud-Kunden erhielten oder
  - die Integrität der im Cloud-Dienst gespeicherten Daten verletzt wurde und die dafür eingerichteten Schutzmaßnahmen (z. B. Datensicherung) nicht wirksam waren,

  sowie die eingeleiteten Maßnahmen des Cloud-Anbieters, um derartigen Vorkommnissen in Zukunft vorzubeugen.

Ein Vorkommnis ist typischerweise dann bedeutsam, wenn mehrere Cloud-Kunden davon betroffen waren und die Betroffenen selbst oder die Öffentlichkeit durch den Cloud-Anbieter darüber informiert wurden. Die Informationen zu den Vorkommnissen und den eingerichteten Schutzmaßnahmen müssen so weit wie möglich transparent gemacht werden, ohne dabei Schwachstellen und potenzielle Angriffsflächen preiszugeben. Ferner darf die Berichterstattung die Vertraulichkeit von Informationen, die einzelne Cloud-Kunden betreffen, nicht gefährden und soll daher keine kleinteilige Darstellung vieler Einzelvorkommnisse enthalten.

Die Systembeschreibung darf keine Informationen auslassen bzw. verzerren, die für die Erfüllung der anwendbaren C5-Kriterien relevant sind. Das bedeutet nicht, dass sämtliche Aspekte des dienstleistungsbezogenen internen Kontrollsystems darzustellen sind, die aus Sicht einzelner Kunden des Cloud-Dienstes als wichtig erachtet werden können. Zu beachten ist, dass mit der Systembeschreibung für die Vielzahl der Kunden ein angemessenes Niveau an Transparenz erreicht werden soll und die Prozesse in Teilen kundenindividuell ausgestaltet sein können.

Bei einer direkten Prüfung hat der Wirtschaftsprüfer die oben genannten Mindestinhalte in der Berichterstattung in allen wesentlichen Belangen darzustellen, damit sich die vorgesehenen Kunden ein angemessenes Bild von der Informationssicherheit des Cloud-Dienstes einschließlich der angewandten Grundsätze, Verfahren und Maßnahmen verschaffen können. Dies schließt hinreichende Angaben zu den Rahmenbedingungen des Cloud-Dienstes ein (vgl. Abschnitt 5).

4.4.4.2 Erklärung der gesetzlichen Vertreter

In der Erklärung der gesetzlichen Vertreter bestätigen diese, dass

- die Systembeschreibung die tatsächliche Ausgestaltung und Einrichtung des dienstleistungsbezogenen internen Kontrollsystems zum zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) bzw. während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2) sachgerecht darstellt und die Mindestinhalte gemäß Abschnitt 4.4.4.1 dieses Kriterienkatalogs enthalten sind,
- die in der Systembeschreibung dargestellten Kontrollen zum zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) bzw. während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2) angemessen ausgestaltet und eingerichtet sind, um die anwendbaren C5-Kriterien zu erfüllen und
- sofern beauftragt, die in der Systembeschreibung dargestellten Kontrollen (Berichterstattung vom Typ 2) während des zu prüfenden Zeitraums wirksam sind.

4.4.5 Berücksichtigung von Subdienstleistungsunternehmen

Gegebenenfalls lagert der Cloud-Anbieter Teile seiner Geschäftsprozesse zur Bereitstellung des Cloud-Dienstes auf weitere Dienstleistungsunternehmen aus (Einsatz von Subdienstleistungsunternehmen). Dies

muss der Cloud-Anbieter in seiner Systembeschreibung darstellen und der Wirtschaftsprüfer in der Prüfung entsprechend berücksichtigen. Die Prüfungsstandards ISAE 3402 bzw. IDW PS 951 n.F. unterscheiden für die Prüfung einer Erklärung dabei zwischen der „Inclusive Methode" und die „Carve-out Methode".

- Inclusive Methode: Bei der Inclusive Methode ist auch das dienstleistungsbezogene interne Kontrollsystem des Subdienstleistungsunternehmens Gegenstand der Systembeschreibung und deren Prüfung. Daher beurteilt der Wirtschaftsprüfer auch die Kontrollen des Subdienstleistungsunternehmens auf deren Angemessenheit und ggf. Wirksamkeit. Insofern liefert die Inclusive Methode eine Berichterstattung über die Prüfung des dienstleistungsbezogenen internen Kontrollsystems beim Dienstleistungsunternehmen und dessen Subdienstleistungsunternehmen.
- Carve-out Methode: Bei dieser Methode erfolgt lediglich eine Beschreibung der von dem Subdienstleistungsunternehmen erbrachten Dienstleistungen gemäß den Mindestinhalten der Systembeschreibung (vgl. Abschnitt 4.4.4.1). Eine Darstellung der Kontrollen des Subdienstleistungsunternehmens erfolgt nicht. Stattdessen hat die Systembeschreibung des Dienstleistungsunternehmens diejenigen Kontrollen darzustellen, die der Überwachung der Wirksamkeit der Kontrollen beim Subdienstleistungsunternehmen dienen. Dieser Kriterienkatalog enthält im Bereich „Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)“ entsprechende Kriterien.

Der Cloud-Anbieter hat die anzuwendende Methode nach eigenem Ermessen auszuwählen und in der Systembeschreibung entsprechend kenntlich zu machen (vgl. Abschnitt 4.4.4.1 zu Mindestinhalten der Systembeschreibung).

Ein Dienstleistungsunternehmen ist nach diesem Kriterienkatalog ein Subdienstleistungsunternehmen, wenn die beiden folgenden Eigenschaften zutreffen:

- Die vom Dienstleistungsunternehmen erbrachten Leistungen sind für das Verständnis der Kunden bezüglich der anwendbaren C5-Kriterien wahrscheinlich relevant.
- Korrespondierende Kontrollen beim Dienstleistungsunternehmen sind erforderlich, um zusammen mit den Kontrollen des Cloud-Anbieters, die anwendbaren C5-Kriterien mit hinreichender Sicherheit zu erfüllen.

Soweit die Kontrollen des Cloud-Anbieters, einschließlich dessen Kontrollen zur Überwachung der Wirksamkeit der Kontrollen des Dienstleistungsunternehmens, die anwendbaren C5-Kriterien mit hinreichender Sicherheit erfüllen, handelt es sich nicht um einen Subdienstleister im Sinne dieses Kriterienkatalogs.

Erfolgt die Bereitstellung des Cloud-Dienstes aus Rechenzentren, die von Dritten betrieben werden, ist insbesondere hinsichtlich des Bereichs „Physische Sicherheit (PS)“ grundsätzlich anzunehmen, dass die obigen Eigenschaften zutreffen und ein Subdienstleisterverhältnis im Sinne dieses Kriterienkatalogs vorliegt. Gleiches gilt z. B. für den Bereich „Regelbetrieb (OPS)“ bei Bereitstellung einer Software unter Nutzung der Infrastruktur oder Plattform eines anderen Cloud-Anbieters. Das Kriterium der Relevanz für den Nutzer, wie auch das Erfordernis von korrespondierenden Kontrollen trifft z. B. bei Geschäftsbeziehungen des Cloud-Anbieters zu Reinigungsfirmen oder Werbeagenturen typischerweise nicht zu.

Im Falle einer direkten Prüfung gelten die obigen Ausführungen sinngemäß.

4.4.6 Beurteilen der Erfüllung von Kriterien bei der Prüfung einer Erklärung

Soweit der Cloud-Anbieter bereits Prüfungen nach anderen Standards und Publikationen durchführen lässt, kann es vorkommen, dass die in der Systembeschreibung dargestellten Kontrollen zwar optimal auf die

Kriterien dieser Standards und Publikationen abgestimmt sind, ihre Beschreibung jedoch nicht alle Bestandteile der C5-Kriterien, denen sie zugeordnet sind, vollständig erfüllen.

Soweit der Cloud-Anbieter für nicht abgedeckte Bestandteile der C5-Kriterien Nachweise über zusätzliche, bisher nicht in der Systembeschreibung dargelegte, aber tatsächlich eingerichtete Kontrollen erbringen kann, hat der Cloud-Anbieter diese Kontrollen in die Systembeschreibung aufzunehmen oder die bestehenden Kontrollbeschreibungen anzupassen und diese Änderungen in geeigneter Form darzustellen.

Auf eine Anpassung der Systembeschreibung kann verzichtet werden, soweit aus der Beschreibung der Prüfungshandlungen des Wirtschaftsprüfers nachvollziehbar hervorgeht, wie er die nicht über die Kontrollbeschreibung abgedeckten Bestandteile der C5-Kriterien geprüft hat. Entsprechende Prüfungshandlungen sind in geeigneter Form zu kennzeichnen (z. B. „Weiterführende Prüfungshandlung zum Beurteilen der vollständigen Erfüllung des C5-Kriteriums“).

Bei einer direkten Prüfung gilt dies sinngemäß.

4.4.7 Beurteilung von Abweichungen

Der Umgang mit festgestellten Abweichungen ist in den Prüfungsstandards geregelt. Zur Beurteilung, ob anwendbare C5-Kriterien durch festgestellte Abweichungen nicht erfüllt werden und das Prüfungsurteil einzuschränken ist, hat der Wirtschaftsprüfer folgende Prüfungshandlungen in Betracht ziehen:

- Befragung des Managements des Cloud-Anbieters, bzgl. dessen Bewertung der Ursache der festgestellten Abweichung;
- Würdigung des Umgangs des Cloud-Anbieters mit der festgestellten Abweichung;
- Prüfung, ob vergleichbare Abweichungen in den Überwachungsprozessen des Cloud-Anbieters identifiziert und welche Maßnahmen daraufhin veranlasst wurden;
- Prüfung, ob kompensierende Kontrollen eingerichtet und wirksam sind, um den aus der Abweichung resultierenden Risiken derart entgegenzuwirken, dass das C5-Kriterium mit hinreichender Sicherheit erfüllt wird. Dies betrifft beispielsweise die Würdigung alternativer organisatorischer und technischer Ansätze des Cloud-Anbieters, die anwendbaren C5-Kriterien zu erfüllen, die bei der Beschreibung der Kriterien dieses Kriterienkatalogs nicht berücksichtigt wurden.

Unabhängig von der Beurteilung, ob eine Abweichung zu einer Einschränkung des Prüfungsurteils führt, sollen der Berichterstattung darüber hinaus weitere Informationen entnehmbar sein. Diese Informationen sollen es den Berichtsadressaten ermöglichen, zu beurteilen, ob der Cloud-Anbieter erkennbare Maßnahmen zur Fehlerbeseitigung und Optimierung seiner Grundsätze, Verfahren und Maßnahmen durchführt. Vor diesem Hintergrund sind in die Berichterstattung folgende Zusatzinformationen des Cloud-Anbieters aufzunehmen:

- Sofern die Abweichung vom Cloud-Anbieter selbst erkannt wurde, ist anzugeben, wann und im Zuge welcher Maßnahmen die Abweichung erkannt wurde.
- Sofern die Abweichung bereits Gegenstand der Berichterstattung über einen vorhergehenden Prüfungszeitraum war, ist anzugeben, wann und im Zuge welcher Maßnahmen die Abweichung erkannt wurde; verbunden mit einem gesonderten Hinweis, dass die Entdeckung in einem vorherigen Prüfungszeitraum erfolgte. Dies setzt voraus, dass der Wirtschaftsprüfer auf vorherige Berichterstattungen des Cloud-Anbieters zugreifen kann. Im Zweifelsfall hat sich der Wirtschaftsprüfer die Einsicht dieser Berichte im Zuge seiner Beauftragung gesondert zusichern zu lassen.
- Maßnahmen zur künftigen Behebung der Abweichung und ab wann diese Maßnahmen voraussichtlich abgeschlossen bzw. wirksam eingerichtet sein werden.

Diese Zusatzinformationen sind nicht Gegenstand der Prüfung. Sie können beispielsweise in einem gesondert gekennzeichneten Abschnitt der Systembeschreibung oder im optionalen Abschnitt „5. Sonstige

Informationen, bereitgestellt durch die gesetzlichen Vertreter des Cloud-Anbieters“ erfolgen (vgl. folgender Abschnitt).

4.4.8 Berichterstattung

Die Berichterstattung über die Prüfung einer Erklärung orientiert sich an den Vorgaben aus ISAE 3402 bzw. IDW PS 951 n.F. Im Falle einer direkten Prüfung finden diese sinngemäß Anwendung. Näheres regelt der folgende Abschnitt.

Bei der Prüfung einer Erklärung umfasst die Berichterstattung die folgenden Bestandteile:

1 Prüfungsbericht des unabhängigen Wirtschaftsprüfers
   a. Auftrag, zugrundeliegende C5 Version und Prüfungsumfang
   b. Verantwortung der gesetzlichen Vertreter des Cloud-Anbieters bzw. des für den/die geprüften Cloud-Dienst(e) verantwortlichen Managements des Cloud-Anbieters
   c. Unabhängigkeit und Qualitätssicherung des Wirtschaftsprüfers/der Wirtschaftsprüfungsgesellschaft (einschließlich Angaben zur Erfüllung der Qualifikationsanforderungen, vgl. Abschnitt 4.4.9)
   d. Verantwortung des Wirtschaftsprüfers
   e. Inhärente Grenzen von Kontrollen bei Dienstleistungsunternehmen
   f. Prüfungsurteil
   g. Adressaten und Nutzung der Bescheinigung
   h. Hinweis auf die Auftragsbedingungen
2 Erklärung der gesetzlichen Vertreter des Cloud-Anbieters bzw. des für den/die Cloud-Dienst(e) verantwortlichen Managements des Cloud-Anbieters
3 Systembeschreibung des Cloud-Anbieters
4 Darstellung der C5-Kriterien und der zugeordneten Kontrollen (Teil der Systembeschreibung), sowie Darstellung der durchgeführten Prüfungshandlungen und der einzelnen Prüfungsergebnisse des Wirtschaftsprüfers
5 Optional in einem gesonderten Abschnitt: Sonstige Informationen, bereitgestellt durch die gesetzlichen Vertreter des Cloud-Anbieters (diese Informationen sind nicht vom Prüfungsurteil abgedeckt)

Im Falle einer direkten Prüfung entfallen die Bestandteile 2 „Erklärung der gesetzlichen Vertreter“ und 3 „Systembeschreibung“. Gleichwohl sind die im Abschnitt 4.4.4.1 genannten Mindestinhalte der Systembeschreibung in der Berichterstattung in allen wesentlichen Belangen darzustellen, damit sich die vorgesehenen Kunden ein angemessenes Bild von der Informationssicherheit des Cloud-Dienstes einschließlich der angewandten Grundsätze, Verfahren und Maßnahmen verschaffen können. Dies schließt hinreichende Angaben zu den Rahmenbedingungen des Cloud-Dienstes ein (vgl. Abschnitt 5). Entsprechende Angaben sind in einem separaten Abschnitt zu machen, z. B. „Darstellung des Cloud-Dienstes und der vom Cloud-Anbieter angewendeten Grundsätze, Verfahren und Maßnahmen“.

Die durchgeführten Prüfungshandlungen sind sowohl bei Prüfungen der Angemessenheit (Berichterstattung vom Typ 1) als auch der Wirksamkeit (Berichterstattung vom Typ 2) darzustellen.

4.4.9 Qualifikation des Prüfers

Gemäß des ISAE 3000 (Revised) / IDW PS 860 hat der Prüfer sich vor Auftragsannahme davon zu überzeugen, dass die Berufspflichten (für Wirtschaftsprüfer § 43 WPO), einschließlich der Pflicht zur Unabhängigkeit, eingehalten werden. Auf Grundlage seiner Kenntnisse über den Prüfungsgegenstand hat der Prüfer zu beurteilen, ob das mit der Prüfung betraute Prüfungsteam über die für die Durchführung der

Prüfung notwendigen Fach- und Branchenkenntnisse verfügt sowie ausreichende Erfahrungen mit den einschlägigen formalen Anforderungen vorliegen oder erlangt werden können.

Nach Auffassung des BSI stellen Prüfungen auf Grundlage dieses Kriterienkataloges besondere Anforderungen an die Qualifikation des Prüfers und des Prüfungsteams. Aus Sicht des BSI sind die nachfolgend aufgeführten Aspekte zu Berufsqualifikationen und Berufserfahrung geeignete Indizien, die erwarten lassen, dass diese besonderen Anforderungen erfüllt werden. Daher sollen die folgenden Aspekte durch jene Mitglieder des Prüfungsteams erfüllt werden, die gemäß des International Standard on Quality Control (ISQC) 1 „Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements" bzw. des damit in Einklang stehenden deutschen IDW Qualitätssicherungsstandards „Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis" (IDW QS 1) oder anderer nationaler Äquivalente des ISQC 1, die laufende Überwachung der Auftragsabwicklung und die abschließende Durchsicht der Auftragsergebnisse (einschließlich Würdigung der Arbeiten, der Dokumentation und der geplanten Berichterstattung) durchführen:

- 3 Jahre relevante Berufserfahrung mit IT-Prüfungen in der Wirtschaftsprüfung

oder eine der folgenden Berufsexamina/ Zertifizierungen:

- Information Systems Audit and Control Association (ISACA) – Certified Information Systems Auditor (CISA) oder Certified Information Security Manager (CISM) oder Certified in Risk and Information Systems Control (CRISC)
- ISO/ IEC 27001 Lead Auditor oder vom BSI zertifizierter ISO 27001-Auditor für Audits auf der Basis von BSI IT-Grundschutz
- Cloud Security Alliance (CSA) – Certificate of Cloud Security Knowledge (CCSK)
- (ISC)² – Certified Cloud Security Professional (CCSP)

Auf Anfrage des Auftraggebers hat der Prüfer in geeigneter Form nachzuweisen, dass das Prüfungsteam die Qualifikationsanforderungen erfüllt.

Die Erfüllung der Qualifikationsanforderungen ist im Abschnitt „Unabhängigkeit und Qualitätssicherung des Wirtschaftsprüfers/der Wirtschaftsprüfungsgesellschaft" der Bescheinigung des unabhängigen Wirtschaftsprüfers zu bestätigen.

4.4.10 Angaben zur Haftungsbegrenzung

Nach Auffassung des BSI sind Angaben zu Haftungsregelungen für den Berichtsempfänger eine wichtige Information.

Die Regelungen zur Haftung des Prüfers – bei Prüfungen außerhalb von gesetzlichen Vorbehaltsaufgaben – richten sich grundsätzlich nach zivilrechtlichen Vorgaben und können durch vertragliche Vereinbarung konkretisiert werden. Eine Haftungsvereinbarung kann individuell oder durch Verwendung vorformulierter Vertragsbedingungen getroffen werden.

Vor diesem Hintergrund ist in der Berichterstattung über die Prüfung auf eine getroffene Haftungsvereinbarung hinzuweisen.

Die Ausführungen hierzu können beispielsweise im Abschnitt „Hinweis auf die Auftragsbedingungen" (ggf. mit Verweis auf weitere Anlagen) erfolgen.

4.5 Umgang mit Aktualisierungen des Kriterienkataloges

Das BSI beabsichtigt diesen Kriterienkatalog entsprechend der allgemeinen technischen Entwicklungen und auch der laufenden Fortentwicklung der zugrundeliegenden Standards, regelmäßig zu aktualisieren.

Cloud-Anbieter und Prüfer sollen in diesem Zusammenhang über ausreichend Zeit verfügen, um die mit der Aktualisierung dieses Kriterienkataloges verbundenen Anpassungen der Systeme und Prozesse sowie der Prüfungsdurchführung vorzunehmen.

Die Kriterien in diesem Kriterienkatalog sind daher für zu prüfende Zeiträume anzuwenden, die am oder nach dem 15. Februar 2021 enden. Eine frühere Anwendung dieser Kriterien ist zulässig.

Im Verlauf eines Prüfungszeitraums kann es vorkommen, dass sich die Beurteilung der Wirksamkeit der vom Cloud-Anbieter angewandten Grundsätze, Verfahren und Maßnahmen sowohl auf den Stand vor, als auch nach Umsetzung entsprechender Anpassungen bezieht. Die vorgenommenen Anpassungen sind in der Systembeschreibung darzulegen (vgl. Abschnitt 4.4.4.1). Bei einer direkten Prüfung hat der Prüfer diese Informationen einzuholen und darzulegen.

Soweit der Prüfungszeitraum in einem Zeitraum endet, der bis zu drei Monate vor dem 15. Februar 2021 liegt, muss der Cloud-Anbieter in der Systembeschreibung ergänzende Angaben auch zu den noch erforderlichen und noch nicht abgeschlossenen Änderungen an seinem dienstleistungsbezogenen internen Kontrollsystem machen. Hieraus muss auch hervorgehen, wann diese Änderungen an seinem dienstleistungsbezogenen internen Kontrollsystem abgeschlossen bzw. wirksam eingerichtet sein sollen. Bei einer direkten Prüfung hat der Prüfer diese Informationen einzuholen und darzulegen.

5 Angaben zu den Rahmenbedingungen des Cloud-Dienstes

Die Angaben zu den Rahmenbedingungen des Cloud-Dienstes dienen der zusätzlichen Information der Kunden über das vom Cloud-Dienst gebotene Niveau an Informationssicherheit. Die Angaben ermöglichen den Cloud-Kunden, die Eignung des Cloud-Dienstes für ihren Anwendungsfall zu beurteilen. Sie sollen außerdem ein vergleichbares Niveau in der Berichterstattung sicherstellen, um Kunden das Vergleichen mehrerer Cloud-Anbieter bzw. Cloud-Dienste, für die ein C5-Bericht ausgestellt wurde, zu erleichtern.

Da die Prüfungsdurchführung bei einer direkten Prüfung nicht auf einer vom Cloud-Anbieter bereitgestellten Systembeschreibung basiert, hat der Prüfer in diesem Fall die Angaben zu den Rahmenbedingungen gemäß der vom Cloud-Anbieter zur Verfügung gestellten Informationen zu dokumentieren.

BC-01 Angaben zu Gerichtsbarkeit und Lokationen

Angaben zu den Rahmenbedingungen des Cloud-Dienstes

Der Cloud-Anbieter macht in der Systembeschreibung und den vertraglichen Vereinbarungen (z. B. Leistungsbeschreibung) nachvollziehbare und transparente Angaben zu

- seiner Gerichtsbarkeit, und
- Lokationen der Daten der Cloud-Kunden bei der Verarbeitung, Sicherung und Speicherung auf Systemkomponenten zur Bereitstellung des Cloud-Dienstes im Verantwortungsbereich des Cloud-Anbieters, einschließlich seiner Unterauftragnehmer.

Der Umfang der Angaben orientiert sich am Bedarf sachverständigen Personals der Cloud-Kunden, die Vorgaben zur Informationssicherheit machen, diese umsetzen oder die Umsetzung überprüfen und die Eignung des Cloud-Dienstes aus rechtlicher und regulatorischer Sicht beurteilen (z. B. IT, Compliance, Interne Revision).

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Falls die Verarbeitung, Sicherung und Speicherung von Daten der Cloud-Kunden aus unterschiedlichen Standorten heraus erfolgt, so ist dies in der Systembeschreibung nachvollziehbar und transparent darzustellen.

BC-02 Angaben zu Verfügbarkeit und Störungsbeseitigung im Normalbetrieb

Angaben zu den Rahmenbedingungen des Cloud-Dienstes

Der Cloud-Anbieter macht in vertraglichen Vereinbarungen (z. B. Leistungsbeschreibung) nachvollziehbare, verbindliche und transparente Angaben zur

- Verfügbarkeit des Cloud-Dienstes
- Kategorisierung und Priorisierung von Störungen;
- Reaktionszeit bei Störungen im Normalbetrieb gemäß der Kategorisierung (Zeitraum bis zum Beginn der Störungsbeseitigung durch den Cloud-Anbieter nach Meldung der Störung);
- Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung) und
- Rechtsfolgen bei Nichteinhaltung.

Die Angaben basieren auf Definitionen, die sachverständiges Personal der Cloud-Kunden eine Beurteilung des Cloud-Dienstes hinsichtlich geschäftlicher Anforderungen ermöglichen. In der Systembeschreibung ist beschrieben, wo diese Angaben auffindbar sind. Soweit die Angaben zur Verfügbarkeit und Störungsbeseitigung nur Durchschnittswerte darstellen, die im Einzelfall nicht verbindlich sind, wird dies gesondert hervorgehoben.

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Neben der Information in der Systembeschreibung, wo diese Angaben auffindbar sind, können die Angaben selbst auch optionaler Bestandteil der Berichterstattung sein, z. B. in einem Abschnitt "Sonstige Informationen, bereitgestellt durch die gesetzlichen Vertreter des Cloud-Anbieters". Der Wirtschaftsprüfer gibt über die Angaben selbst kein Prüfungsurteil ab.

BC-03 Angaben zu Wiederanlaufparametern im Notbetrieb

Der Cloud-Anbieter stellt sachverständigem Personal der Cloud-Kunden im Bedarfsfall nachvollziehbare und transparente Angaben zu folgenden Wiederanlaufparametern des Cloud-Dienstes zur Verfügung:

- Maximal tolerierbare Ausfallzeit / Recovery Time Objective (RTO)
- Maximal zulässiger Datenverlust / Recovery Point Objective (RPO)
- Wiederanlaufzeit zur Aufnahme des Notbetriebs
- Wiederanlauf-Niveau (Kapazität bezogen auf den Normalbetrieb)
- Wiederherstellungszeit zum Normalbetrieb

Die Angaben ermöglichen den Cloud-Kunden, eine Beurteilung des Cloud-Dienstes im Rahmen ihrer eigenen Business Impact Analyse durchzuführen.

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Neben der Information in der Systembeschreibung, wo diese Angaben auffindbar sind, können die Angaben selbst auch optionaler Bestandteil der Berichterstattung sein, z. B. in einem Abschnitt "Sonstige Informationen, bereitgestellt durch die gesetzlichen Vertreter des Cloud-Anbieters". Der Wirtschaftsprüfer gibt über die Angaben selbst kein Prüfungsurteil ab.

BC-04 Angaben zur Verfügbarkeit der Rechenzentren

Der Cloud-Anbieter stellt sachverständigem Personal der Cloud-Kunden im Bedarfsfall nachvollziehbare und transparente Angaben über die Verfügbarkeit der Rechenzentren zur Verfügung, die zur Bereitstellung des Cloud-Dienstes genutzt werden (einschließlich von Unterauftragnehmern betriebene Rechenzentren). Aus den Angaben gehen die Verfügbarkeiten und Ausfallzeiten bezogen auf ein Jahr gemäß branchenüblicher Klassifikationssysteme hervor. Die Angaben ermöglichen den Cloud-Kunden eine Beurteilung des Cloud-Dienstes im Rahmen ihrer Business Impact Analyse durchzuführen.

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Eine branchenübliche Klassifizierung ist das Tier-Klassifikationssystem des Uptime Institute. Dieses sieht folgende Stufen (Tier) für die Verfügbarkeiten und Ausfallzeiten bezogen auf ein Jahr vor:

- Tier I: 99,671 %; bis zu 28,8 Stunden kumulierte Ausfallzeit pro Jahr
- Tier II: 99,741 %; bis zu 22,7 Stunden kumulierte Ausfallzeit pro Jahr
- Tier III: 99,982 %; bis zu 1,6 Stunden kumulierte Ausfallzeit pro Jahr
- Tier IV: 99,995 %; bis zu 25 Minuten kumulierte Ausfallzeit pro Jahr

Werden Anforderungen an die Hochverfügbarkeit eines Rechenzentrums gestellt, eignet sich der HV-Benchmark des BSI, der folgende Verfügbarkeitsklassen (VK) vorsieht:

- VK 0: ohne Anforderungen an die Verfügbarkeit (~ 95%); bis zu 438 Stunden kumulierte Ausfallzeit pro Jahr
- VK 1: normale Verfügbarkeit (99%); bis zu 88 Stunden kumulierte Ausfallzeit pro Jahr
- VK 2: hohe Verfügbarkeit (99,9%); bis zu 9 Stunden kumulierte Ausfallzeit pro Jahr
- VK 3: sehr hohe Verfügbarkeit (99,99%); bis zu 53 Minuten kumulierte Ausfallzeit pro Jahr
- VK 4: höchste Verfügbarkeit (99,999%); bis zu 6 Minuten kumulierte Ausfallzeit pro Jahr

- VK 5: Desaster-tolerant

Die Angaben können optionaler Bestandteil der Berichterstattung sein, z. B. in einem Abschnitt "Sonstige Informationen, bereitgestellt durch die gesetzlichen Vertreter des Cloud-Anbieters". Der Wirtschaftsprüfer gibt über die Angaben selbst kein Prüfungsurteil ab.

BC-05 Angaben zum Umgang mit Ermittlungsanfragen staatlicher Stellen

Der Cloud-Anbieter macht in der Systembeschreibung nachvollziehbare und transparente Angaben zum Umgang mit Ermittlungsanfragen staatlicher Stellen für den Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden. Die Angaben umfassen folgende Aspekte:

- Verfahren zur Verifizierung der Rechtsgrundlage solcher Anfragen,
- Verfahren zur Information und Einbindung der betroffenen Cloud-Kunden bei Erhalt solcher Anfragen,
- Widerspruchsmöglichkeiten der betroffenen Cloud-Kunden,
- ob der Cloud-Anbieter bei verschlüsselten Daten der Cloud-Kunden im Falle solcher Anfragen die Möglichkeit zur Entschlüsselung hat und wie er diese für den Zugriff oder die Offenbarung anwendet.

Der Umfang der Angaben orientiert sich am Bedarf sachverständigen Personals der Cloud-Kunden, die Vorgaben zur Informationssicherheit machen, diese umsetzen oder die Umsetzung überprüfen und die Eignung des Cloud-Dienstes aus rechtlicher und regulatorischer Sicht beurteilen (bspw. IT, Compliance, Interne Revision).

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Die Rechtsgrundlagen, auf die sich diese Stellen (bspw. Strafverfolgungsbehörden, Geheimdienste) stützen, sind regional unterschiedlich. Dabei ist insbesondere die anwendbare Jurisdiktion an den Lokationen zu berücksichtigen, an denen Daten der Cloud-Kunden verarbeitet, gespeichert, gesichert und aufbewahrt werden.

In Deutschland sind derartige Befugnisse in den Gesetzen des Bundeskriminalamts (oder der Gesetze der jeweiligen Landesämter), verschiedenen Prozessordnungen für Gerichte und den Gesetzen für die Nachrichtendienste (BNDG, BVerfSchG, jeweilige Gesetze über die Verfassungsschutzämter der Länder, MADG) und dem G10-Gesetz geregelt.

In anderen Ländern sind andere Gesetze einschlägig und dem Cloud-Kunden ggf. nur vereinzelt aus den Medien bekannt, z. B. der CLOUD Act ("Clarifying Lawful Overseas Use of Data Act") aus den USA oder das Cyber Security Law der Volkrepublik China. In Verbindung mit den anderen Informationen zum Cloud-Dienst soll es dem Kunden möglich sein, mit diesen Informationen eine Risikoabschätzung der eigenen Betroffenheit vorzunehmen.

BC-06 Angaben zu Zertifizierungen oder Bescheinigungen

Der Cloud-Anbieter macht in seiner Systembeschreibung nachvollziehbare und transparente Angaben zu vorhandenen und gültigen Zertifizierungen oder Bescheinigungen unabhängiger Dritter in Bezug auf die folgenden Aspekte des Cloud-Dienstes:

- Konformität der Managementsysteme für Informationssicherheit, Business Continuity und Qualität mit anwendbaren internationalen Standards,
- Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO),
- Angemessenheit und Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems in Bezug auf geeignete Kriterien,
- Zertifizierungen oder Bescheinigungen zu branchenspezifischen Anforderungen der Cloud-Kunden.

Soweit für die Zertifizierung oder Bescheinigung anwendbar, werden folgende Angaben gemacht:

- Datum der Ausstellung
- ausstellende Organisation

- Zeitpunkt oder Zeitraum der Gültigkeit bzw. der Abdeckung.

Der Umfang der Angaben orientiert sich am Bedarf sachverständigen Personals der Cloud-Kunden, die Vorgaben zur Informationssicherheit machen, diese umsetzen oder die Umsetzung überprüfen und die Eignung des Cloud-Dienstes aus rechtlicher und regulatorischer Sicht beurteilen (bspw. IT, Compliance, Interne Revision).

Ergänzende Informationen - Hinweise zu den Rahmenbedingungen

Die Transparenz kann zusätzlich durch Offenlegung von SLAs, die auf dem ISO/IEC 19086 oder vergleichbaren Standards basieren, erhöht werden.

Die Erfüllung der Rahmenbedingung setzt nicht voraus, dass der Cloud-Anbieter zu allen genannten Aspekten eine Zertifizierung oder Bescheinigung vorhält.

6 Basiskriterien, Zusatzkriterien und ergänzende Informationen

6.1 Organisation der Informationssicherheit (OIS)

Zielsetzung: *Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation.*

OIS-01 Informationssicherheits-managementsystem (ISMS)

Basiskriterium

Der Cloud-Anbieter betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001. Der Anwendungsbereich des ISMS umfasst die Organisationseinheiten, Standorte und Verfahren des Cloud-Anbieters zur Bereitstellung des Cloud-Dienstes.

Die Maßnahmen für Aufbau, Verwirklichung, Aufrechterhaltung und fortlaufende Verbesserung des ISMS sind dokumentiert. Die Dokumentation umfasst:

- Anwendungsbereich des ISMS (Abschnitt 4.3 von ISO/IEC 27001)
- Erklärung zur Anwendbarkeit (Abschnitt 6.1.3)
- Ergebnisse der letzten Managementbewertung (Abschnitt 9.3).

Zusatzkriterium

Das Informationssicherheitsmanagementsystem (ISMS) weist eine gültige Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz auf.

Ergänzende Informationen

Zum Kriterium

Das Basiskriterium kann auch ohne gültige Zertifizierung des ISMS nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz erfüllt werden, soweit die vorgelegte Dokumentation die Anforderungen der ISO/IEC 27001 erfüllt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche Prüfung des ISO 27001 Zertifikats ist teilweise möglich, da das Vorhandensein eines Zertifikats kontinuierlich überprüft werden kann, indem das Erstellungsdatum eingelesen wird und die Authentizität geprüft wird. Allerdings ist das Zertifikat in der Regel für drei Jahre ausgestellt und es werden sich im Regelfall keine dynamischen Veränderungen ergeben.

OIS-02 Leitlinie zur Informationssicherheit

Basiskriterium

Die oberste Leitung des Cloud-Anbieters hat eine Leitlinie zur Informationssicherheit verabschiedet und an die internen und externen Mitarbeiter sowie die Cloud-Kunden kommuniziert. Die Leitlinie beschreibt

- den Stellenwert der Informationssicherheit, abgeleitet von den Anforderungen der Cloud-Kunden mit Bezug zur Informationssicherheit,
- die Sicherheitsziele und das angestrebte Sicherheitsniveau, abgeleitet von den Geschäftszielen und Aufgaben des Cloud-Anbieters,
- die wichtigsten Aspekte der Sicherheitsstrategie zum Erreichen der gesetzten Sicherheitsziele

- die Organisationsstruktur für Informationssicherheit im Anwendungsbereich des ISMS.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die oberste Leitung ist eine natürliche Person oder Personengruppe, welche die letztgültige Entscheidung für die Institution trifft und für diese die Verantwortung trägt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dieses automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OIS-03 Schnittstellen und Abhängigkeiten

Basiskriterium

Schnittstellen und Abhängigkeiten zwischen Tätigkeiten zur Bereitstellung des Cloud-Dienstes, die vom Cloud-Anbieter selbst durchgeführt werden und Tätigkeiten, die von Dritten durchgeführt werden, sind dokumentiert und kommuniziert. Dies umfasst den Umgang mit folgenden Ereignissen:

- Schwachstellen
- Sicherheitsvorfälle und
- Störungen

Art und Umfang der Dokumentation orientieren sich am Informationsbedarf sachverständigen Personals der betroffenen Organisationen, um die Tätigkeiten angemessen durchführen zu können.

Die Kommunikation von Änderungen an den Schnittstellen und Abhängigkeiten erfolgt so zeitnah, dass die betroffenen Dritten mit organisatorischen und technischen Maßnahmen angemessen darauf reagieren können, bevor diese wirksam werden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Der Cloud-Anbieter kann die im Basiskriterium beschriebenen Schnittstellen und Abhängigkeiten beispielsweise in Richtlinien und Anweisungen definieren und dokumentieren. Mitwirkungspflichten der Cloud-Kunden sollten in Leistungsbeschreibungen und Verträgen beschrieben werden.

Dritte im Sinne dieses Basiskriteriums sind z. B. Cloud-Kunden und Subdienstleister.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass Richtlinien und Vorgaben zur Einhaltung vertraglich festgehaltener Vereinbarungen mit dem Cloud-Anbieter bezüglich Verantwortlichkeiten, Mitwirkungspflichten sowie Schnittstellen zum Melden von Sicherheitsvorfällen angemessen definiert, dokumentiert und eingerichtet sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Schnittstellen und Abhängigkeiten können sich zwar ad-hoc verändern, jedoch ist eine automatisierte kontinuierliche Prüfung auf kritische Abhängigkeiten und Schnittstellen derzeit nur mit sehr großem Aufwand möglich.

OIS-04 Aufgabentrennung

Basiskriterium

Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind auf Basis einer Risikobeurteilung gemäß OIS-06 getrennt, um Risiken unbefugter oder unbeabsichtigter Änderungen oder Missbrauch der im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten der Cloud-Kunden zu reduzieren.

Die Risikobeurteilung umfasst folgende Bereiche, soweit diese zur Bereitstellung des Cloud-Dienstes anwendbar sind und im Verantwortungsbereich des Cloud-Anbieters liegen:

- Verwaltung von Rechteprofilen, Genehmigung und Zuweisung von Zugangs- und Zugriffsberechtigungen (vgl. IDM-01),
- Entwicklung, Test und Freigabe von Änderungen (vgl. DEV-01),
- Betrieb der Systemkomponenten.

Kann aus organisatorischen oder technischen Gründen keine Trennung eingerichtet werden, sind Maßnahmen zur Überwachung der Tätigkeiten eingerichtet, um unbefugte oder unbeabsichtigte Änderungen sowie Missbrauch aufzudecken und entsprechende Gegenmaßnahmen einzuleiten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Identifizierte Ereignisse, die möglicherweise unbefugte oder unbeabsichtigte Änderungen an oder Missbrauch von Daten der Cloud-Kunden darstellen, können z. B. als Sicherheitsvorfall behandelt werden, vgl. SIM-01.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung ist vor allem bei Änderungen an den Rollenprofilen und Verantwortlichkeiten möglich. Dies würde eine initiale Prüfung der definierten Rollen und Verantwortlichkeiten durch den Cloud-Anbieter voraussetzen. Daraufhin könnten die monatlich neu hinzugefügten oder veränderten Rollen automatisiert und kontinuierlich geprüft werden.

OIS-05 Kontakt zu relevanten Behörden und Interessenverbänden

Basiskriterium

Der Cloud-Anbieter pflegt Kontakte zu relevanten Behörden und Ministerien, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren. Die Informationen fließen in die Verfahren zum Umgang mit Risiken (vgl. OIS-06) und Schwachstellen (vgl. OPS-19) ein.

Zusatzkriterium

Soweit der Cloud-Dienst durch Organisationen des öffentlichen Sektors in Deutschland genutzt wird, pflegt der Cloud-Anbieter Kontakte zum Nationalen IT-Lagezentrum und dem CERT-Bund des BSI.

Ergänzende Informationen

Zum Kriterium

Relevante Kontakte sind beispielsweise:

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- OWASP Foundation
- CERT-Verbünde DFN-CERT, TF-CSIRT etc.

Organisationen des öffentlichen Sektors in Deutschland sind z. B. Behörden und Ministerien.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung der Kontakte des Cloud-Anbieters zu relevanten Behörden und Interessenverbänden kann durch eine fortwährende Übersendung relevanter

Informationen (etwa einer Liste der kontaktierten Stellen oder von Nachweisen für den Erhalt einer Antwort) bewerkstelligt werden. Ein fortwährender Informationseingang demonstriert die konstante Verbindung zu relevanten Behörden und Interessenverbänden. Weiterhin könnte die Verteilung der Information und ggfs. die Dokumentation der Bearbeitung erkannter Risiken und Schwachstellen kontinuierlich für die Abdeckung dieses Kriterium geprüft werden.

OIS-06 Richtlinie für den Umgang mit Risiken

Basiskriterium

Richtlinien und Anweisungen für das Verfahren zum Umgang mit Risiken sind gemäß SP-01 hinsichtlich der folgenden Aspekte dokumentiert, kommuniziert und bereitgestellt:

- Identifikation von Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen innerhalb des Anwendungsbereichs des ISMS und Zuweisung von Risikoeigentümern,
- Analyse der Eintrittswahrscheinlichkeiten und Auswirkungen bei Eintritt sowie Bestimmung des Risikoniveaus,
- Bewertung der Risikoanalyse auf Basis definierter Kriterien zur Risikoakzeptanz und Priorisierung der Behandlung,
- Behandlung der Risiken durch Maßnahmen, einschließlich Genehmigung der Maßnahmen und Akzeptanz der Restrisiken durch Risikoeigentümer,
- Dokumentation der Tätigkeiten zur Anwendung des Verfahrens, um bei wiederholter Anwendung konsistente, gültige und vergleichbare Ergebnisse zu erhalten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die Bestimmung des Risikoniveaus anhand von Eintrittswahrscheinlichkeiten und Auswirkungen kann durch qualitative, semi-quantitative und quantitative Methoden (vgl. ISO 31010) erfolgen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung und Informationen zum aktuellen Überarbeitungs- und Freigabestatus zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OIS-07 Anwendung des Verfahrens für den Umgang mit Risiken

Basiskriterium

Der Cloud-Anbieter wendet das Verfahren zum Umgang mit Risiken anlassbezogen, aber mindestens jährlich an. Beim Identifizieren von Risiken werden folgende Aspekte berücksichtigt, soweit diese für den bereitgestellten Cloud-Dienst anwendbar sind und im Verantwortungsbereich des Cloud-Anbieters liegen:

- Verarbeitung, Speicherung oder Übertragung von Daten der Cloud-Kunden mit unterschiedlichen Schutzbedarfen,
- Auftreten von Schwachstellen und Störungen in technischen Schutzmaßnahmen zur Separierung gemeinsam genutzter Ressourcen,
- Angriffe über Zugangspunkte, einschließlich Schnittstellen, die aus öffentlichen Netzen erreichbar sind,
- Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche, die aus organisatorischen oder technischen Gründen nicht getrennt werden können,

- Abhängigkeiten von Subdienstleistern.

Die Analyse, Bewertung und Behandlung der Risiken, einschließlich der Genehmigung der Maßnahmen und Akzeptanz der Restrisiken, wird mindestens jährlich durch die Risikoeigentümer auf Angemessenheit überprüft.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Dieses Kriterium bezieht sich ausschließlich auf Risiken, die im Verantwortungsbereich des Cloud-Anbieters liegen. Auch beim Auslagern von Tätigkeiten zur Bereitstellung des Cloud-Dienstens auf Subdienstleister verbleibt die Verantwortung für diese Risiken beim Cloud-Anbieter.

Anforderungen an die Maßnahmen zur Behandlung dieser Risiken sind den Kriterien im Bereich „Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)“ zu entnehmen.

Gemeinsam genutzte Ressourcen sind z. B. Netze, Arbeitsspeicher oder Speicher.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Das Verfahren zum Umgang mit Risiken muss mindestens jährlich geprüft werden und ist daher Teil einer zyklischen Prüfung. Eine kontinuierliche Prüfung dieser Anforderung könnte daher nur darin bestehen, das Datum der letzten Überprüfung zurückzugeben.

6.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP)

Zielsetzung: *Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.*

SP-01 Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen

Basiskriterium

Von der Leitlinie zur Informationssicherheit abgeleitete Richtlinien und Anweisungen sind nach einer einheitlichen Struktur dokumentiert. Sie werden sach- und bedarfsgerecht an alle internen und externen Mitarbeiter des Cloud-Anbieters kommuniziert und bereitgestellt.

Die Richtlinien und Anweisungen sind versioniert und von der obersten Leitung des Cloud-Anbieters oder von dazu autorisiertem Personal genehmigt.

Die Richtlinien und Anweisungen beschreiben mindestens die folgenden Aspekte:

- Ziele,
- Anwendungsbereiche,
- Rollen und Verantwortlichkeiten, einschließlich Anforderungen an die Qualifikation des Personals und das Einrichten von Vertretungsregelungen,
- Rollen und Abhängigkeiten von anderen Organisationen (insbesondere Cloud-Kunden und Subdienstleister),
- Maßnahmen zur Umsetzung der Sicherheitsstrategie,
- anwendbare rechtliche und regulatorischer Anforderungen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die sach- und bedarfsgerechte Kommunikation und Bereitstellung sind vor dem Hintergrund der Größe und Komplexität der Organisation des Cloud-Anbieters und der Art des angebotenen Cloud-Dienstes zu beurteilen. Mögliche Kriterien sind:

- Thematisierung der Richtlinien und Anweisungen in der Einarbeitung neuer Mitarbeiter
- Schulung und Informationskampagnen bei Verabschiedung von neuen oder der Überarbeitung bestehender Richtlinien und Anweisungen
- Form der Bereitstellung

Richtlinien und Anweisungen werden zu den folgenden Basiskriterien gefordert und an den angegebenen Stellen inhaltlich näher spezifiziert:

- Richtlinie für den Umgang mit Risiken (OIS-06)
- Richtlinie für den zulässigen Gebrauch und sicheren Umgang mit Assets (AM-02)
- Sicherheitsanforderungen für Räumlichkeiten und Gebäude (PS-01)
- Physische Zutrittskontrolle (PS-04)
- Konzept zum Schutz vor Schadprogrammen (OPS-04)
- Konzept zur Datensicherung und Wiederherstellung (OPS-06)
- Konzept zur Protokollierung und Überwachung (OPS-10)
- Konzept zum Umgang mit Metadaten (OPS-11)
- Konzept zum Umgang mit Schwachstellen, Störungen und Fehlern (OPS-18)
- Richtlinie für Zugangs- und Zugriffsberechtigungen (IDM-01)
- Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung (CRY-01)
- Richtlinien zur Datenübertragung (COS-08)
- Richtlinien zur Entwicklung/Beschaffung von Informationssystemen (DEV-01)
- Richtlinien zur Änderung von Informationssystemen (DEV-03)

- Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter (SSO-01)
- Richtlinie für den Umgang mit Sicherheitsvorfällen (SIM-01)
- Richtlinien und Verfahren zur Business Impact Analyse (BCM-02)
- Richtlinie für die Planung und Durchführung von Audits (COM-02).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

In Bezug auf die Einheitlichkeit und den Inhalt der Richtlinien und Anweisungen besteht der Bedarf einer manuellen Prüfung, daher ist eine kontinuierliche Prüfung nur bedingt zielführend.

Die Kommunikation / Bereitstellung der Richtlinien und Anweisungen kann über verschiedene Register abgefragt werden. Register für alle genehmigten Richtlinien und Anweisungen können als Grundlage für die Überprüfung der über die üblichen Kanäle bereitgestellten Richtlinien / Anweisungen dienen, die sich evtl. mit einer Prüfung der Zugangsberechtigungen kombinieren lässt. Diese Voraussetzungen muss der Cloud-Anbieter zunächst schaffen.

Versionierungen innerhalb des Dokuments nach erneuter Freigabe durch im Berechtigungskonzept definierte Personen (-gruppen) sind automatisiert prüfbar und daher für die kontinuierliche Prüfung geeignet.

SP-02 Überprüfung und Freigabe von Richtlinien und Anweisungen

Basiskriterium

Die Richtlinien und Anweisungen zur Informationssicherheit werden mindestens jährlich durch sachverständiges Personal des Cloud-Anbieters auf ihre Angemessenheit überprüft. Die Überprüfung berücksichtigt mindestens die folgenden Aspekte:

- Organisatorische und technische Änderungen in den Verfahren zur Bereitstellung des Cloud-Dienstes,
- rechtliche und regulatorische Änderungen im Umfeld des Cloud-Anbieters.

Überarbeitete Richtlinien und Anweisungen werden genehmigt, bevor diese Gültigkeit erlangen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche, automatisierte Prüfung der inhaltlichen Änderungen an Richtlinien und Anweisungen ist zum derzeitigen Stand der Technik nur teilweise praktikabel umsetzbar.

Eine kontinuierliche Prüfung der Berechtigung bzw. Sachverständigkeit des Überprüfenden erscheint ebenso nicht zielführend, da dies nicht an feste Parameter einer automatisierten Auswertung gebunden werden kann. Eine kontinuierliche Prüfung dieses Kriteriums könnte daher nur darin bestehen, das Datum der letzten Überprüfung zurückzugeben.

SP-03 Abweichungen von bestehenden Richtlinien und Anweisungen

Basiskriterium

Ausnahmen von Richtlinien und Anweisungen zur Informationssicherheit durchlaufen das Verfahren zum Umgang mit Risiken gemäß OIS-06, einschließlich Genehmigung der Ausnahmen und Akzeptanz der damit einhergehenden Risiken durch die Risikoeigentümer.

Die Genehmigung von Ausnahmen ist dokumentiert, zeitlich befristet und wird mindestens jährlich durch die Risikoeigentümer auf Angemessenheit überprüft.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Ausnahmen im Sinne des Basiskriteriums können organisatorische oder technische Ursachen haben, z. B.:

- eine Organisationseinheit soll von vorgesehen Prozessen und Verfahren abweichen, um Anforderungen eines Cloud-Kunden zu erfüllen,
- einer Systemkomponente fehlen technischen Eigenschaften, um diese gemäß den anwendbaren Anforderungen zu konfigurieren.

Cloud-Kunden können durch geeignete Kontrollen sicherstellen, dass sie sich beim Cloud-Anbieter über Ausnahmen von Richtlinien und Anweisungen zur Informationssicherheit informieren, um die damit einhergehenden Risiken für die eigene Informationssicherheit zu beurteilen und angemessen zu behandeln.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Ausnahmen zu Richtlinien sollen in einem jährlichen Zyklus überprüft werden. Demnach ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass die kontinuierliche Prüfung das Datum der letzten Veränderung der Ausnahmen zu Leitlinien zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt.

Plausibilität oder Sinnhaftigkeit der Änderung in der Ausnahme einer Richtlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

6.3 Personal (HR)

Zielsetzung: *Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.*

HR-01 Überprüfung der Qualifikation und Vertrauenswürdigkeit

Basiskriterium

Die Qualifikation und Vertrauenswürdigkeit aller internen und externen Mitarbeiter des Cloud-Anbieters mit Zugriff auf Daten der Cloud-Kunden oder Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung zuständig sind, wird vor Beginn des Beschäftigungsverhältnisses gemäß der lokalen Gesetzgebung und Regulierung durch den Cloud-Anbieter überprüft. Soweit rechtlich zulässig, umfasst die Überprüfung folgende Bereiche:

- Verifikation der Person durch Personalausweis
- Verifikation des Lebenslaufs
- Verifikation von akademischen Titeln und Abschlüssen
- Führungszeugnis bzw. nationale Pendants
- Bewerten des Risikos der Erpressbarkeit.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Externe Mitarbeiter im Sinne des Kriteriums sind solche, die Tätigkeiten gemäß den Prozessen und Verfahren des Cloud-Anbieters durchführen. Mitarbeiter von Subdienstleistern, die Tätigkeiten nach Prozessen und Verfahren des Subdienstleisters durchführen, fallen nicht unter dieses Kriterium.

Die Überprüfung der Qualifikation und Vertrauenswürdigkeit kann durch einen spezialisierten Dienstleister unterstützt werden. Je nach nationaler Gesetzgebung sind auch nationale Pendants des deutschen Führungszeugnisses zulässig.

Die Bewertung, inwieweit ein potenzieller Mitarbeiter erpressbar ist, kann bspw. durch die Prüfung der Bonität erfolgen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche Prüfung ist hier nur bedingt zielführend, da die dazugehörigen Prozesse und Schritte einmalig im Rahmen einer zyklischen Prüfung getestet werden können. Zudem erschweren lokale Abweichungen in Gesetzen und Regulierungen eine systembasierte Prüfung.

Denkbar wäre eine kontinuierliche Abfrage der im System hinterlegten Prozessschritte bei jeder Neueinstellung bezogen auf die angegebenen Bereiche anhand einer im HR-System gepflegten Liste der Mitarbeiter, in die auch Mitarbeiter bei Neueinstellung eingepflegt werden.

Hierzu müsste der Cloud-Anbieter diese Schritte systembasiert durchlaufen und dokumentieren. Der Prüfer könnte dann mithilfe eines Agenten oder eines angeschlossenen Monitoring-Systems Abweichungen vom Standardprozess erkennen.

HR-02 Beschäftigungs- und Vertragsbedingungen

Basiskriterium

Die internen und externen Mitarbeiter des Cloud-Anbieters werden in Beschäftigungs- und Vertragsbedingungen auf die Einhaltung anwendbarer Richtlinien und Anweisungen mit Bezug zur Informationssicherheit verpflichtet.

Die Leitlinie zur Informationssicherheit sowie die davon abgeleiteten Richtlinien und Anweisungen sind durch die internen und externen Mitarbeiter nachweislich zur Kenntnis zu nehmen, bevor Zugriff auf Daten der Cloud-Kunden oder

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, gewährt wird.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Der Cloud-Anbieter stellt gemäß SP-01 sicher, dass die Richtlinien und Anweisungen den rechtlichen und regulatorischen Anforderungen entsprechen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Bezogen auf die Verpflichtung der Mitarbeiter auf die Einhaltung bestimmter Anforderungen ist eine kontinuierliche Prüfung nicht zielführend, da dies auch im Rahmen der üblichen Prüfungen abgedeckt werden kann, bzw. ein einmaliger Nachweis ausreicht.

Bezogen auf den Nachweis, dass Zugriff auf Daten erst nach Kenntnisnahme der Anweisungen gewährt wurde, ist eine kontinuierliche Prüfung durchaus denkbar und praktikabel. Der Cloud-Anbieter müsste hierfür die Zustimmung/Kenntnisnahme systembasiert gestalten (z. B. mithilfe von Tickets oder Vermerken in der Personalakte des jeweiligen Mitarbeiters). Zudem wäre zu protokollieren, auf welche Daten der Mitarbeiter wann Zugriff erhalten hat. Eine klare Definition und Abgrenzung von Kundendaten sowie Daten in der Produktiv-Umgebung ist erforderlich.

Der Prüfer kann mithilfe dieser Daten einen Soll-Ist-Abgleich durchführen und dementsprechend Abweichungen feststellen. Die Daten könnten mithilfe eines Agenten und/oder eines Monitoring Systems überwacht werden.

HR-03 Programm zur Sicherheitsausbildung und Sensibilisierung

Basiskriterium

Der Cloud-Anbieter betreibt ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm, das von allen internen und externen Mitarbeitern des Cloud-Anbieters regelmäßig durchlaufen wird. Das Programm wird, ausgehend von Änderungen an Richtlinien und Anweisungen sowie der aktuellen Bedrohungslage, regelmäßig aktualisiert und umfasst die folgenden Aspekte:

- Umgang mit Systemkomponenten, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, gemäß den anwendbaren Richtlinien und Anweisungen,
- Umgang mit Daten der Cloud-Kunden gemäß den anwendbaren Richtlinien und Anweisungen,
- Information über die aktuelle Bedrohungslage,
- richtiges Verhalten bei Sicherheitsvorfällen.

Zusatzkriterium

Die durch das Sensibilisierungs- und Schulungsprogramm erzielten Lernerfolge werden zielgruppenbezogen gemessen und ausgewertet. Die Messungen umfassen quantitative und qualitative Aspekte. Die Ergebnisse fließen in die Verbesserung des Sensibilisierungs- und Schulungsangebots ein.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Das Konzept hinter dem Sensibilisierungs- und Schulungsprogramm erfordert keine kontinuierliche Prüfung und ist mit einer zyklischen Prüfung ausreichend abgedeckt.

Allerdings kann das Absolvieren der Schulungen über Schulungsportale nachvollzogen werden. Für eine kontinuierliche Prüfung, dass jeder Mitarbeiter, die für ihn bzw. seine Rollenbeschreibung relevanten Schulungen absolviert und ggf. wiederholt hat, ist beim Cloud-Anbieter eine klare systembasierte Definition der notwendigen Schulungen je Rollenbeschreibung vorzunehmen. Ebenso sind die erwarteten Termine, zu denen die jeweilige Schulung abzulegen ist, zu hinterlegen. Die Dokumentation, dass die Schulung vom Mitarbeiter absolviert, und ggf. erfolgreich mit einer Prüfung abgeschlossen wurde, sollte im selben Portal erfolgen.
Der Prüfer hat dann die Möglichkeit, die Ergebnisse der Schulungen von Mitarbeitern des Cloud-Anbieters auf Abweichungen hin zu untersuchen, indem er die erwarteten Schulungstermine mit dem tatsächlichen Datum, an dem der Mitarbeiter die Schulung absolvierte, automatisiert und kontinuierlich abgleicht.

HR-04 Maßregelungsprozess

Basiskriterium

Bei Verstößen gegen Richtlinien und Anweisungen erfolgen Maßregelungen gemäß eines definierten Prozesses, der folgende Aspekte umfasst:

- Prüfung, ob tatsächlich ein Verstoß vorliegt
- Berücksichtigung der Art und Schwere des Verstoßes sowie dessen Auswirkung.

Die internen und externen Mitarbeiter des Cloud-Anbieters sind über mögliche Maßregelungen informiert.

Die Anwendung von Maßregelungen wird in geeigneter Weise dokumentiert.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Der Cloud-Anbieter stellt gemäß SP-01 sicher, dass die Richtlinien und Anweisungen die anwendbaren rechtlichen und regulatorischen Anforderungen reflektieren.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Kontinuierliche Prüfung nicht zielführend, da die dazugehörigen Prozesse und Schritte einmalig im Rahmen einer zyklischen Prüfung getestet werden können.

Eine systembasierte Definition der Verstöße sowie dazugehöriger Maßregelungen erscheint nicht praktikabel, da in diesem Zusammenhang häufig Einzelfallentscheidungen notwendig sind, die von vordefinierten Algorithmen nicht abzudecken sind.

HR-05 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Basiskriterium

Interne sowie externe Mitarbeiter sind nachweislich darüber informiert, wie lange welche Verantwortlichkeiten, die sich aus den Richtlinien und Anweisungen mit Bezug zur Informationssicherheit ergeben, auch bei Beendigung oder Änderung der Beschäftigung bestehen bleiben.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Der Cloud-Anbieter stellt gemäß SP-01 sicher, dass die Richtlinien und Anweisungen die anwendbaren rechtlichen und regulatorischen Anforderungen reflektieren.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Im Rahmen einer vollumfänglichen systembasierten Dokumentation der HR-Daten, ist eine Bestätigung des Mitarbeiters denkbar, dass er zu den geforderten Themen informiert wurde. Diese sollte bei Beendigung des Beschäftigungsverhältnisses erneut eingeholt werden.

Läge eine solche Dokumentation in standardisierter und digitaler Form vor, wäre es dem Prüfer möglich, jeden Austritt auf diese Bestätigung hin zu prüfen und Abweichungen zu erkennen. Somit ist eine kontinuierliche Prüfung möglich.

HR-06 Vertraulichkeitsvereinbarungen

Basiskriterium

Die mit internen Mitarbeitern, externen Dienstleistern sowie Lieferanten des Cloud-Anbieters zu schließenden Geheimhaltungs- oder Vertraulichkeitsvereinbarungen basieren auf den vom Cloud-Anbieter identifizierten Anforderungen zum Schutz vertraulicher Informationen und betrieblicher Details.

Die Vereinbarungen sind mit externen Dienstleistern und Lieferanten bei Vertragsabschluss zu schließen. Mit internen Mitarbeitern des Cloud-Anbieters sind die Vereinbarungen zu schließen, bevor die Berechtigung zum Zugriff auf Daten der Cloud-Kunden erteilt wird.

Die Anforderungen sind zu dokumentieren sowie in regelmäßigen Abständen (mindestens jährlich) zu überprüfen. Soweit sich aus der Überprüfung ergibt, dass die Anforderungen anzupassen sind, werden die Geheimhaltungs- oder Vertraulichkeitsvereinbarungen aktualisiert.

Der Cloud-Anbieter hat die internen Mitarbeiter, externen Dienstleister und Lieferanten hierüber zu informieren und mit diesen die aktualisierten Geheimhaltungs- oder Vertraulichkeitsvereinbarungen zu schließen.

Zusatzkriterium

Soweit sich aus der Überprüfung Anpassungen an den Geheimhaltungs- oder Vertraulichkeitserklärungen ergeben, sind die internen und externen Mitarbeiter des Cloud-Anbieters darüber in Kenntnis zu setzen und neue Bestätigungen einzuholen.

Ergänzende Informationen

Zum Kriterium

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein:

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

Geheimhaltungs- oder Vertraulichkeitsvereinbarungen können, soweit dies rechtsverbindlich ist, mittels einer elektronischen Signatur unterschrieben werden.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Unterzeichnung von Vertraulichkeits-vereinbarungen mit internen Mitarbeitern, externen Dienstleistern und Lieferanten kann standardisiert erfolgen und digital gespeichert werden.

Eine automatisierte kontinuierliche Auswertung kann anschließend vorgenommen werden, in der geprüft wird, ob alle Parteien eine solche Vertraulichkeitsvereinbarung unterzeichnet haben und ob die Vereinbarung auf dem neuesten Stand ist.

6.4 Asset Management (AM)

Zielsetzung: *Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenes Schutzniveau über deren gesamten Lebenszyklus sicherstellen.*

AM-01 Inventarisierung der Assets

Basiskriterium

Der Cloud-Anbieter hat Verfahren für eine Inventarisierung der Assets eingerichtet.

Die Inventarisierung erfolgt automatisch und/oder durch für die Assets zuständige Personen oder Gruppen, um eine vollständige, richtige, gültige und konsistente Erfassung über den Lebenszyklus der Assets sicherzustellen.

Zu den Assets werden jene Informationen erfasst, die zur Anwendung des Verfahrens für den Umgang mit Risiken (vgl. OIS-07), einschließlich der Maßnahmen zur Behandlung dieser Risiken über den Lebenszyklus der Assets benötigt werden. Änderungen an diesen Informationen werden protokolliert.

Zusatzkriterium

Anwendungen zur Protokollierung und Überwachung berücksichtigen die zu den Assets erfassten Informationen, um bei Ereignissen, die zu einer Verletzung der Schutzziele führen können, die Auswirkungen auf Dienste und Funktionen des Cloud-Dienstes zu erkennen und eine Information der betroffenen Cloud-Kunden gemäß den vertraglichen Vereinbarungen zu unterstützen.

Ergänzende Informationen

Zum Kriterium

Assets im Sinne dieses Kriterienbereichs sind die für die Informationssicherheit des Cloud-Dienstes während der Erstellung, Verarbeitung, Speicherung, Übermittlung, Löschung oder Zerstörung von Informationen benötigten Objekte im Verantwortungsbereich des Cloud-Anbieters, z. B. Firewalls, Loadbalancer, Webserver, Anwendungsserver und Datenbankserver.

Diese Objekte bestehen wiederum aus Hardware- und Software-Objekten:

Hardware-Objekte sind:

- physische und virtuelle Infrastruktur-Ressourcen (z. B. Server, Speichersysteme, Netzkomponenten),
- sowie Endgeräte, soweit der Cloud-Anbieter in einer Risikobewertung festgestellt hat, dass diese bei Verlust oder unautorisierten Zugriffen die Informationssicherheit des Cloud-Dienstes gefährden könnten (z. B. Mobilgeräte, die als Security-Token zur Authentifizierung genutzt werden).

Software-Objekte sind z. B. Hypervisor, Container, Betriebssysteme, Datenbanken, Microservices und Programmierschnittstellen (APIs).

Der Lebenszyklus eines Assets umfasst:

- Anschaffung
- Inbetriebnahme
- Instandhaltung
- Außerbetriebnahme und
- Entsorgung.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Cloud-Anbieter muss eine automatische Erfassung der Assets (in einer Datenbank) sicherstellen. Dabei ist auch die automatische Erfassung physischer Assets sicherzustellen. Denkbar wäre aber auch eine automatische Erfassung dieser Assets bei Erstanmeldung in einem Netz. Die Erstellung virtueller Assets kann direkt mit der Eintragung in die Datenbank verbunden sein.

Werden alle Assets automatisch erfasst, können Veränderungen an der Datenbank dokumentiert werden (Logs) und diese Logs anschließend kontinuierlich ausgewertet werden. Hierbei ist

auf Vollständigkeit der im Inventar und in den Logs enthaltenen Informationen zu achten.

Der Prüfer kann bei vorhandenen automatisierten Prozessen eine Auswertung über die Veränderungen des Inventars mittels Logs erstellen.

Um auch die Überprüfung auf Vollständigkeit gewährleisten zu können, müsste im ersten Schritt eine Abfrage aller derzeitigen Assets beim Cloud-Anbieter geschehen. Diese Liste mit Assets könnte im Anschluss mit den Einträgen der Asset Management Datenbank abgeglichen werden.

AM-02 Richtlinie für den zulässigen Gebrauch und sicheren Umgang mit Assets

Basiskriterium

Richtlinien und Anweisungen für den zulässigen Gebrauch und den sicheren Umgang mit Assets sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und adressieren folgende Aspekte im Lebenszyklus von Assets, soweit diese für das Asset anwendbar sind:

- Genehmigungsverfahren für Anschaffung, Inbetriebnahme, Instandhaltung, Außerbetriebnahme und Entsorgung durch autorisiertes Personal oder System-komponenten,
- Inventarisierung,
- Klassifizierung und Kennzeichnung auf Basis des Schutzbedarfs der Informationen sowie Maßnahmen zur ermittelten Schutzstufe,
- sichere Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung,
- Anforderungen an Software- und Image-Versionen sowie Anwendung von Patches,
- Umgang mit Software für die kein Support und keine Sicherheitsaktualisierungen mehr verfügbar sind,
- Einschränkung von Software-Installationen oder Nutzung von Diensten,
- Schutz vor Schadsoftware,
- Remote-Deaktivierung, Löschung oder Sperrung,
- physische Übergabe und Transport;
- Umgang mit Störungen und Schwachstellen,
- vollständige und unwiderrufliche Löschung der Daten bei Außerbetriebnahme.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

AM-03 Inbetriebnahme von Hardware

Basiskriterium

Der Cloud-Anbieter hat einen Freigabeprozess für den Einsatz von inbetriebzunehmender Hardware, welche zur Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet wird, in welchem die aus der Inbetriebnahme entstehenden Risiken identifiziert, analysiert und mitigiert werden. Die Genehmigung erfolgt nach Verifikation der sicheren Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung gemäß der vorgesehenen Verwendung und auf Basis der anwendbaren Richtlinien.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Das Basiskriterium bezieht sich nur auf physische Hardware-Objekte, z. B. Server, Speichersysteme und Netzkomponenten.

Virtuelle Hardware- und Software-Objekte werden in den Kriterienbereichen (OPS) und (DEV) betrachtet.

Der Freigabeprozess berücksichtigt typischerweise sowohl die grundsätzliche Freigabe zur Nutzung der Hardware als auch die finale Freigabe der konfigurierten Assets.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Genehmigung der Inbetriebnahme von Hardware durch autorisiertes Personal muss digital dokumentiert werden, um eine kontinuierliche Prüfung zu ermöglichen. Hierzu ist beispielsweise ein Ticket System geeignet.

Im jeweiligen Ticket müssen sowohl das autorisierte Personal als auch die Verifikation der Konfiguration hinterlegt sein.

Damit ist es für den Prüfer möglich, die Tickets in einem automatisierten Verfahren zu überprüfen. Hierzu ist ein automatisierter Abgleich des autorisierten Personals gegen eine Datenbank, welche alle potenziellen Genehmiger beinhaltet, erforderlich. Zudem muss die Verifikation der Konfiguration im Ticket automatisiert geprüft werden.

Der konforme Gebrauch der Assets kann anschließend über ein Agentensystem sichergestellt werden, welches aktive Assets überprüft. Für eine kontinuierliche Prüfung kann dann der Status dieses Systems durch den Prüfer abgefragt werden.

AM-04 Außerbetriebnahme von Hardware

Basiskriterium

Die Außerbetriebnahme von Hardware, welche der Cloud-Anbieter in der Produktionsumgebung zum Betrieb von Systemkomponenten einsetzt, erfordert eine Genehmigung auf Basis der anwendbaren Richtlinien.

Die Außerbetriebnahme beinhaltet die vollständige und unwiderrufliche Löschung der Daten oder die ordnungsgemäße Vernichtung der Datenträger.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die Löschung von Daten bzw. physische Zerstörung von Datenträgern kann z. B. gemäß DIN 66399 oder BSI Grundschutz Baustein CON.6 erfolgen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Genehmigung der Außerbetriebnahme von Hardware durch autorisiertes Personal muss digital dokumentiert werden, um eine kontinuierliche Prüfung zu ermöglichen. Hierzu ist beispielsweise ein Ticket System geeignet.

Im jeweiligen Ticket müssen sowohl das autorisierte Personal als auch die Verifikation der vollständigen Löschung der Daten hinterlegt sein.

Damit ist es für den Prüfer möglich, die Tickets in einem automatisierten Verfahren zu überprüfen. Hierzu ist ein automatisierter Abgleich des autorisierten Personals gegen eine Datenbank, welche alle potenziellen Genehmiger beinhaltet, erforderlich. Zudem muss die im Ticket dokumentierte Löschung der Daten automatisiert geprüft werden.

Der konforme Gebrauch der Assets kann über ein Agentensystem sichergestellt werden, welches aktive Assets überprüft. Für eine kontinuierliche Prüfung kann dann der Status dieses Systems durch den Prüfer abgefragt werden.

AM-05 Verpflichtung auf zulässigen Gebrauch und sicheren Umgang mit ausgehändigten Assets sowie Rückgabe

Basiskriterium

Interne und externe Mitarbeiter des Cloud-Anbieters werden nachweislich auf die Richtlinien und Anweisungen für den zulässigen Gebrauch und den sicheren Umgang mit Assets verpflichtet, bevor diese verwendet werden dürfen, soweit der Cloud-Anbieter in einer Risikobewertung festgestellt hat, dass diese bei Verlust oder unautorisierten Zugriffen die Informationssicherheit des Cloud-Dienstes gefährden könnten.

Ausgehändigte Assets werden bei der Beendigung des Beschäftigungsverhältnisses nachweislich zurückgegeben.

Zusatzkriterium

Physische Assets der internen und externen Mitarbeiter unterliegen einer zentralen Verwaltung.

Die zentrale Verwaltung ermöglicht eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder -Sperrung.

Ergänzende Informationen

Zum Kriterium

Das Basiskriterium betrifft im Wesentlichen Mobilgeräte (z. B. Notebooks, Tablets, Smartphones etc.), insbesondere, wenn auf diesen Geräten vertrauliche Informationen gespeichert sind, die bei unautorisierten Zugriffen dazu genutzt werden können, privilegierten Zugriff auf den Cloud-Dienst zu erhalten (z. B. wenn diese als Security-Token zur Authentifizierung genutzt werden).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Verpflichtung der Mitarbeiter auf die Richtlinien und Anweisung kann in digitaler Form erfolgen. Damit kann ein Überwachungssystem erstellt werden, welches die nicht-Verpflichtung von Mitarbeitern auf Richtlinien protokolliert.

Der Prüfer kann in diesem Falle die Ausnahmen in Form von Protokollen prüfen und Nachweise dafür anfordern, welche zusätzlichen Schritte beim Cloud-Anbieter in diesen Fällen getätigt wurden, um ggf. vorhandene Risiken zu minimieren.

Der konforme Gebrauch der Assets kann anschließend über ein Agentensystem sichergestellt werden. Dieses System überprüft aktive Assets. Für eine kontinuierliche Prüfung kann dann der Status dieses Systems durch den Prüfer abgefragt werden.

AM-06 Klassifizierung und Kennzeichnung von Assets

Basiskriterium

Assets werden klassifiziert und, falls möglich, gekennzeichnet. Klassifizierung und Kennzeichnung eines Assets entsprechen dem Schutzbedarf der Informationen, die es verarbeitet, speichert oder übermittelt.

Der Schutzbedarf wird durch die für Assets zuständigen Personen oder Gruppen des Cloud-Anbieters nach einem einheitlichen Schema ermittelt. Das Schema sieht Schutzstufen für die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität vor.

Zusatzkriterium

Anwendungen zur Protokollierung und Überwachung berücksichtigen den Schutzbedarf der Assets, um bei Ereignissen, die zu einer Verletzung der Schutzziele führen können, das dafür zuständige Personal so zu informieren, dass erforderliche Maßnahmen mit einer geeigneten Priorität eingeleitet werden. Maßnahmen für Ereignisse bei Assets mit einem erhöhten Schutzbedarf haben Priorität vor Ereignissen bei Assets mit einem geringeren Schutzbedarf.

Ergänzende Informationen

Zum Kriterium

Sofern der Cloud-Anbieter keine differenzierte Klassifizierung der Assets vornimmt, sind alle Assets dem höchsten definierten Schutzbedarf zuzurechnen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden können durch geeignete Kontrollen sicherstellen, dass der Schutzbedarf der Informationen, die mit dem Cloud-Dienst verarbeitet oder gespeichert werden dürfen, angemessen ermittelt wird.

Cloud-Kunden können zudem durch geeignete Kontrollen sicherstellen, dass die mit dem Cloud-Dienst verarbeiteten oder gespeicherten Informationen gemäß ihrem Schutzbedarf vor Manipulieren, Kopieren, Modifizieren, Umleiten oder Löschen geschützt sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Klassifizierung der Assets und die Bestimmung des Schutzbedarfs sollte bei initialer Erfassung der Assets geschehen. Somit sollte die Klassifizierung auch in einem Asset Management Tool dokumentiert werden. Die Ermittlung des Schutzbedarfs kann zudem in standardisierter Form erfolgen und digital gespeichert werden. Gibt es Änderungen in der Klassifizierung so sollten diese auch durch Logs festgehalten sein.

Der Prüfer kann automatisch testen, ob alle Assets in der Plattform klassifiziert sind und ob die Klassifizierung anhand eines standardisierten Formats bestimmt wurde. Für Änderungen in der Klassifizierung kann automatisch nachvollzogen werden, ob diese auch anhand des einheitlichen Schemas erfolgt sind. Hierzu können die angefertigten Logs im Rahmen einer kontinuierlichen Prüfung ausgewertet werden.

6.5 Physische Sicherheit (PS)

Zielsetzung: *Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.*

PS-01 Sicherheitsanforderungen für Räumlichkeiten und Gebäude

Basiskriterium

Sicherheitsanforderungen für Räumlichkeiten und Gebäude mit Bezug zum bereitgestellten Cloud-Dienst sind aus den Sicherheitszielen der Informationssicherheitsleitlinie, dem identifizierten Schutzbedarf für den Cloud-Dienst und der Bewertung von Risiken zur physischen und umgebungsbezogenen Sicherheit abgeleitet. Die Sicherheitsanforderungen sind in einer Richtlinie oder einem Konzept gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt.

Die Sicherheitsanforderungen für Rechenzentren basieren auf Kriterien, die den anerkannten Regeln der Technik entsprechen. Sie sind geeignet die folgenden Gefährdungen gemäß den geltenden gesetzlichen und vertraglichen Anforderungen zu adressieren:

- Fehlerhafte Planung
- Unberechtigter Zutritt
- Unzureichende Überwachung
- Unzureichende Klimatisierung
- Feuer und Rauch
- Wasser
- Ausfall der Stromversorgung
- Verschmutzung.

Soweit der Cloud-Anbieter zur Bereitstellung des Cloud-Dienstes Räumlichkeiten oder Gebäude nutzt, die von Dritten betrieben werden, beschreibt das Dokument welche Sicherheitsanforderungen der Cloud-Anbieter an diese Dritten stellt. Die angemessene und wirksame Überprüfung der Umsetzung erfolgt gemäß den Kriterien zur Steuerung und Überwachung von Subdienstleistern (vgl. SSO-01, SSO-02).

Zusatzkriterium

Die Sicherheitsanforderungen umfassen Zeitvorgaben für den autarken Betrieb beim Eintritt außergewöhnlicher Ereignisse (z. B. länger anhaltender Stromausfall, Hitzeperioden, Niedrigwasser bei Kälteversorgung mit Flusswasser) sowie maximal tolerierbare Ausfallzeiten von Versorgungseinrichtungen.

Die Zeitvorgaben für einen autarken Betrieb sehen bei einem Ausfall der externen Stromversorgung mindestens 48 Stunden vor.

Für einen autarken Betrieb während einer Hitzeperiode sind die höchsten bislang im Radius von mindestens 50 km um die Standorte der Räumlichkeiten und Gebäude gemessenen, Außentemperaturen mit einem Sicherheitsaufschlag von 3 K ermittelt. Die Sicherheitsanforderungen sehen vor, dass die zulässigen Betriebs- und Umgebungsparameter der Kälteversorgung auch an mindestens 5 unmittelbar aufeinander folgenden Tagen mit diesen Außentemperaturen einschließlich Sicherheitsaufschlag eingehalten werden (vgl. PS-06 Schutz vor Ausfall der Versorgungseinrichtungen).

Soweit zur Klimatisierung Wasser aus einem Fluss entnommen wird, ist ermittelt, bei welchen Wasserständen und Wassertemperaturen die Klimatisierung wie lange aufrechterhalten werden kann.

Die maximal tolerierbaren Ausfallzeiten von Versorgungseinrichtungen sind geeignet, die in der Dienstgütevereinbarung enthaltenen Verfügbarkeitsanforderungen einzuhalten.

Ergänzende Informationen

Zum Kriterium

Räumlichkeiten und Gebäude mit Bezug zum bereitgestellten Cloud-Dienst umfassen Rechenzentren und Serverräume, die Systemkomponenten beherbergen, mit denen Daten der Cloud-Kunden verarbeitet werden sowie die für den Betrieb dieser Systemkomponenten benötigten technischen Versorgungseinrichtungen (z. B. Stromversorgung, Kälteversorgung,

Löschtechnik, Telekommunikation, Sicherheitstechnik etc.). Ausweich- oder Redundanzrechenzentren.

Räumlichkeiten und Gebäude, die von Dritten betrieben werden sind z. B. Serverhousing, Colocation oder IaaS.

Räumlichkeiten und Gebäude, in denen keine Daten von Cloud-Kunden im Cloud-Dienst verarbeitet oder gespeichert werden (z. B. Büroräume des Cloud-Anbieters, Serverräume mit Systemkomponenten für interne Entwicklungs- und Testsysteme) sind nicht Gegenstand dieses Kriterienbereichs.

Die anerkannten Regeln der Technik sind in einschlägigen Normen definiert, z. B. DIN EN 50600 (Einrichtungen und Infrastrukturen von Rechenzentren).

Eine fehlerhafte Planung kann die Betriebssicherheit und Verfügbarkeit der Räumlichkeiten oder Gebäude gefährden. Dies kann insbesondere aus einer falschen Bewertung elementarer Gefährdungen am Standort (z. B. Luftverkehr, Erdbeben, Hochwasser, Gefahrstoffe) sowie einer fehlerhaften Konzeptionierung der Bandbreite oder Energieversorgung resultieren.

Zeitvorgaben für den autarken Betrieb sowie maximal tolerierbare Ausfallzeiten von Versorgungseinrichtungen werden typischerweise im Rahmen der Business Impact Analyse erhoben (vgl. BCM-02, BCM-03).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die geforderte Dokumentation kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts der Dokumentation kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

PS-02 Redundanzmodell

Basiskriterium

Die Bereitstellung des Cloud-Dienstes erfolgt aus zwei Standorten, die sich einander Redundanz geben. Die Standorte entsprechen den Sicherheitsanforderungen des Cloud-Anbieters (vgl. PS-01 Sicherheitskonzept) und weisen einen hinreichenden Abstand zueinander auf, um eine Betriebsredundanz zu erreichen. Die Betriebsredundanz ist so ausgelegt, dass die in der Dienstgütevereinbarung enthaltenen Verfügbarkeitsanforderungen eingehalten werden.

Die Funktionsfähigkeit der Redundanz wird mindestens jährlich durch geeignete Tests und Übungen überprüft (vgl. BCM-04 - Verifizierung, Aktualisierung und Test der Betriebskontinuität).

Zusatzkriterium

Die Bereitstellung des Cloud-Dienstes erfolgt aus mehr als zwei Standorten, die sich einander Redundanz geben. Die Standorte sind räumlich ausreichend weit voneinander entfernt aufgebaut, um eine Georedundanz zu erreichen. Bei einem zeitgleichen Ausfall zweier Standorte steht mindestens ein dritter Standort weiterhin zur Verfügung, um einen Totalausfall zu verhindern.

Die Georedundanz ist so ausgelegt, dass die in der Dienstgütevereinbarung enthaltenen Verfügbarkeitsanforderungen eingehalten werden.

Die Funktionsfähigkeit der Redundanz wird mindestens jährlich durch geeignete Tests und Übungen überprüft (vgl. BCM-04 - Verifizierung, Aktualisierung und Test der Betriebskontinuität).

Ergänzende Informationen

Zum Kriterium

Eine Betriebsredundanz der Standorte zueinander im Sinne des Basiskriteriums ist gegeben, wenn auf Basis der Bewertung elementarer Gefährdungen am Standort entsprechende Abstände der Räumlichkeiten und Gebäude zu diesen Gefahren eingehalten werden. Sehr großräumige Ereignisse, die aufgrund ihres

Ausmaßes gleichzeitig oder zeitnah mehrere Standorte der gleichen Redundanzgruppe betreffen könnten (z. B. Hochwasser, Erdbeben), bleiben dabei unberücksichtigt.

Eine Georedundanz der Standorte zueinander im Sinne des optionalen, weitergehenden Kriteriums ist gegeben, wenn ein sehr großräumiges Ereignis an einem Standort keinesfalls gleichzeitig oder zeitnah mehrere Standorte der gleichen Redundanzgruppe trifft.

Die BSI-Publikation "Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren" gibt hierzu Hilfestellungen.

Es gibt Cloud-Anbieter, die das Thema Ausfallsicherheit des Cloud-Dienstes auf physischer Ebene nicht mehr durch Redundanz aus zwei unabhängigen Standorten, sondern durch Resilienz adressieren. Hierbei wird der Cloud-Service simultan aus mehr als zwei Standorten erbracht. Die zugrundeliegende verteilte Rechenzentrums-Architektur stellt sicher, dass der Ausfall eines Standortes oder von Komponenten eines Standortes nicht die definierten Verfügbarkeitskriterien des Cloud-Dienstes verletzt. Eine solche Architektur kann eine alternative Erfüllung (s. Kapitel 4.4.7) des Kriteriums darstellen. Die im Kriterium geforderten Tests und Übungen zur Funktionsfähigkeit gelten sinngemäß auch für resiliente Architekturen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass das vorliegende Redundanzmodell des Cloud-Anbieters und die Nachweise zur Überprüfung des Modells mit den eigenen Anforderungen zur Verfügbarkeit und Verlässlichkeit des Cloud-Dienstes konform sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine jährliche Überprüfung der Funktionsfähigkeit der Redundanz ist nur teilweise für eine kontinuierliche Prüfung geeignet. Eine kontinuierliche Prüfung könnte jeweils den Zeitpunkt der letzten Transaktion zur Herbeiführung der Redundanz zurückgeben. Zudem wäre es möglich, jede Transaktion die zur Redundanz beiträgt, durch Logs zu dokumentieren und diese automatisiert und kontinuierlich auszuwerten. Zudem könnte der Status der Redundanz kontinuierlich abgefragt werden.

PS-03 Perimeterschutz

Basiskriterium

Die bauliche Hülle von Räumlichkeiten und Gebäuden mit Bezug zum bereitgestellten Cloud-Dienst sind physisch solide und durch angemessene Sicherheitsmaßnahmen geschützt, die den Sicherheitsanforderungen des Cloud-Anbieters entsprechen (vgl. PS-01 Sicherheitskonzept).

Die Sicherheitsmaßnahmen sind geeignet, unberechtigte Zutritte rechtzeitig zu erkennen und zu verhindern, damit diese die Informationssicherheit des betrachteten Cloud-Dienstes nicht beeinträchtigen.

Die äußeren Türen, Fenster und sonstigen Bauelemente erreichen ein den Sicherheitsanforderungen angemessenes Niveau und halten einem Einbruchsversuch mindestens 10 Minuten stand. Die umgebenden Wandkonstruktionen sowie die Schließeinrichtungen erfüllen die damit einhergehenden Anforderungen.

Zusatzkriterium

Die am Standort eingerichteten Sicherheitsmaßnahmen umfassen permanent anwesendes Sicherheitspersonal (mindestens 2 Personen), Videoüberwachung und Einbruchmeldeanlagen.

Ergänzende Informationen

Zum Kriterium

Sicherheitsmaßnahmen zum Erkennen unbefugter Zutritte können Sicherheitspersonal, Videoüberwachung oder Einbruchmeldeanlagen sein.

Die Widerstandsklasse RC4 nach DIN EN 1627 sieht vor, dass Türen, Fenster und sonstige

Bauelemente einem Einbruchversuch mindestens 10 Minuten standhalten. Ein internationales Äquivalent zu dieser Norm ist der US-amerikanische Standard SD-STD-01.01 Rev.G.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche Prüfung der baulichen Hülle von Gebäuden ist nur teilweise möglich. Lediglich der Schutz gegen unberechtigte Zugriffe kann in Form von Zutritt-Logs auswertbare Daten liefern, die gespeichert werden.

PS-04 Physische Zutrittskontrolle

Basiskriterium

An Zugängen zu Räumlichkeiten und Gebäuden mit Bezug zum bereitgestellten Cloud-Dienst sind physische Zutrittskontrollen gemäß den Sicherheitsanforderungen des Cloud-Anbieters (vgl. PS-01 Sicherheitskonzept) eingerichtet, um unberechtigte Zutritte zu verhindern.

Die Zutrittskontrollen werden durch ein Zutrittskontrollsystem gesteuert.

Die Anforderungen an das Zutrittskontrollsystem sind gemäß SP-01 in einer Richtlinie oder einem Konzept dokumentiert, kommuniziert und bereitgestellt und umfassen die folgenden Aspekte:

- Geregeltes Verfahren für die Vergabe und den Entzug von Zutritts-Berechtigungen (vgl. IDM-02) auf Basis des Prinzips der geringsten Berechtigung („Least-Privilege-Prinzip") und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-Know-Prinzip"),
- Automatische Sperrung der Zutritts-Berechtigungen, wenn diese über einen Zeitraum von 2 Monaten nicht genutzt wurden
- Automatischer Entzug der Zutritts-Berechtigungen, wenn diese über einen Zeitraum von 6 Monaten nicht genutzt wurden,
- Zwei-Faktor-Authentisierung für den Zutritt zu Bereichen, die Systemkomponenten beherbergen, mit denen Informationen der Cloud-Kunden verarbeitet werden,
- Besucher und Fremdpersonal werden während aller Arbeiten in den Räumlichkeiten und Gebäuden von der Zutrittskontrolle individuell erfasst, als solche gekennzeichnet (z. B. durch sichtbares Tragen eines Besucherausweises) und während ihres Aufenthalts beaufsichtigt,
- Vorhandensein und Beschaffenheit einer Protokollierung der Zutritte, die es dem Cloud-Anbieter im Sinne einer Wirksamkeitsprüfung ermöglicht, zu überprüfen, ob nur definierte Personen die Räumlichkeiten und Gebäude mit Bezug zum bereitgestellten Cloud-Dienst betreten haben.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Zutrittskontrolle durch ein Access-Card-System kann durch den Cloud-Anbieter in Form von Logs dokumentiert werden. Diese Logs können automatisiert ausgewertet werden. Zudem können unbefugte Zutritte durch diese Logs nachvollzogen werden, was sich automatisiert auswerten lässt.

Daher ist eine kontinuierliche Prüfung möglich.

Sofern der Entzug von Zutritts-Berechtigungen standardisiert erfolgt und ebenso dokumentiert wird, ist auch hier eine automatisierte Auswertung möglich und somit eine kontinuierliche Prüfung durchführbar.

PS-05 Schutz vor Feuer und Rauch

Basiskriterium

Räumlichkeiten und Gebäuden mit Bezug zum bereitgestellten Cloud-Dienst sind durch

bauliche, technische und organisatorische Maßnahmen vor Feuer und Rauch geschützt, die den Sicherheitsanforderungen des Cloud-Anbieters (vgl. PS-01 Sicherheitskonzept) entsprechen und die folgenden Aspekte umfassen:

a) Bauliche Maßnahmen:

Einrichtung von Brandabschnitten mit einer Feuerwiderstandsdauer von mindestens 90 Minuten bei allen raumbildenden Teilen.

b) Technische Maßnahmen:

- Brandfrüherkennung mit automatischer Spannungsfreischaltung. Die Überwachungsbereiche sind hinreichend kleinteilig konzipiert, damit die Verhinderung einer Ausbreitung von Entstehungsbränden in einem angemessenen Verhältnis zur Aufrechterhaltung der Verfügbarkeit des bereitgestellten Cloud-Dienstes steht,
- Löschanlage oder Sauerstoffreduzierung,
- Brandmeldeanlage mit Meldung an die örtliche Feuerwehr.

c) Organisatorische Maßnahmen:

- Regelmäßige Brandschutzbegehungen, um die Einhaltung der Brandschutzvorgaben zu prüfen und
- Regelmäßige Brandschutzübungen.

Zusatzkriterium

Es findet eine Überwachung der Umgebungsparameter statt. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an das dafür sachverständige Personal weitergeleitet.

Ergänzende Informationen

Zum Kriterium

Die Überwachung der Umgebungsparameter ist in PS-01 adressiert. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an das dafür sachverständige Personal des Cloud-Anbieters weitergeleitet.

Raumbildende Teile sind Wände, Decken, Böden, Türen, Lüftungsklappen etc.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung ist möglich, sofern die eingebaute Technik zur Prüfung der Schutzmaßnahmen auswertbare Daten produziert und diese in standardisierter Form gespeichert werden. Dadurch könnte der Status der Sicherheitsmaßnahmen zumindest zu einem gewissen Grad standardisiert dokumentiert und durch den Prüfer kontinuierlich ausgewertet werden.

Ist diese Technik noch nicht ausreichend und eine Begehung des Rechenzentrums nötig, ist eine kontinuierliche Prüfung nur bedingt zielführend und die Möglichkeit zur kontinuierlichen Prüfung nur teilweise gegeben.

PS-06 Schutz vor Ausfall der Versorgungseinrichtungen

Basiskriterium

Maßnahmen zur Ausfallvorsorge der technischen Versorgungseinrichtungen, die für den Betrieb von Systemkomponenten benötigt werden, mit denen Informationen der Cloud-Kunden verarbeitet werden, sind gemäß den Sicherheitsanforderungen des Cloud-Anbieters (vgl. PS-01 Sicherheitskonzept) hinsichtlich der folgenden Aspekte dokumentiert und eingerichtet:

a) Betriebsredundanz (N+1) in der Strom- und Kälteversorgung

b) Einsatz angemessen dimensionierter unterbrechungsfreier Stromversorgungen (USV) und Netzersatzanlagen (NEA), die so ausgelegt sind, dass bei einem Stromausfall alle Datenbestände unbeschädigt bleiben. Die Funktionsfähigkeit von USV und NEA wird mindestens jährlich durch geeignete Tests und

Übungen überprüft (vgl. BCM-04 - Verifizierung, Aktualisierung und Test der Betriebskontinuität).

c) Instandhaltung (Wartung, Inspektion, Instandsetzung/Reparatur) der Versorgungseinrichtungen in Übereinstimmung mit den Herstellerempfehlungen

d) Schutz der Leitungen für Stromversorgung und Telekommunikation vor Unterbrechung, Störung, Beschädigung und Abhören. Der Schutz wird regelmäßig, mindestens aber alle zwei Jahre, sowie bei Manipulationsverdacht durch qualifiziertes Personal hinsichtlich der folgenden Aspekte überprüft:

- Spuren gewaltsamer Öffnungsversuche an geschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltung und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen,
- unzulässige Einbauten und Veränderungen.

Zusatzkriterium

Unterbrechungsfreie Stromversorgungen (USV) und Netzersatzanlagen (NEA) sind so ausgelegt, dass die in der Dienstgütevereinbarung enthaltenen Verfügbarkeitsanforderungen eingehalten werden.

Die Kälteversorgung ist so ausgelegt, dass die zulässigen Betriebs- und Umgebungsparameter auch an mindestens 5 unmittelbar aufeinander folgenden Tagen mit den höchsten bislang in einem Radius von mindestens 50 km um die Standorte der Räumlichkeiten und Gebäude gemessenen, Außentemperaturen mit einem Sicherheitsaufschlag von 3 K (bezogen auf die Außentemperatur) eingehalten werden. Die höchsten bislang gemessenen Außentemperaturen hat der Cloud-Anbieter zuvor ermittelt (vgl. PS-01 Sicherheitskonzept).

Die Anbindung an das Telekommunikationsnetz ist mit ausreichender Redundanz ausgelegt, so dass der Ausfall eines Telekommunikationsnetzes keine Beeinträchtigung der Sicherheit oder Leistungsfähigkeit des Cloud-Anbieters zur Folge hat.

Ergänzende Informationen

Zum Kriterium

Maßnahmen zur Ausfallvorsorge technischer Versorgungseinrichtungen sind z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Telekommunikation, Sicherheitstechnik etc.

Cloud-Anbieter können z. B. durch geordnetes Herunterfahren der Server sicherstellen, dass bei einem Stromausfall alle Datenbestände unbeschädigt bleiben.

Leitungen für Stromversorgung und Telekommunikation können z. B. mittels unterirdischer Zuführungen über unterschiedliche Zuleitungswege vor Unterbrechung, Störung, Beschädigung und Abhören geschützt werden.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die physische Sicherheit der Räumlichkeiten sowie die Ausfallsicherheit der versorgungstechnischen Einrichtungen sollte vor Ort durch eine Inspektion des Rechenzentrums geprüft werden.

Eine kontinuierliche Überprüfung ist daher nur bedingt sinnvoll. Sofern die genutzte Technologie zur Fehlervermeidung auswertbare Protokolldaten liefert, kann dieses Kriterium teilweise kontinuierlich überprüft werden. Dies ersetzt eine physische Prüfung jedoch nicht.

Andernfalls kann eine kontinuierliche Prüfung zumindest teilweise unter Angabe des letzten Prüfdatums durchgeführt werden.

PS-07 Überwachung der Betriebs- und Umgebungsparameter

Basiskriterium

Betriebsparameter der technischen Versorgungseinrichtungen (vgl. PS-06) sowie die Umgebungsparameter der Räumlichkeiten und Gebäuden mit Bezug zum bereitgestellten Cloud-Dienst werden gemäß den Sicherheitsanforderungen des Cloud-Anbieters (vgl. PS-01 Sicherheitskonzept) überwacht und geregelt. Bei Verlassen des zulässigen Regelbereichs wird das dafür sachverständige Personal oder die autorisierten Systemkomponenten des Cloud-Anbieters automatisch informiert, um umgehend die erforderlichen Maßnahmen zur Rückführung in den Regelbereich einzuleiten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Betriebsparameter und Umgebungsparameter der Räumlichkeiten und Gebäude sind z. B. Lufttemperatur und -feuchtigkeit, Leckage.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Überwachung und Regelung der Betriebsparameter der technischen Versorgungseinrichtungen wird automatisiert durchgeführt und standardisiert dokumentiert, beispielsweise in Logs.

Diese Logs sind dann durch den Prüfer automatisiert und kontinuierlich auswertbar.

6.6 Regelbetrieb (OPS)

Zielsetzung: *Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.*

OPS-01 Kapazitätsmanagement – Planung

Basiskriterium

Die Planung von Kapazitäten und Ressourcen (Personal und IT-Ressourcen) folgt einem etablierten Verfahren, um mögliche Kapazitätsengpässe zu vermeiden. Die Verfahren umfassen Prognosen von zukünftigen Kapazitätsanforderungen, um Nutzungstrends zu identifizieren und Risiken der Systemüberlastung zu beherrschen.

Cloud-Anbieter stellen durch geeignete Maßnahmen sicher, dass sie bei Kapazitätsengpässen oder Ausfällen hinsichtlich Personal und IT-Ressourcen die mit den Cloud-Kunden vereinbarten Anforderungen an die Bereitstellung des Cloud-Dienstes, gemäß der jeweiligen Vereinbarungen weiterhin erfüllen, insbesondere solche hinsichtlich dedizierter Nutzung von Systemkomponenten.

Zusatzkriterium

Die Prognosen werden in Abstimmung mit der Dienstgütevereinbarung zur Planung und Vorbereitung der Provisionierung berücksichtigt.

Ergänzende Informationen

Zum Kriterium

Aus Wirtschaftlichkeitsgründen streben Cloud-Anbieter typischerweise eine hohe Auslastung der IT-Ressourcen (CPU, Arbeitsspeicher, Speicherplatz, Netz) an. In Multi-Mandanten-Umgebungen müssen die vorhandenen Ressourcen zwischen den Cloud-Kunden (Mandanten) trotzdem so aufgeteilt werden, dass die Dienstgütevereinbarungen eingehalten werden. Insoweit sind die angemessene Planung und Überwachung von IT-Ressourcen kritisch für die Verfügbarkeit und Wettbewerbsfähigkeit des Cloud-Dienstes. Soweit die Verfahren nicht dokumentiert sind oder als Betriebsgeheimnis des Cloud-Anbieters einer höheren Vertraulichkeit unterliegen, muss der Cloud-Anbieter die Verfahren im Rahmen dieser Prüfung mindestens mündlich erläutern können.

Cloud-Kunden haben den Kapazitäts- und Ressourcenbedarf, der vom Cloud-Anbieter abgedeckt werden soll, zu planen und diesen im SLA mit dem Cloud-Anbieter widerzuspiegeln. Der Bedarf kann ebenso durch geeignete Kontrollen regelmäßig überprüft und das SLA ggf. entsprechend angepasst werden.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die Prüfung der Planung von Kapazitäten und Ressourcen erfordert eine Prüfung der Plausibilität und/oder Sinnhaftigkeit des Inhalts. Dies kann derzeit kaum automatisiert und kontinuierlich geprüft werden

OPS-02 Kapazitätsmanagement – Überwachung

Basiskriterium

Technische und organisatorische Maßnahmen zur Überwachung und Provisionierung bzw. De-Provisionierung von Cloud-Dienstleistungen sind definiert. Dadurch stellt der Cloud-Anbieter sicher, dass Ressourcen bereitgestellt bzw. Leistungen gemäß den vertraglichen Vereinbarungen erbracht werden und die Einhaltung der Dienstgütevereinbarungen sichergestellt ist.

Zusatzkriterium

Zur Überwachung der Kapazität und der Verfügbarkeit stehen dem Cloud-Kunden die relevanten Informationen in einem Self-Service-Portal zur Verfügung.

Ergänzende Informationen

Zum Kriterium

Technische und organisatorische Maßnahmen umfassen typischerweise:

- Einsatz von Monitoring Tools mit Alarmierungsfunktion beim Überschreiten definierter Schwellwerte,
- Prozess zum Korrelieren von Events und Schnittstelle zum Incident Management,
- eine durchgängige Überwachung der Systeme durch qualifiziertes Personal,
- Redundanzen in den IT-Systemen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die mit dem Cloud-Anbieter vertraglich getroffenen Vereinbarungen zum Bereitstellen von Ressourcen bzw. der zu erbringenden Leistungen überwacht werden können. Im Falle von Abweichungen stellen geeignete Kontrollen eine Information des Cloud-Anbieters sicher, sodass der Cloud-Anbieter geeignete Maßnahmen einleiten kann.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Teil der Überwachung von Ressourcen kann kontinuierlich durch die Prüfung von Kapazitätsvorhersagen und der Überwachung des Ressourcenmanagement-Tools geprüft werden. Weiterhin können die Logs der Provisionierungen und De-Provisionierungen sowie ihr Einfluss auf das Ressourcenmanagement kontinuierlich durch die Änderungen im Ressourcenmanagement geprüft werden.

OPS-03 Kapazitätsmanagement – Steuerung von Ressourcen

Basiskriterium

Entsprechend den Möglichkeiten des jeweiligen Servicemodells ist der Cloud-Kunde in der Lage die Aufteilung der ihm zur Verwaltung/Nutzung zugeordneten Systemressourcen zu steuern und zu überwachen, um eine Überbelegung der Ressourcen zu vermeiden und eine hinreichende Performance zu erreichen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Ressourcen entsprechend den Möglichkeiten des Servicemodells sind z. B.

- Rechenkapazität
- Speicherkapazität
- Konfiguration von Netzeigenschaften
- Application Programming Interfaces (APIs)
- Datenbanken.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Systemressourcen in ihrem Verantwortungsbereich steuern und überwachen.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Das Vorhandensein von Tools zur eigenen Steuerung der Ressourcen für die Cloud-Kunden stellt an sich bereits eine kontinuierliche Begebenheit dar, die sich kontinuierlich abfragen lässt, so der Cloud-Anbieter die Funktionalität dieser Tools mittels Protokollen etc. belegen kann. Dies kontinuierlich abzufragen, bringt für die Prüfung jedoch keinen großen Mehrnutzen.

Jedoch kann die Funktionalität der bereitgestellten Tools, insofern auswertbar durch den Cloud-Anbieter dokumentiert, kontinuierlich geprüft werden.

OPS-04 Schutz vor Schadprogrammen - Konzept

Basiskriterium

Richtlinien und Anweisungen mit Vorgaben zum Schutz vor Schadprogrammen sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt:

- Nutzung systemspezifischer Schutzmechanismen,
- Betrieb von Schutzprogrammen auf Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden,
- Betrieb von Schutzprogrammen für Endgeräte der Mitarbeiter.

Zusatzkriterium

Der Cloud-Anbieter erstellt regelmäßige Reports über die durchgeführten Überprüfungen, welche durch autorisiertes Personal oder Gremien überprüft und analysiert werden. Richtlinien und Anweisungen beschreiben die technischen Maßnahmen zur sicheren Konfiguration und Überwachung der Managementkonsole (sowohl des Self-Service vom Kunden als auch die Cloud-Administration des Dienstleisters), um diese vor Schadprogrammen zu schützen. Die Aktualisierung erfolgt mit der höchsten Frequenz, die der/die Hersteller vertraglich anbietet/anbieten.

Ergänzende Informationen

Zum Kriterium

Schutzprogramme für Endgeräten der Mitarbeiter können beispielsweise serverbasierte Schutzprogramme sein, bei denen Dateien in Anhängen auf dem Server geprüft werden oder der Netzverkehr gefiltert wird.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OPS-05 Schutz vor Schadprogrammen - Umsetzung

Basiskriterium

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, sind gemäß der in den Richtlinien und Anweisungen zum Schutz vor Schadprogrammen definierten Vorgaben geschützt.

Soweit Schutzprogramme mit einer signatur- und/oder verhaltensbasierten Erkennung und Entfernung von Schadprogrammen eingerichtet sind, werden diese Schutzprogramme mindestens täglich aktualisiert.

Zusatzkriterium

Die Konfiguration der Schutzmechanismen wird automatisch überwacht. Abweichungen von den Vorgaben werden automatisch an das dafür sachverständige Personal berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.

Ergänzende Informationen

Zum Kriterium

Der Schutz vor Schadprogrammen kann durch betriebssystem-spezifische Schutzmechanismen oder expliziten Schutzprogrammen (z. B. zur signatur- und verhaltensbasierte Erkennung und Entfernung von Schadprogrammen) umgesetzt werden.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, mit Sicherheitsprodukten zur Erkennung und Beseitigung von Schadprogrammen versehen sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Im ersten Schritt sollte die Sicherstellung der Vollständigkeit der Abdeckung aller Systeme

geprüft werden. Dies sollte durch die kontinuierliche Prüfung eines Tools und seiner Zu- und Abgänge überwacht werden.

Im zweiten Schritt sollten die Log-Files für die Updates der einzelnen Server sowie die regelmäßigen Scans kontinuierlich geprüft werden. Identifizierte Schadsoftware oder Unregelmäßigkeiten sollten im Rahmen der kontinuierlichen Überprüfung markiert und nachverfolgt werden.

OPS-06 Vorgaben zur Datensicherung und Wiederherstellung – Konzept

Basiskriterium

Richtlinien und Anweisungen mit Vorgaben zur Datensicherung- und Wiederherstellung sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt.

- Umfang und Häufigkeit der Datensicherung sowie die Dauer der Aufbewahrung entsprechen den vertraglichen Vereinbarungen mit den Cloud-Kunden sowie den Anforderungen an die betriebliche Kontinuität des Cloud-Anbieters hinsichtlich maximal tolerierbarer Ausfallzeit (Recovery Time Objective, RTO) und maximal zulässigem Datenverlust (Recovery Point Objective, RPO),
- Die Datensicherung erfolgt in verschlüsselter Form, die dem aktuellen Stand der Technik entspricht,
- Der Zugriff auf die gesicherten Daten und die Durchführung von Wiederherstellungen erfolgt nur durch autorisierte Personen,
- Tests von Wiederherstellungsverfahren (vgl. OPS-08).

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Im Datensicherungskonzept ist dargelegt, welche Art von Datensicherungen vorgenommen werden (z. B. Art und Weise, Datentyp, Dauer) und spezifiziert welche Daten auch in Sonderfällen (z. B. reine Verwendung von Computer Nodes ohne Datenhaltung) gesichert werden müssen. Bei der Datensicherung ist zwischen Backups und Snapshots virtueller Maschinen zu unterscheiden. Snapshots ersetzen kein Backup, können jedoch Teil der Backup-Strategie zum Erreichen des Recovery Point Objectives (RPO) sein, sofern sie zusätzlich außerhalb der ursprünglichen Datenlokation gespeichert werden.

Die geschäftlichen Anforderungen des Cloud-Anbieters für Umfang, Häufigkeit und Dauer der Datensicherung ergeben sich aus der Business Impact Analyse (vgl. BCM-03) für Entwicklungs- und Betriebsprozesse des Cloud-Dienstes. Soweit unterschiedliche Datensicherungs- und Wiederherstellungsverfahren für Daten unter Verantwortung des Cloud-Kunden und des Cloud-Anbieter bestehen, sind beide Varianten in eine Prüfung nach diesem Kriterienkatalog einzubeziehen. Für Verfahren zur Sicherung der Daten des Cloud-Anbieters ist nur die Angemessenheit und Implementierung der Kontrollen nachzuweisen, nicht aber deren Wirksamkeit. Für Verfahren zur Sicherung der Daten der Cloud-Kunden hat darüber hinaus auch eine Nachweisführung über die Wirksamkeit zu erfolgen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vertraglichen Vereinbarungen, welche mit dem Cloud-Anbieter bezüglich Umfang, Häufigkeit und Dauer der Aufbewahrung der Daten getroffen werden, den geschäftlichen Anforderungen entsprechen. Die geschäftlichen Anforderungen werden im Rahmen der Business Impact Analyse erhoben (vgl. BCM-02).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann

derzeit kaum automatisiert und kontinuierlich geprüft werden.

OPS-07 Datensicherung und Wiederherstellung – Überwachung

Basiskriterium

Der Cloud-Anbieter überwacht die Durchführung der Datensicherung mit technischen und organisatorischen Maßnahmen. Störungen werden durch qualifizierte Mitarbeiter des Cloud-Anbieters untersucht und zeitnah behoben, um die Einhaltung der vertraglichen Verpflichtungen gegenüber den Cloud-Kunden oder den geschäftlichen Anforderungen des Cloud-Anbieters bezüglich des Umfang und der Häufigkeit der Datensicherung sowie der Dauer der Aufbewahrung zu gewährleisten.

Zusatzkriterium

Zur Überwachung der Datensicherung stehen dem Cloud-Kunden die relevanten Protokolle oder die zusammengefassten Ergebnisse in einem Self-Service Portal zur Verfügung.

Ergänzende Informationen

Zum Kriterium

Sofern die Datensicherung nicht Bestandteil des zwischen Cloud-Anbieter und Cloud-Kunde geschlossenen Vertrages ist, ist dieses Kriterium nicht anwendbar. Dieser Sachverhalt ist vom Cloud-Anbieter in der Systembeschreibung transparent darzustellen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Datensicherung der in ihren Verantwortungsbereich fallenden Daten durch technische und organisatorische Maßnahmen überwacht wird.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Durchführung aller verschiedenen Datensicherungen kann durch die kontinuierliche Prüfung der Log-Dateien und der damit einhergehenden Ergebnisse der Datensicherung durchgeführt werden. Jegliche Fehler in der Datensicherung würden kontinuierlich aufgezeigt werden und könnten durch geeignete Maßnahmen und Dokumentation in der Prüfung erklärt werden.

OPS-08 Datensicherung und Wiederherstellung – Regelmäßige Tests

Basiskriterium

Wiederherstellungsverfahren werden vom Cloud-Anbieter regelmäßig, mindestens jährlich, getestet. Die Tests erlauben eine Beurteilung darüber, ob die vertraglichen Vereinbarungen sowie die Vorgaben zur maximal tolerierbarer Ausfallzeit (Recovery Time Objective, RTO) und zum maximal zulässigem Datenverlust (Recovery Point Objective, RPO) eingehalten werden (vgl. BCM-02).

Abweichungen von den Vorgaben werden an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten beim Cloud-Anbieter berichtet, damit diese die Abweichungen umgehend beurteilen und erforderliche Maßnahmen einleiten können.

Zusatzkriterium

Auf Kundenwunsch informiert der Cloud-Anbieter den Cloud-Kunden über die Ergebnisse der Wiederherstellungstests.
Wiederherstellungstests sind in das Notfallmanagement des Cloud-Anbieters eingebettet.

Ergänzende Informationen

Zum Kriterium

Sofern die Datensicherung nicht Bestandteil des zwischen Cloud-Anbieter und Cloud-Kunde geschlossenen Vertrages ist, ist dieses Kriterium nicht anwendbar. Dieser Sachverhalt ist vom Cloud-Anbieter in der Systembeschreibung transparent darzustellen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Werden die Tests über die Wiederherstellungsverfahren in regelmäßigen Abständen durchgeführt, kann der Zeitpunkt der Durchführung automatisiert geprüft werden. Allerdings ist der Aufwand einer kontinuierlichen Prüfung dieses Kriteriums hoch und der Mehrwert eher gering, wenn die Tests in einem jährlichen Zyklus durchgeführt werden. Eine kontinuierliche Prüfung kann mindestens das Datum des letzten Tests der Wiederherstellung ergeben.

OPS-09 Datensicherung und Wiederherstellung – Aufbewahrung

Basiskriterium

Der Cloud-Anbieter überträgt zu sichernde Daten an einen Remote-Standort oder transportiert diese auf Sicherungsdatenträgern an einen Remote-Standort. Soweit die Datensicherung über ein Netz zum Remote-Standort übertragen wird, erfolgt die Datensicherung oder die Übertragung der Daten in einer verschlüsselten Form, die dem Stand der Technik entspricht. Die Entfernung zum Hauptstandort ist nach hinreichender Abwägung der Faktoren Wiederherstellungszeiten und Auswirkung von Katastrophen auf beide Standorte gewählt. Die Maßnahmen zur physischen und umgebungsbezogenen Sicherheit am Remote-Standort entsprechen dem Niveau am Hauptstandort.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Sofern die Datensicherung nicht Bestandteil des zwischen Cloud-Anbieter und Cloud-Kunde geschlossenen Vertrages ist, ist dieses Kriterium nicht anwendbar. Dieser Sachverhalt ist vom Cloud-Anbieter in der Systembeschreibung transparent darzustellen.

Ein Remote-Standort kann z. B. ein weiteres Rechenzentrum des Cloud-Anbieters sein.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Sollte der Transport von Daten physisch erfolgen, könnte sich eine kontinuierliche Prüfung dieses Kriteriums auf die Bestätigung der erfolgreichen Einlagerung richten. Bei elektronischer Übertragung können die Logfiles der Übertragung kontinuierlich ausgewertet und das Ergebnis dieser Prüfung übermittelt werden.

OPS-10 Protokollierung und Überwachung – Konzept

Basiskriterium

Der Cloud-Anbieter hat Richtlinien und Anweisungen etabliert, welche das Protokollieren und Überwachen von Ereignissen auf Systemkomponenten in seinem Verantwortungsbereich regeln. Diese Richtlinien und Anweisungen sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und enthalten folgende Aspekte:

- Definition von Ereignissen, die zu einer Verletzung der Schutzziele führen können,
- Vorgaben zum Aktivieren, Stoppen und Pausieren der verschiedenen Protokollierungen,
- Informationen bezüglich des Zwecks sowie des Aufbewahrungszeitraums der Protokollierungen,
- Festlegung von Rollen und Verantwortlichkeiten für die Einrichtung und Überwachung der Protokollierung,
- Zeitsynchronisation von Systemkomponenten,
- Einhaltung rechtlicher und regulatorischer Rahmenbedingungen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Rechtliche und regulatorische Rahmenbedingungen sind z. B. gesetzliche Anforderungen an Aufbewahrung und Löschung von Daten.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass für jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, eine angemessene Protokollierung und Überwachung von Ereignissen erfolgt, welche die Sicherheit und Verfügbarkeit des Cloud-Dienstes beeinträchtigen können (z. B. Administratoraktivitäten, Systemfehler, Authentifizierungsprüfungen, Datenlöschungen etc.).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Richtlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OPS-11 Protokollierung und Überwachung – Konzept zum Umgang mit Metadaten

Basiskriterium

Richtlinien und Anweisungen mit Vorgaben zur sicheren Handhabung von Metadaten (Nutzungsdaten) sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt:

- Sammlung und Nutzung von Metadaten erfolgt ausschließlich für Abrechnungszwecke, zum Beheben von Störungen und Fehlern (Incident Management) sowie zum Bearbeiten von Sicherheitsvorfällen (Security Incident Management),
- Ausschließliche Nutzung anonymisierter Metadaten zur Bereitstellung und Verbesserung des Cloud-Dienstes, sodass kein Rückschluss auf den Cloud Kunden oder Nutzer möglich ist,
- keine kommerzielle Nutzung,
- Speicherung für einen festgelegten Zeitraum, der in einem angemessenen Zusammenhang mit den Zwecken der Erhebung steht,
- unverzügliche Löschung, wenn die Zwecke der Erhebung erfüllt sind und eine weitere Speicherung nicht mehr erforderlich ist,
- Bereitstellung an Cloud-Kunden gemäß den vertraglichen Vereinbarungen.

Zusatzkriterium

Personenbezogene Daten werden automatisiert und soweit technisch möglich aus den Protokolldaten entfernt, bevor der Cloud-Anbieter diese verarbeitet. Die Entfernung erfolgt in einer Form, die es dem Cloud-Anbieter weiterhin ermöglicht, die Protokolldaten für den Zweck zu nutzen, zu dem sie erhoben wurden.

Ergänzende Informationen

Zum Kriterium

Metadaten sind alle Daten, die beim Cloud-Anbieter durch die Nutzung seines Dienstes durch den Cloud-Kunden anfallen und keine Inhaltsdaten sind. Dazu gehören u. a. Anmelde/Abmelde-Zeiten, IP-Adressen, GPS-Position des Kunden, welche Ressourcen (Netz, Storage, Computer) genutzt wurden, auf welche Daten wann zugegriffen wurde, mit wem Daten geteilt wurden, mit wem kommuniziert wurde etc. Diese Daten werden zum Teil für Abrechnungszwecke und für das (Security) Incident Management verwendet. Sie sind darüber hinaus aber auch geeignet, Kundenverhalten und (je nach Cloud-Dienst) ein Großteil von Entscheidungs- und Arbeitsprozessen für den Cloud-Anbieter transparent zu machen. Mit dem Kriterium soll die Sammlung und Nutzung der Metadaten transparent und klar eingegrenzt werden.

Zudem beziehen sich Metadaten auf Daten die beim Zugriff des Cloud-Anbieters auf

Kundendaten (beispielsweise zur Indexierung) entstehen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OPS-12 Protokollierung und Überwachung – Zugriff, Speicherung und Löschung

Basiskriterium

Die Vorgaben zur Protokollierung und Überwachung von Ereignissen sowie zur sicheren Handhabung von Metadaten werden durch technisch gestützte Verfahren hinsichtlich der folgender Beschränkungen umgesetzt:

- Zugriff nur für auf autorisierte Benutzer und Systeme
- Speicherung für den festgelegten Zeitraum
- Löschung, wenn weitere Speicherung für den Zweck der Erhebung nicht mehr erforderlich ist.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine kontinuierliche Prüfung ist hier nur bedingt zielführend, da bei der Prüfung des Umgangs mit Metadaten in erster Linie die Prüfung der Richtlinien sowie zugehörigen Konfigurationen der Tools für die Sicherung, Verarbeitung und Löschung von Metadaten erfolgt. Hinzu kommen ggf. noch die vertraglichen Grundlagen für die Nutzung von Metadaten.

Eine kontinuierliche Prüfung könnte gegebenenfalls die Konfiguration zur Löschung oder Anonymisierung der Metadaten umfassen und automatisiert abfragen, ob die Konfiguration weiterhin besteht und korrekt implementiert ist. In diesem Fall wäre eine teilweise Möglichkeit zur kontinuierlichen Prüfung gegeben.

OPS-13 Protokollierung und Überwachung – Erkennung von Ereignissen

Basiskriterium

Die Protokollierungsdaten werden gemäß den Vorgaben zur Protokollierung und Überwachung automatisch auf Ereignisse überwacht, die zu einer Verletzung der Schutzziele führen können. Dies umfasst auch die Erkennung von Beziehungen zwischen Ereignissen (Ereigniskorrelation).

Identifizierte Ereignisse werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um die Ereignisse umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Cloud-Anbieter kann die Liste der überwachungskritischen Assets automatisiert testen und diese Überprüfung in Logs festhalten.

Die Log-Dateien können vom Prüfer anschließend automatisiert und kontinuierlich auf Unregelmäßigkeiten geprüft werden.

OPS-14 Protokollierung und Überwachung – Aufbewahrung der Protokollierungsdaten

Basiskriterium

Der Cloud-Anbieter bewahrt die erstellten Protokollierungsdaten unabhängig von der Quelle dieser Daten, geeignet und unveränderlich aggregiert auf, sodass eine zentrale, autorisierte Auswertung der Daten möglich ist. Protokollierungsdaten werden gelöscht, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind.

Zwischen Protokollierungsservern und den zu protokollierenden Assets erfolgt eine Authentisierung, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen. Die Übertragung erfolgt nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management).

Zusatzkriterium

Der Cloud-Anbieter bietet auf Anfrage des Cloud-Kunden eine kundenspezifische Protokollierung (in Bezug auf Umfang und Dauer der Aufbewahrung) an und stellt diese dem Kunden zur Verfügung. In Abhängigkeit des Schutzbedarfs des Cloud-Anbieters und der technischen Realisierbarkeit wird eine logische oder eine physikalische Trennung von Protokoll- und Nutzdaten vorgenommen.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Aufbewahrung von Protokollierungsdaten an zentraler Stelle kann durch Logs beim Speichern der Daten dokumentiert werden. Ebenso kann die Löschung dieser Daten automatisiert erfolgen und durch Logs dokumentiert werden.

Der Prüfer kann anschließend eine automatisierte und kontinuierliche Auswertung dieser Logs durchführen.

OPS-15 Protokollierung und Überwachung – Zurechenbarkeit

Basiskriterium

Die erstellten Protokollierungsdaten erlauben eine eindeutige Identifizierung von Benutzerzugriffen auf Tenant-Ebene, um (forensische) Analysen im Falle eines Sicherheitsvorfalls zu unterstützen.

Für die Durchführung der forensischen Analysen und Sicherungen von Infrastrukturkomponenten sowie deren Netzkommunikation stehen Schnittstellen zur Verfügung.

Zusatzkriterium

Der Cloud-Anbieter stellt auf Anfrage des Cloud-Kunden die ihn betreffenden Protokolle in angemessener Form und zeitnah zur Verfügung, damit dieser die ihn betreffenden Vorfälle selbst untersuchen kann.

Ergänzende Informationen

Zum Kriterium

Infrastrukturkomponenten im Sinne dieses Kriteriums sind z. B. Fabric-Controller, Netzkomponenten und Virtualisierungs-Server.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass eindeutige Benutzerkennungen vergeben werden, die im Falle eines Sicherheitsvorfalls eine entsprechende Analyse zulassen.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Damit die erstellten Protokollierungsdaten eine eindeutige Identifizierung erlauben, muss die Erstellung dieser Daten entsprechend konfiguriert werden. Diese Konfiguration muss nicht kontinuierlich überprüft werden, sondern nur bei Änderung.

Ebenso können die Schnittstellen initial geprüft und anschließend bei Änderungen erneut getestet werden.

OPS-16 Protokollierung und Überwachung – Konfiguration

Basiskriterium

Der Zugriff auf Systemkomponenten zur Protokollierung- und Überwachung im Verantwortungsbereich des Cloud-Anbieters ist auf autorisierte Benutzer beschränkt. Änderungen an der Konfiguration erfolgen gemäß den anwendbaren Richtlinien und Anweisungen (vgl. DEV-03).

Zusatzkriterium

Der Zugriff auf Systemkomponenten zur Protokollierung und Überwachung im Verantwortungsbereich des Cloud-Anbieters erfordert eine Zwei-Faktor-Authentifizierung.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die kontinuierliche Prüfung dieser Zugriffsbeschränkung kann mittels der Protokollierung aller Änderungen an Zugriffsrechten für die Systemkomponenten zur Protokollierung und Überwachung erfolgen. Änderungen können kontinuierlich je nach Sinnhaftigkeit und Zugriffsnotwendigkeit der Person automatisiert geprüft werden.

OPS-17 Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software

Basiskriterium

Der Cloud-Anbieter überwacht die Protokollierungs- und Überwachungssysteme in seinem Verantwortungsbereich. Ausfälle werden automatisch und umgehend an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, sodass diese die Ausfälle beurteilen und erforderliche Maßnahmen einleiten können.

Zusatzkriterium

Die Systemkomponenten zur Protokollierung- und Überwachung sind so aufgebaut, dass bei Ausfällen einzelner Komponenten die Funktionalität insgesamt nicht eingeschränkt ist.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Automatisch kommunizierte Ausfälle können durch Logs automatisiert dokumentiert werden.

Eine kontinuierliche und automatisierte Prüfung dieser Ausfälle kann durch den Prüfer durchgeführt werden, indem diese Logs ausgewertet werden.

OPS-18 Umgang mit Schwachstellen, Störungen und Fehlern – Konzept

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SP-01 dokumentiert, kommuniziert und

bereitgestellt, um das zeitnahe Identifizieren und Adressieren von Schwachstellen der Systemkomponenten, die für die Bereitstellung des Cloud-Dienstes verwendet werden, zu gewährleisten. Diese Richtlinien und Anweisungen enthalten Vorgaben zu folgenden Aspekten:

- Regelmäßiges Identifizieren von Schwachstellen (Vulnerabilities),
- Beurteilen des Schweregrads identifizierter Schwachstellen,
- Priorisieren und Umsetzen von Maßnahmen zur zeitnahen Behebung oder Mitigation identifizierter Schwachstellen auf Basis des Schweregrades gemäß definierter Zeitvorgaben,
- Umgang mit Systemkomponenten, für die basierend auf einer Risikobewertung keine Maßnahmen zur zeitnahen Behebung oder Mitigation der Schwachstellen eingeleitet werden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Identifizierte Schwachstellen können nach etablierten Metriken wie etwa CVSS oder OWASP eingeordnet werden. Die Entscheidung, identifizierte Schwachstellen nicht zu beheben oder zu mitigieren, muss der Cloud-Anbieter ausgehend von einer Risikobewertung treffen. Gegebenenfalls sind risikokompensierende Maßnahmen zu ergreifen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Systemkomponenten in ihrem Verantwortungsbereich regelmäßig auf Schwachstellen überprüfen und diese durch geeignete Maßnahmen adressieren.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

OPS-19 Umgang mit Schwachstellen, Störungen und Fehlern – Penetrationstests

Basiskriterium

Der Cloud-Anbieter lässt mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführen. Die Penetrationstests erfolgen nach einer dokumentierten Testmethodik und umfassen die für die Erbringung des Cloud-Dienstes relevanten Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters„ die im Rahmen einer Risiko-Analyse als solche identifiziert wurden.

Der Cloud-Anbieter hat den Schweregrad der in Penetrationstests getroffenen Feststellungen nach definierten Kriterien zu beurteilen.

Für Feststellungen mit mittlerer oder hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit des Cloud-Dienstes sind innerhalb definierter Zeitfenster Maßnahmen zur zeitnahen Behebung oder Mitigation durchzuführen.

Zusatzkriterium

Die Tests finden halbjährlich statt. Diese müssen zwingend durch unabhängige Externe durchgeführt werden. Internes Personal für Penetrationstests darf die externen Dienstleister dabei unterstützen.

Ergänzende Informationen

Zum Kriterium

Die Schwachstellen sollten gemäß Schadenpotenzial klassifiziert sein und ein Zeitraum sollte für die erforderliche Reaktion genannt werden. Als Orientierung kann die

folgende Einstufung gemäß der BSI-Publikation „Ein Praxis-Leitfaden für IS-Penetrationstests" dienen:

- Hoch: Sofortige Reaktion
- Mittel: Kurzfristige Reaktion
- Niedrig: Mittelfristige Reaktion
- Information: Langfristige Reaktion.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Da Penetrationstests jährlich durchgeführt werden, ist eine kontinuierliche Prüfung hier nicht zielführend, da der Aufwand der Automatisierung der Prüfung größer wäre als der erwartete Nutzen.

Es könnte lediglich der Zeitpunkt des letzten Tests in einer kontinuierlichen Prüfung zurückgegeben werden.

OPS-20 Umgang mit Schwachstellen, Störungen und Fehlern – Messungen, Analysen und Bewertungen der Verfahren

Basiskriterium

Der Cloud-Anbieter führt regelmäßige Messungen, Analysen und Bewertungen der Verfahren zum Umgang mit Schwachstellen (Vulnerabilities) und Störungen (Incidents) durch, um deren fortdauernde Eignung, Angemessenheit und Wirksamkeit zu überprüfen. Ergebnisse werden mindestens quartalsweise durch verantwortliches Personal des Cloud-Anbieters bewertet, um Maßnahmen zur fortlaufenden Verbesserung zu initiieren oder deren Wirksamkeit zu überprüfen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Eine geeignete Weise zur Dokumentation von Schwachstellen und Störungen ist beispielsweise das Common Vulnerabilities and Exposures (CVE) oder damit vergleichbare Weisen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Messungen, Analysen und Bewertungen basieren auf Daten, die kontinuierlich abgefragt werden könnten, um die daraus abgeleiteten Ergebnisse zu plausibilisieren.

Die Initiierung und Überprüfung von Maßnahmen zur fortlaufenden Verbesserung bedarf einer manuellen Prüfung.

OPS-21 Einbindung des Cloud-Kunden bei Störungen (Incidents)

Basiskriterium

Der Cloud-Anbieter informiert den Cloud-Kunden regelmäßig und in angemessener Form, die den vertraglichen Vereinbarungen entspricht, über den Status der den Cloud-Kunden betreffenden Störungen (Incidents) und bindet diesen, soweit angemessen und erforderlich, in deren Behebung ein. Sobald eine Störung aus Sicht des Cloud-Anbieters behoben wurde, wird der Cloud-Kunde gemäß den vertraglichen Vereinbarungen über die getroffenen Maßnahmen informiert.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen

des Cloud-Anbieters bezüglich sie betreffender Störungen erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle des Cloud-Anbieters weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung ist möglich, wenn Kunden über einen standardisierten Kommunikationsweg über Vorfälle (Incidents) informiert werden und dies dokumentiert (E-Mails, Logs) wird.

Der Prüfer kann dann die angefertigte Dokumentation automatisiert und kontinuierlich auswerten.

Es erscheint zielführend, die Auswertung der Kommunikation der Vorfälle an Kunden mit der Auswertung der Behebung der Vorfälle zu verbinden. Sobald die Vorfälle im besten Falle automatisiert behoben wurden, wird eine automatische Meldung an den Kunden generiert und versendet, welche dokumentiert wird.

Damit ist es dem Prüfer möglich, auszuwerten, ob der Kunde regelmäßig und zu allen ihn betreffenden Incidents, aber auch nicht darüber hinaus, sachgerecht informiert wurde.

OPS-22 Prüfung und Dokumentation offener Schwachstellen

Basiskriterium

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters für die Erbringung des Cloud-Dienstes werden gemäß den Vorgaben zum Umgang mit Schwachstellen (vgl. OPS-18), mindestens monatlich, automatisiert auf bekannte Schwachstellen (Vulnerabilities) geprüft, der Schweregrad nach definierten Kriterien beurteilt und Maßnahmen zur zeitnahen Behebung oder Mitigation innerhalb definierter Zeitfenster eingeleitet.

Zusatzkriterium

Sicherheitspatches werden ab dem Zeitpunkt ihrer Verfügbarkeit in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen eingespielt:

- Kritisch (CVSS = 9.0 - 10.0): 3 Stunden
- Hoch (CVSS = 7.0 - 8.9): 3 Tage
- Mittel (CVSS = 4.0 - 6.9): 1 Monat
- Niedrig (CVSS = 0.1 - 3.9): 3 Monate

Ergänzende Informationen

Zum Kriterium

Im Gegensatz zu Penetrationstests (vgl. OPS-20), die manuell und nach einem individuellen Schema ablaufen, erfolgt die Prüfung auf offene Schwachstellen automatisiert, unter Verwendung sog. Vulnerability Scanner.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher jene Systemkomponenten, die unter ihrer Verantwortung stehen, regelmäßig auf Schwachstellen zu überprüfen und diese durch geeignete Maßnahmen zu adressieren.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die periodische Prüfung auf Schwachstellen und die daraus resultierenden Ergebnisse, sowie die Analyse und Behebung von identifizierten Schwachstellen werden vom Cloud-Anbieter dokumentiert.

Eine automatisierte und kontinuierliche Prüfung dieser Vorgehensweise kann durch den Prüfer umgesetzt werden, indem die dokumentierten Ergebnisse automatisch ausgewertet werden.

OPS-23 Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung

Basiskriterium

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, sind gemäß allgemein akzeptierter Branchenstandards gehärtet. Die je

Systemkomponente anzuwendenden Vorgaben zur Härtung sind dokumentiert.

Soweit nicht veränderliche ("immutable") Images eingesetzt werden, wird die Einhaltung der Vorgaben zur Härtung bei der Erstellung der Images in einem konsistenten Verfahren überprüft. Konfigurations- und Log-Dateien bezüglich der kontinuierlichen Bereitstellung dieser Images werden aufbewahrt.

Zusatzkriterium

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters werden automatisch auf Einhaltung der Vorgaben zur Härtung überwacht. Abweichungen von den Vorgaben werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um sodass diese die Abweichungen umgehend einer Beurteilung unterziehen und erforderliche Maßnahmen einleiten können.

Ergänzende Informationen

Zum Kriterium

Systemkomponenten im Sinne des Basiskriteriums sind die für die Informationssicherheit des Cloud-Dienstes während der Erstellung, Verarbeitung, Speicherung, Übertragung, Löschung oder Zerstörung von Informationen benötigten Objekte im Verantwortungsbereich des Cloud-Anbieters, z. B. Firewalls, Loadbalancer, Webserver, Anwendungsserver und Datenbankserver. Diese Systemkomponenten bestehen wiederum aus Hardware- und Software-Objekten. Dieses Kriterium beschränkt sich auf Software-Objekte, z. B. Hypervisor, Betriebssysteme, Datenbanken, Programmierschnittstellen (APIs), Images (z. B. für virtuelle Maschinen und Container) sowie Anwendungen zur Protokollierung und Überwachung sicherheitsrelevanter Ereignisse.

Die Konfigurations- und Log-Dateien bezüglich nicht veränderlicher Images beinhalten beispielsweise:

- Konfiguration der eingesetzten Images bezüglich umgesetzter Vorgaben zur Härtung inklusive Versionshistorie,
- Log-Dateien bezüglich der Datei-Integritätsüberwachung der im produktiven Einsatz befindlichen Images.

Allgemein akzeptierte Branchenstandards sind z. B. der Security Configuration Benchmark des Center for Internet Security (CIS) oder die entsprechenden Bausteine im BSI IT-Grundschutz-Kompendium.

Die Einhaltung der Vorgaben zur Härtung kann z. B. durch eine Datei-Integritätsüberwachung überwacht werden.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, gemäß allgemein etablierter und akzeptierter Industriestandards zu härten. Die angewendeten Härtungsmaßnahmen resultieren aus einer Risikobeurteilung der geplanten Nutzung des Cloud-Dienstes.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Überprüfung zur Einhaltung der Vorgaben zur Härtung der Systemkomponenten kann automatisiert getestet und anschließend dokumentiert (Logs) werden.

Der Prüfer kann diese Logs automatisch und kontinuierlich auswerten und somit eine kontinuierliche Prüfung ausführen.

OPS-24 Separierung der Datenbestände in der Cloud-Infrastruktur

Basiskriterium

Auf gemeinsam genutzten virtuellen und physischen Ressourcen gespeicherte und verarbeitete Daten der Cloud-Kunden sind gemäß eines dokumentierten Konzepts auf Basis einer Risikoanalyse gemäß OIS-07 sicher und strikt separiert, um die Vertraulichkeit und Integrität dieser Daten zu gewährleisten.

Zusatzkriterium

Ressourcen im Speichernetz (Storage) sind durch sichere Zonierung (LUN Binding und LUN Masking) segmentiert.

Ergänzende Informationen

Zum Kriterium

Als gemeinsam genutzte Ressourcen sind u. a. Arbeitsspeicher, Rechenkerne und Speichernetze zu verstehen. Eine technische Segregation (Trennung) der gespeicherten und verarbeiteten Daten der Cloud-Kunden in gemeinsam genutzten Ressourcen kann durch Firewalls, Zugriffslisten, Tagging (Auszeichnung des Datenbestandes), VLANs, Virtualisierung und Maßnahmen im Speichernetz (z. B. LUN Binding und LUN Masking) oder starke Verschlüsselung (vgl. CRY-01) erreicht werden. Soweit Angemessenheit und Wirksamkeit der Segregation nicht mit hinreichender Sicherheit beurteilt werden können (z. B. aufgrund einer komplexen Implementierung), kann der Nachweis auch über Prüfungsergebnisse sachverständiger Dritter erfolgen (z. B. Sicherheitsaudit zur Validierung des Konzepts). Die Segregation übertragener Daten ist Gegenstand des Kriteriums COS-06.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vom Cloud-Dienst bereitgestellten Funktionen zur Segregation gemeinsam genutzter virtueller und physischer Ressourcen so genutzt werden, dass Risiken mit Bezug zur Segregation entsprechend dem Schutzbedarf der Daten hinreichend adressiert sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Segregierung gemäß eines dokumentierten Konzepts erfolgt mittels einer Konfiguration, welche nicht mit hoher Frequenz verändert wird. Eine kontinuierliche Prüfung dieser Konfiguration könnte gegebenenfalls auswerten, ob die Konfiguration und somit die Trennung der Daten korrekt implementiert ist. Allerdings wäre der Aufwand zur kontinuierlichen Prüfung hoch und der Nutzen aufgrund der geringen Änderungsrate der Konfiguration gering. Somit wäre eine kontinuierliche Prüfung hier nur bedingt zielführend. Falls die Einhaltung der getroffenen Maßnahmen überwacht wird, kann eine automatisierte Prüfung dieses Kriteriums erfolgen.

Denkbar wäre auch, die tatsächliche Separierung der Daten kontinuierlich zu prüfen. Hierzu müssten beim Cloud-Provider entsprechende Agenten eingesetzt werden, die den Datenstrom zwischen den Kunden-Instanzen (oder dessen Fehlen) dauerhaft und dokumentiert (Logs) überwachen.

6.7 Identitäts- und Berechtigungsmanagement (IDM)

Zielsetzung: *Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (in der Regel privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.*

IDM-01- Richtlinie für Zugangs- und Zugriffsberechtigungen

Basiskriterium

Ein auf den Geschäfts- und Sicherheitsanforderungen des Cloud-Anbieters basierendes Rollen- und Rechtekonzept sowie eine Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter des Cloud-Anbieters sowie für Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, sind gemäß SP-01 mit folgenden Vorgaben dokumentiert, kommuniziert und bereitgestellt:

- Vergabe eindeutiger Benutzernamen,
- Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen auf Basis des Prinzips der geringsten Berechtigung („Least-Privilege-Prinzip") und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-Know-Prinzip"),
- Funktionstrennung zwischen operativen und kontrollierenden Funktionen („Segregation of Duties"),
- Funktionstrennung in der Verwaltung von Rechteprofilen, Genehmigung und Zuweisung von Zugangs- und Zugriffsberechtigungen,
- Genehmigung der Vergabe oder Änderung durch autorisiertes Personal oder autorisierte Systemkomponenten bevor auf Daten der Cloud-Kunden oder Systemkomponenten zur Bereitstellung des Cloud-Dienstes zugegriffen werden kann,
- regelmäßige Überprüfung vergebener Zugangs- und Zugriffsberechtigungen,
- Sperrung und Entzug von Zugangsberechtigungen bei Inaktivität,
- Zeitbasierter oder anlassbezogener Entzug bzw. Anpassung von Zugriffsberechtigungen bei Veränderungen des Aufgabengebiets,
- Zwei- oder Mehr-Faktor-Authentisierung für Benutzer mit privilegierten Zugriffsberechtigungen,
- Anforderungen an Genehmigung und Dokumentation der Verwaltung von Zugangs- und Zugriffsberechtigungen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Systemkomponenten im Sinne des Basiskriteriums siehe Definition bei OPS-23. Automatisierte Autorisierungsprozesse im Sinne dieses Basiskriterium betreffen Verfahren zur automatisierten Softwareauslieferung (Continuous Delivery) sowie zum automatisierten Provisionieren und Deprovisionieren von Zugangs- und Zugriffsberechtigungen auf Basis genehmigter Anträge.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden. Die Aspekte, welche in der Richtlinie genannt werden, können in einzelne Kriterien überführt und in eine kontinuierlichen Prüfung eingebettet werden. Einzelaspekte der Richtlinie, die kontinuierlich geprüft werden können:

- eindeutiger Benutzername
- Funktionstrennung
- Rechteprofilverwaltung (Genehmigungen)
- Autorisiertes Personal oder autorisierte Systemkomponenten
- Regelmäßige Überprüfung
- Inaktivitätssperrung
- Mehrfaktor-Authentisierung.

Genehmigung und Dokumentation Einzelaspekte der Richtlinie, die nicht praktikabel kontinuierlich geprüft werden können:

- Umsetzung von Least-Privilege/Need-to-Know-Prinzipien,
- Entzug oder Anpassung von Zugriffsberechtigungen bei Veränderungen des Aufgabengebiets

IDM-02 Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen

Basiskriterium

Geregelte Verfahren für die Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter des Cloud-Anbieters sowie für Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, stellen die Einhaltung des Rollen- und Rechtekonzepts sowie der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen sicher.

Zusatzkriterium

Der Cloud-Anbieter bietet Cloud-Kunden einen Self-Service an, mit welchem diese Zugangs- und Zugriffsberechtigungeneigenständig vergeben und ändern können.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine kontinuierliche Prüfung von Verfahren ist stark abhängig von der dahinterliegenden Systematik und Automatisierung der Verfahren beim Cloud-Anbieter. Im Einzelfall kann dies abweichen, pauschal erscheint die kontinuierliche Prüfung hier nicht zielführend.

IDM-03 Sperrung und Entzug von Zugangsberechtigungen bei Inaktivität oder mehrfach fehlgeschlagenen Anmeldungen

Basiskriterium

Zugangsberechtigungen interner und externer Mitarbeiter des Cloud-Anbieters sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, werden gesperrt, wenn diese über einen Zeitraum von zwei Monaten nicht genutzt wurden. Das Entsperren erfordert die Genehmigung durch eine hierzu autorisierte Instanz.

Nach spätestens sechs Monaten werden die gesperrten Zugangsberechtigungen entzogen. Nach Entzug ist das Verfahren für die Vergabe (vgl. IDM-02) erneut zu durchlaufen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Eine Sperrung kann aus einer längeren Abwesenheit des Mitarbeiters resultieren, z. B. durch Krankheit, Elternzeit oder Sabbatical.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Automatisierte Prozesse können einfach in die kontinuierliche Prüfung aufgenommen werden. Hierbei sind beim Cloud-Anbieter angemessene Auswertungs- und Reporting-Mechanismen einzusetzen. Der Prüfer muss hierbei Daten-Analysen anwenden, um Abweichungen festzustellen.

IDM-04 Entzug oder Anpassung von Zugriffsberechtigungen bei Veränderungen des Aufgabengebiets

Basiskriterium

Zugriffsberechtigungen werden bei Änderungen im Aufgabengebiet der internen und externen Mitarbeiter des Cloud-Anbieters oder der Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, zeitnah entzogen. Privilegierte Zugriffsberechtigungen werden spätestens 48 Stunden nach Inkrafttreten der Änderung angepasst oder entzogen. Alle anderen Zugriffsberechtigungen werden spätestens nach 14 Tagen angepasst oder entzogen. Nach Entzug ist das Verfahren für die Vergabe (vgl. IDM-02) erneut zu durchlaufen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Auslöser von Änderungen des Aufgabengebiets interner und externen Mitarbeiter können Änderungen im Beschäftigungsverhältnis (z. B. Kündigung, Versetzung) oder in Verträgen und Vereinbarungen sein. Für privilegierte Zugriffsberechtigungen im Sinne des Basiskriteriums gilt die Definition bei IDM-06.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Es gilt, die Änderungen des Aufgabengebietes inhaltlich und zusammen mit dem Zeitpunkt des Inkrafttretens zu erfassen, um diese mit den durchgeführten Anpassungen an den Zugriffsberechtigungen abzugleichen. Eine kontinuierliche Prüfung erscheint möglich, erfordert aber hohen Implementierungsaufwand.

IDM-05 Regelmäßige Überprüfung der Zugriffsberechtigungen

Basiskriterium

Zugriffsberechtigungen interner und externer Mitarbeiter des Cloud-Anbieters sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, werden mindestens jährlich daraufhin überprüft, ob diese noch dem tatsächlichen Aufgaben- bzw. Einsatzgebiet entsprechen. Die Überprüfung erfolgt durch hierzu autorisierte Personen aus den Organisationseinheiten des Cloud-Anbieters, die aufgrund ihres Wissens über die Aufgabengebiete der Mitarbeiter oder Systemkomponenten die Angemessenheit der vergebenen Zugriffsberechtigungen beurteilen können. Identifizierte Abweichungen werden zeitnah, spätestens aber 7 Tage nach ihrer Feststellung durch geeignetes Ändern oder Entziehen der Zugriffsberechtigungen behandelt.

Zusatzkriterium

Privilegierte Berechtigungen werden mindestens halbjährlich überprüft.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die eigentliche Überprüfung kann nicht automatisiert erfasst werden. Es könnte eine Erfassung von dabei entstehenden,

dokumentarisch genutzten Unterlagen stattfinden (z. B. Bestätigung, dass die Rechtevergabe überprüft wurde). Eine kontinuierliche Prüfung könnte somit angeben, wann diese Überprüfung das letzte Mal durchgeführt wurde. Der Cloud-Anbieter muss hierfür den Überprüfungsprozess automatisieren (insb. die Bestätigung der Durchführung der Überprüfung), sodass der Prüfer die durchzuführenden Schritte auf Abweichungen überprüfen kann.

IDM-06 Privilegierte Zugriffsberechtigungen

Basiskriterium

Vergabe und Änderung von privilegierten Zugriffsberechtigungen für interne und externe Mitarbeiter sowie technische Benutzer des Cloud-Anbieters erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen (vgl. IDM-01) oder einer separaten Richtlinie. Privilegierte Zugriffsberechtigungen werden personalisiert sowie gemäß einer Risikobewertung zeitlich befristet und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-Know-Prinzip") zugewiesen. Technische Benutzer werden zudem internen oder externen Mitarbeitern des Cloud-Anbieters zugewiesen. Die Aktivitäten von Benutzern mit privilegierten Zugriffsberechtigungen werden protokolliert, um einen Missbrauch dieser Berechtigungen im Verdachtsfall aufdecken zu können. Die protokollierten Informationen werden automatisch auf definierte Ereignisse überwacht, die einen Missbrauch darstellen können. Bei Identifikation eines solchen Ereignisses wird das dafür zuständige Personal des Cloud-Anbieters automatisch informiert, um unverzüglich beurteilen zu können, ob ein Missbrauch vorliegt und entsprechende Maßnahmen einzuleiten sind. Bei nachweislich missbräuchlicher Nutzung privilegierter Zugriffsberechtigungen werden Disziplinarmaßnahmen gemäß HR-04 eingeleitet.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Privilegierte Zugriffsberechtigungen im Sinne des Basiskriteriums sind solche, die Mitarbeitern des Cloud-Anbieters eine der folgenden Aktivitäten ermöglichen:

- lesenden oder schreibenden Zugriff auf die im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten der Cloud-Kunden, soweit diese nicht verschlüsselt sind oder die Verschlüsselung für den Zugriff durch den Cloud-Anbieter aufgehoben werden kann,
- Änderungen an der betrieblichen und/oder sicherheitstechnischen Konfiguration der Systemkomponenten in der Produktionsumgebung, insbesondere das Starten, Stoppen, Löschen oder Deaktivieren von Systemkomponenten, wenn dies die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten der Cloud-Kunden beeinträchtigen kann (auch mittelbar, z. B. durch Deaktivieren der Protokollierung und Überwachung sicherheitsrelevanter Ereignisse).

Missbräuchlich genutzte privilegierte Zugriffsberechtigungen können z. B. als Sicherheitsvorfall behandelt werden, vgl. SIM-01.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Vergabe von Prüfungsberechtigungen ist manuell zu prüfen. Dies beinhaltet die Klassifizierung als privilegiert, Personalisierung und die Bewertung des Need-to-Know-Prinzips. Die zeitliche Befristung könnte ausgelesen werden, hierzu wäre der Implementierungsaufwand voraussichtlich aber sehr hoch. Eine kontinuierliche Prüfung erscheint hier nicht zielführend. Lediglich der Systemstatus könnte kontinuierlich überprüft werden. Das automatische Auslösen einer Benachrichtigung bei Verdachtsfällen könnte abgeglichen werden mit dokumentierten Maßnahmen, um diesen Fällen zu entgegnen. Hierzu muss jedoch dieser gesamte Prozess digitalisiert werden, der Aufwand hierzu erscheint derzeit sehr hoch. Eine

kontinuierliche Prüfung könnte jedoch den Zeitpunkt der letzten manuellen Prüfung ausgeben.

IDM-07 Zugriff auf Daten der Cloud-Kunden

Basiskriterium

Der Cloud-Kunde wird durch den Cloud-Anbieter über Ereignisse informiert, bei denen interne oder externe Mitarbeiter des Cloud-Anbieters, ohne vorherige Zustimmung des Cloud-Kunden, lesend oder schreibend auf die im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten der Cloud-Kunden zugreifen werden oder zugegriffen haben. Die Information erfolgt je Ereignis, soweit die Daten des Cloud-Kunden nicht verschlüsselt sind/waren, die Verschlüsselung für den Zugriff aufgehoben wird/wurde oder die vertraglichen Vereinbarungen eine solche Information nicht explizit ausschließen. Aus der Information gehen Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs hervor. Die Informationen sind hinreichend detailliert, um sachverständigen Personen des Cloud-Kunden eine Risikobeurteilung des Zugriffs zu ermöglichen. Die Information erfolgt gemäß der vertraglichen Vereinbarung, spätestens aber 72 Stunden nach dem Zugriff.

Zusatzkriterium

Zugriffe auf die im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten durch interne oder externe Mitarbeiter des Cloud-Anbieters bedürfen der vorherigen Zustimmung durch autorisiertes Personal des Cloud-Kunden, soweit die Daten des Cloud-Kunden nicht verschlüsselt sind, die Verschlüsselung für den Zugriff aufgehoben wird oder die vertraglichen Vereinbarungen eine solche Zustimmung nicht explizit ausschließen. Für die Zustimmung werden dem autorisierten Personal aussagekräftige Information über Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs vorgelegt, um eine Risikobeurteilung des Zugriffs zu ermöglichen.

Ergänzende Informationen

Zum Kriterium

Sachverständige Personen im Sinne dieses Kriteriums sind Personen aus z. B. IT, Compliance oder Interne Revision.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung der durchgeführten Benachrichtigungen erscheint nur dann praktikabel, wenn die genannten Zugriffe auch automatisiert protokolliert und klassifiziert werden. Die inhaltliche Überprüfung der Benachrichtigungen kann nur dann erfolgen, wenn die Inhalte nach einem bestimmten Schema vom Cloud-Anbieter strukturiert sind. Dann können ein Abgleich sowie eine Plausibilisierung stattfinden. Eine kontinuierliche Prüfung würde dann alle Benachrichtigungen nach deren Eingang testen und somit überprüfen, inwiefern der Prozess in allen Fällen richtig abgelaufen ist.

IDM-08 Vertraulichkeit von Authentisierungsinformationen

Basiskriterium

Die Zuteilung von Authentisierungsinformationen zum Zugriff auf Systemkomponenten zur Bereitstellung des Cloud-Dienstes an interne und externe Benutzer des Cloud-Anbieters und Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, erfolgt in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt.

Soweit Passwörter als Authentisierungsinformationen eingesetzt werden, ist deren Vertraulichkeit durch folgende Verfahren sichergestellt, soweit dies technisch möglich ist:

- Benutzer können das Passwort initial selbst erstellen oder müssen ein initial

vorgegebenes Passwort bei der ersten Anmeldung an der Systemkomponente ändern. Ein initial vorgegebenes Passwort verliert nach maximal 14 Tagen seine Gültigkeit
- Beim Erstellen von Passwörtern wird das Einhalten der Passwort-Vorgaben (vgl. IDM-09) erzwungen, soweit dies technisch möglich ist
- Der Benutzer wird über das Ändern oder Zurücksetzen des Passworts informiert
- Die serverseitige Speicherung erfolgt unter Anwendung kryptographisch starker Passworthashfunktionen

Abweichungen sind durch eine Risikoanalyse bewertet und daraus abgeleitete, mitigierende Maßnahmen umgesetzt.

Zusatzkriterium

Die Benutzer bestätigen in einer Erklärung (vgl. HR-06), dass sie persönliche (bzw. geteilte) Authentisierungsinformationen vertraulich behandeln und ausschließlich für sich (bzw. innerhalb der Gruppe) behalten.

Ergänzende Informationen

Zum Kriterium

Zur Verwendung einer Passworthashfunktion eignet sich beispielsweise Argon2i.

Erklärungen können, soweit dies rechtsverbindlich ist, mittels einer elektronischen Signatur unterschrieben werden.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Soweit die Umsetzung durch eine entsprechende Systemkonfiguration erzwungen wird, kann der Status der Konfiguration bzw. deren letzten Änderung regelmäßig überprüft werden.

IDM-09 Authentisierungsmechanismen

Basiskriterium

Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes verwendet werden, authentifizieren Benutzer der internen und externen Mitarbeiter des Cloud-Anbieters sowie der Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben. Der Zugriff auf die Produktionsumgebung erfordert eine Zwei- oder Mehr-Faktor-Authentisierung. Innerhalb der Produktionsumgebung erfolgt die Authentifizierung der Benutzer durch Passwörter, digital signierte Zertifikate oder Verfahren, die ein mindestens gleichwertiges Sicherheitsniveau erreichen. Soweit digital signierte Zertifikate verwendet werden, erfolgt die Verwaltung gemäß der Richtlinie zur Schlüsselverwaltung (vgl. CRY-01). Die Passwort-Vorgaben sind aus einer Risikobewertung abgeleitet sowie in einer Richtlinie für Passwörter gemäß SP-01, dokumentiert, kommuniziert und bereitgestellt. Die Einhaltung der Vorgaben wird durch die Konfiguration der Systemkomponenten erzwungen, soweit dies technisch möglich ist.

Zusatzkriterium

Der Zugriff auf die nicht-Produktionsumgebung erfordert eine Zwei- oder Mehr-Faktor-Authentisierung. Innerhalb der nicht-Produktionsumgebung erfolgt die Authentifizierung der Benutzer durch Passwörter, digital signierte Zertifikate oder Verfahren, die ein mindestens gleichwertiges Sicherheitsniveau erreichen.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Soweit die Umsetzung durch eine entsprechende Systemkonfiguration erzwungen wird, kann der Status der Konfiguration bzw. deren letzten Änderung regelmäßig überprüft werden.

6.8 Kryptographie und Schlüsselmanagement (CRY)

Zielsetzung: *Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information*

CRY-01 Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für Verschlüsselungsverfahren und Schlüsselverwaltung sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt, in denen die folgenden Aspekte beschrieben sind:

- die Nutzung starker Verschlüsselungsverfahren und die Verwendung sicherer Netzprotokolle, die dem Stand der Technik entsprechen,
- risikobasierte Vorschriften für den Einsatz von Verschlüsselung, die mit Schemata zur Informationsklassifikation abgeglichen sind und den Kommunikationskanal sowie die Art, Stärke und Qualität der Verschlüsselung berücksichtigen,
- Anforderungen für das sichere Erzeugen, Speichern, Archivieren, Abrufen, Verteilen, Entziehen und Löschen der Schlüssel,
- Berücksichtigung der relevanten rechtlichen und regulatorischen Verpflichtungen und Anforderungen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Der Stand der Technik bezüglich starker Verschlüsselungsverfahren und sicherer Netzprotokolle ist in der jeweils aktuellen Fassung der folgenden technischen Richtlinien des BSI festgelegt:

- BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen"
- BSI TR-02102-2 „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"
- BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)"
- BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)".

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

CRY-02 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)

Basiskriterium

Der Cloud-Anbieter hat für das Übertragen von Daten der Cloud-Kunden über öffentliche Netze Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung etabliert.

Zusatzkriterium

Der Cloud-Anbieter hat für das Übertragen aller Daten Verfahren und technische Maßnahmen zur

starken Verschlüsselung und Authentifizierung etabliert.

Ergänzende Informationen

Zum Kriterium

Bei der Übertragung von Daten mit einem normalen Schutzbedarf innerhalb der Infrastruktur des Cloud-Anbieters ist keine zwingende Verschlüsselung anzuwenden, soweit die Übertragung nicht über öffentliche Netze erfolgt. In diesem Fall kann die nicht-öffentliche Umgebung des Cloud-Anbieters grundsätzlich als vertrauenswürdig angesehen werden. Als starke Transportverschlüsselungen, die dem Stand der Technik entsprechen, werden aktuell die Protokolle TLS 1.2 bzw. TLS 1.3, jeweils in Kombination mit Perfect Forward Secrecy angesehen. Die konkrete Konfiguration sollte den Empfehlungen der (jeweils aktuellen Fassung) der Technische Richtlinie des BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)" folgen. Die Nutzung von Wildcard Zertifikaten wird im Allgemeinen nicht als sicheres Verfahren erachtet.

Das Basiskriterium zur Übertragung von Daten der Cloud-Kunden betrifft z. B. das Versenden von elektronischen Nachrichten über öffentliche Netze.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass ihre Daten gemäß dem jeweiligen Schutzbedarf über verschlüsselte Verbindungen übertragen werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Verfahren und technischen Maßnahmen zur Verschlüsselung von Daten während der Übertragung werden zentral konfiguriert. Diese Konfiguration ändert sich nur selten. Deswegen wäre eine kontinuierliche Prüfung nicht zielführend, da lediglich Veränderungen an dieser Konfiguration überprüft werden müssten. Im Rahmen der kontinuierlichen Prüfung kann der Systemstatus aber kontinuierlich überprüft und regelmäßig ausgegeben werden. Dies gilt ebenso für das Zusatzkriterium.

CRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung

Basiskriterium

Der Cloud-Anbieter hat Verfahren und technische Maßnahmen zur Verschlüsselung von Daten der Cloud-Kunden bei der Speicherung etabliert. Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich dem Cloud-Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt. Ausnahmen folgen einem geregelten Verfahren. Die Verfahren zur Verwendung privater Schlüssel, inklusive gegebenenfalls bestehender Ausnahmen, sind mit dem Cloud-Kunden vertraglich zu vereinbaren.

Zusatzkriterium

Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich und ohne Ausnahme dem Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt.

Ergänzende Informationen

Zum Kriterium

Eine Ausnahme von der Anforderung, dass Schlüssel ausschließlich den Cloud-Kunden bekannt sind, kann z. B. das Verwenden eines Generalschlüssels durch den Cloud-Anbieter darstellen. Setzt der Cloud-Anbieter ein Verfahren zur Verwendung eines Generalschlüssels ein, sollte er die Angemessenheit sowie Wirksamkeit des Verfahrens und der Maßnahmen regelmäßig stichprobenhaft überprüfen. Dieses Kriterium bezieht sich nicht auf Daten, die für die Erbringung des Cloud-Dienstes funktionsbedingt nicht verschlüsselt sein können.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die

in ihrem Verantwortungsbereich liegen (z. B. virtuelle Maschinen innerhalb einer IaaS-Lösung), sicher, dass ihre Daten bei der Speicherung gemäß dem jeweiligen Schutzbedarf verschlüsselt werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Verschlüsselung Daten der Cloud-Kunden ist zentral konfiguriert und daher nur bedingt für eine kontinuierliche Prüfung geeignet. Ausnahmen zur Verschlüsselung von Daten gemäß eines geregelten Verfahrens sowie die Abstimmung des Verfahrens mit Cloud-Kunden sollten dokumentiert und genehmigt werden. Auch dies eignet sich nur bedingt für eine kontinuierliche Prüfung, da diese Ausnahmen in Einzelfällen von Fall zu Fall beschlossen werden und nicht in hoher Frequenz auftreten. In einer kontinuierlichen Prüfung kann per Systemzustand abgefragt werden, ob die Verschlüsselung aktiv ist und die genehmigten Ausnahmen eingehalten werden.

CRY-04 Sichere Schlüsselverwaltung

Basiskriterium

Die Verfahren und technische Maßnahmen zur sicheren Verwaltung von Schlüsseln im Verantwortungsbereich des Cloud-Anbieters beinhalten mindestens die folgenden Aspekte:

- Schlüsselgenerierung für unterschiedliche kryptographische Systeme und Applikationen,
- Ausstellung und Einholung von Public-Key-Zertifikaten,
- Provisionierung und Aktivierung von Schlüsseln,
- Sicheres Speichern von Schlüsseln (Separierung des Key-Management-Systems von Anwendungs- und Middleware Ebene), einschließlich der Beschreibung wie autorisierte Nutzer den Zugriff erhalten,
- Ändern oder Aktualisieren von kryptographischen Schlüssel einschließlich Richtlinien, die festlegen, unter welchen Bedingungen und auf welche Weise die Änderungen bzw. Aktualisierungen zu realisieren sind,
- Umgang mit kompromittierten Schlüsseln,
- Entzug und Löschen von Schlüsseln,
- Falls pre-shared keys verwendet werden, sind die Besonderheiten in Bezug auf sichere Nutzung dieses Verfahrens gesondert aufgeführt.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Schlüssel sollten z. B. im Falle von Kompromittierung oder Mitarbeiterveränderungen entzogen bzw. gelöscht werden. Der Cloud-Anbieter schützt die von Cloud-Kunden selbst erstellten und in den Cloud-Dienst eingebrachten Schlüssel nach den gleichen Maßgaben, nach denen er die von ihm selbst erstellten Schlüssel schützt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Damit Verfahren und technische Maßnahmen zur Schlüsselverwaltung die geforderten Aspekte berücksichtigen, müssen diese Aspekte in der entsprechenden Konfiguration umgesetzt sein. Diese Konfigurationen werden nur selten verändert und lediglich diese Veränderungen wären zielführend kontinuierlich zu prüfen. Daher ist eine kontinuierliche Prüfung hier nur bedingt zielführend. In einer kontinuierlichen Prüfung könnte jedoch der Systemstatus ausgelesen und bei Unregelmäßigkeiten wiedergegeben und dokumentiert werden.

6.9 Kommunikationssicherheit (COS)

Zielsetzung: *Sicherstellen des Schutzes von Informationen in* Netzen *und den entsprechenden informationsverarbeitenden Systemen.*

COS-01 Technische Schutzmaßnahmen

Basiskriterium

Basierend auf den Ergebnissen einer gemäß OIS-06 durchgeführten Risiko-Analyse, hat der Cloud-Anbieter technische Schutzmaßnahmen implementiert, die geeignet sind, netzbasierte Angriffe auf Basis anomaler Eingangs- oder Ausgangs-Traffic-Muster und/oder Distributed-Denial-of-Service (DDoS) Angriffe zeitnah zu erkennen und darauf zu reagieren. Aus entsprechend implementierten technischen Schutzmaßnahmen stammende Daten werden in ein übergreifendes SIEM-System (Security Information and Event Management) eingespeist, sodass für korrelierende Ereignisse erforderliche (Gegen-) Maßnahmen initiiert werden können. Die Schutzmaßnahmen sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt.

Zusatzkriterium

Der Cloud-Anbieter stellt mit technischen Maßnahmen sicher, dass seinem (physischen oder virtuellen) Netz keine unbekannten (physischen oder virtuellen) Geräte beitreten.

Ergänzende Informationen

Zum Kriterium

Netzbasierte Angriffe können z. B. durch MAC-Spoofing und ARP-Poisoning-Angriffe erfolgen. Technische Maßnahmen zum Verhindern des Beitretens unbekannter physischer oder virtueller Geräte zu einem physischen oder virtuellen Netz können sich z. B. an MACSec gemäß IEEE 802.1X:2010 orientieren.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen (z. B. virtuelle Maschinen innerhalb einer IaaS-Lösung), sicher, dass sie netzbasierte Angriffe auf Basis anomaler Eingangs- und Ausgangs-Traffic Muster (z. B. durch MAC-Spoofing und ARP-Poisoning-Angriffe) und/oder Distributed-Denial-of-Service (DDoS) Angriffe zeitnah erkennen und auf diese reagieren.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die technischen Schutzmaßnahmen eignen sich nur bedingt für eine kontinuierliche Prüfung, da diese nur selten verändert werden. Die Daten, die in das übergreifende SIEM-System eingespeist werden und die Erkennung von korrelierenden Ereignissen, eignen sich jedoch für eine kontinuierliche Prüfung. Diese Daten lassen sich automatisiert und kontinuierlich auswerten, ebenso wie die Überwachung der korrelierenden Ereignisse.

COS-02 Sicherheitsanforderungen an Verbindungen im Netz des Cloud-Anbieters

Basiskriterium

Für die Herstellung von Verbindungen innerhalb des Netzes des Cloud Anbieters sind spezifische Sicherheitsanforderungen konzipiert, veröffentlicht und bereitgestellt. In den Sicherheitsanforderungen ist für den Verantwortungsbereich des Cloud Anbieters festgelegt:

- in welchen Fällen die Sicherheitszonen zu separieren sind und in welchen Fällen Cloud-Kunden logisch oder physisch zu trennen sind,
- welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
- wie der Datenverkehr für Administration und Monitoring netztechnisch zu trennen ist,
- welche interne, standortübergreifende Kommunikation zugelassen ist,
- welche übergreifende Kommunikation zugelassen ist.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Standortübergreifende Kommunikation kann z. B. für einzelne Regionen oder Rechenzentren via z. B. WAN, LAN, VPN, RAS realisiert werden.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die geforderten Sicherheitsanforderungen werden zentral dokumentiert und selten verändert. Eine kontinuierliche Prüfung ist somit nur bedingt zielführend.

COS-03 Überwachung von Verbindungen im Netz des Cloud-Anbieters

Basiskriterium

Es wird zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzen unterschieden. Diese sind basierend auf einer Risikobewertung in verschiedene Sicherheitszonen für interne und externe Netzbereiche (und ggf. DMZ) separiert. Physische und virtualisierte Netzumgebungen sind so konzipiert und konfiguriert, dass die hergestellte Verbindung zu vertrauenswürdigen oder nicht vertrauenswürdigen Netzen gemäß den definierten Sicherheitsanforderungen beschränkt und überwacht wird. Die Gesamtheit der vorgenommenen Konzeption und Konfiguration zur Überwachung der genannten Verbindungen wird risikoorientiert, mindestens jährlich, in Bezug auf die daraus resultierenden Sicherheitsanforderungen überprüft. Identifizierte Schwachstellen und Abweichungen werden gemäß dem Verfahren zum Umgang mit Risiken (vgl. OIS-06) einer Risikobeurteilung unterzogen und Maßnahmen zur Behandlung definiert und nachverfolgt (vgl. OPS-18). In festgelegten Abständen wird die geschäftliche Rechtfertigung für die Verwendung aller Dienste, Protokolle und Ports überprüft. Darüber hinaus umfasst die Überprüfung auch die Begründungen für kompensierende Maßnahmen für die Verwendung von Protokollen, die als unsicher angesehen werden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die Überprüfung der Sicherheitsanforderungen hängt von den eingerichteten Maßnahmen zur Ausgestaltung der Netze ab und kann z. B. die Überwachung und Durchsicht von Firewall-Regeln oder Protokolldateien auf Auffälligkeiten sowie Sichtprüfungen physischer Netzkomponenten auf Veränderungen umfassen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für die virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass diese gemäß ihren Netzsicherheitsanforderungen konzipiert, konfiguriert und dokumentiert sind (z. B. logische Segmentierung der Organisationseinheiten des Cloud-Kunden).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Werden die geschäftliche Rechtfertigung und die regelmäßige Überprüfung des Konzepts zur Überwachung standardisiert dokumentiert, lassen sich diese Prozesse automatisiert auswerten. Somit kann eine kontinuierliche Prüfung angesetzt werden. Die Trennung der Netze eignet sich ebenfalls für eine kontinuierliche Prüfung, da hier der Status der Trennung kontinuierlich überprüft werden kann.

COS-04 Netzübergreifende Zugriffe

Basiskriterium

Jeder Netzperimeter wird von Sicherheitsgateways kontrolliert. Die Zugangsberechtigung für netzübergreifende Zugriffe basiert auf einer Sicherheitsbewertung

auf Grundlage der Anforderungen der Cloud-Kunden.

Zusatzkriterium

Jeder Netzperimeter wird von redundanten und hochverfügbaren Sicherheitsgateways kontrolliert.

Ergänzende Informationen

Zum Kriterium

Netzübergreifende Zugriffe sind Zugriffe von einem Netz in ein anderes Netz über einen definierten Netzperimeter.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für die Perimeter der virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass der Zugriff durch Sicherheitsgateways gemäß seines Schutzbedarfs kontrolliert wird.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Wird die Kontrolle der Netzperimeter dokumentiert (beispielsweise durch Protokolle/Logs), können diese Logs automatisiert ausgewertet werden. Dadurch bietet sich die Möglichkeit einer kontinuierlichen Prüfung für diesen Teil des Kriteriums. Erfolgt die Sicherheitsbewertung für Zugangsberechtigungen beim Cloud-Anbieter in standardisierter Form, so kann auch diese automatisiert ausgewertet werden. In diesem Falle wäre auch eine kontinuierliche Prüfung für den zweiten Teil des Kriteriums möglich.

COS-05 Netze zur Administration

Basiskriterium

Es existieren gesonderte Netze zur administrativen Verwaltung der Infrastruktur und für den Betrieb von Managementkonsolen, die logisch oder physisch vom Netz der Cloud-Kunden getrennt und durch Multi-Faktor-Authentifizierung vor unberechtigten Zugriffen geschützt sind (vgl. IDM-09). Netze, die seitens des Cloud Anbieters zum Zwecke der Migration oder dem Erzeugen von virtuellen Maschinen dienen, sind ebenfalls physisch oder logisch von anderen Netzen separiert.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine kontinuierliche Prüfung ist hier nur bedingt zielführend, da Infrastrukturkomponenten sowie die logische und physische Trennung der Netze initial implementiert werden und eine kontinuierliche Überprüfung dieser Komponenten zwar einen Systemstatus erfragen kann, es jedoch schwer ist, alle Aspekte kontinuierlich zu testen.

COS-06 Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen

Basiskriterium

Der Datenverkehr von Cloud-Kunden in gemeinsam genutzten Netzumgebungen wird gemäß eines dokumentierten Konzepts zur Segmentierung auf Netzebene segregiert, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten.

Zusatzkriterium

Bei IaaS/PaaS ist die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt. Zur Definition einer starken Verschlüsselung ist die technische Richtlinie TR02102 des BSI zu berücksichtigen.

Ergänzende Informationen

Zum Kriterium

Soweit Angemessenheit und Wirksamkeit der logischen Segmentierung nicht mit hinreichender Sicherheit beurteilt werden können (z. B. aufgrund einer komplexen Implementierung), kann der Nachweis auch über Prüfungsergebnisse sachverständiger Dritter erfolgen (z. B. Sicherheitsaudit zur Validierung des Konzepts). Die Segregation gespeicherter und verarbeiteter Daten ist Gegenstand des Kriteriums OPS-25. Zur sicheren Segmentierung gemeinsam genutzter Ressourcen bei Webanwendungen, die als SaaS bereitgestellt werden, sollte die Session-ID in der Grundstufe

- zufallsgeneriert sein und eine ausreichende Entropie von mindestens 128 Bit (16 Zeichen) haben, um dem Erraten der Session-ID (zum Beispiel durch einen Brute-Force-Angriff) standzuhalten,
- bei der Übertragung und clientseitigen Speicherung ausreichend geschützt sein,
- eine begrenzte Gültigkeit (Timeout) haben, die gemessen an den Anforderungen zur Nutzung der Webanwendung möglichst kurz ist.

Nach erfolgreicher Authentisierung über einen ungesicherten Kommunikationskanal (HTTP) soll auf einen gesicherten Kommunikationskanal (HTTPS) gewechselt werden.

Bei IaaS/PaaS ist die sichere Trennung durch physisch getrennte Netze oder durch starke Verschlüsselung der Netze sichergestellt. Zur Definition einer starken Verschlüsselung ist die technische Richtlinie TR02102 des BSI zu berücksichtigen (vgl. CRY-01).

Falls der Cloud-Anbieter keine gemeinsam genutzten Netzumgebungen für Cloud-Kunden verwendet und somit eine physische Trennung vornimmt, ist das Basiskriterium nicht anwendbar.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen für den Datenverkehr und die virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass diese gemäß ihren Netzsicherheitsanforderungen konzipiert, konfiguriert und dokumentiert sind (z. B. logische Segmentierung der Organisationseinheiten der Cloud-Kunden).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die logische Segregierung des Netzverkehrs von Cloud-Kunden auf Netzebene ist zentral konfiguriert und wird nur selten verändert. Somit ist eine kontinuierliche Prüfung nicht zielführend, da keine hoch frequentierte automatisierte Abfrage erfolgen kann, welche die kontinuierliche Prüfung stützt.

COS-07 Dokumentation des Netzes

Basiskriterium

Die logische Struktur des Netzes, das zum Erbringen oder Betreiben des Cloud-Dienstes verwendet wird, ist nachvollziehbar und aktuell dokumentiert, um im Wirkbetrieb Fehler in der Verwaltung zu vermeiden und um im Störungsfall eine zeitgerechte Wiederherstellung gemäß den vertraglichen Verpflichtungen zu gewährleisten. Aus der Dokumentation geht insbesondere hervor, wie die Subnetze zugeordnet und wie das Netz zoniert sowie segmentiert wird. Darüber hinaus werden die geografischen Lokationen angegeben, in denen die Daten der Cloud-Kunden gespeichert werden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Bei einer Zonierung handelt es sich um eine Segmentierung der Subnetze mit einer an den Netzperimetern implementierten Firewall.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die Dokumentation der logischen Struktur des Netzes wird selten verändert und ist zentral dokumentiert. Somit ist eine kontinuierliche Prüfung nicht zielführend. Eine kontinuierliche Prüfung könnte aber das Datum der letzten Änderung der Dokumentation zurückgeben.

COS-08 Richtlinien zur Datenübertragung

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zum Schutz der Datenübertragung vor unbefugtem Abfangen, Manipulieren, Kopieren, Modifizieren, Umleiten oder Vernichten sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben stellen einen Bezug zur Klassifikation von Informationen her (vgl. AM-06).

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Eine Maßnahme gegen das unbefugte Abfangen, Manipulieren, Kopieren, Modifizieren, Umleiten oder Vernichten von Daten während der Übertragung ist z. B. der Einsatz von Transportverschlüsselung gemäß CRY-02.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die an den Cloud-Dienst übertragenen Daten gemäß ihrem Schutzbedarf vor Manipulieren, Kopieren, Modifizieren, Umleiten oder Löschen geschützt sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

6.10 Portabilität und Interoperabilität (PI)

Zielsetzung: *Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen.*

PI-01 Dokumentation und Sicherheit der Eingangs- und Ausgangs-Schnittstellen

Basiskriterium

Der Cloud-Dienst kann von anderen Cloud-Diensten oder IT-Systemen der Cloud-Kunden über dokumentierte Eingangs- und Ausgangs-Schnittstellen angesprochen werden. Dazu ist für sachverständiges Personal ersichtlich dokumentiert, wie die Schnittstellen zur Rückgabe der Daten genutzt werden können.

Die Kommunikation erfolgt über standardisierte Kommunikationsprotokolle, mit denen die Vertraulichkeit und Integrität der übertragenen Informationen gemäß ihrem Schutzbedarf sichergestellt wird. Die Kommunikation über nicht vertrauenswürdige Netze ist gemäß CRY-02 verschlüsselt.

Art und Umfang der Dokumentation zu den Schnittstellen orientieren sich am Bedarf sachverständigen Personals der Cloud-Kunden, um die Nutzung dieser Schnittstellen zu ermöglichen. Die Informationen werden so gepflegt, dass sie für den bereitgestellten Cloud-Dienst in der für die produktive Nutzung vorgesehenen Version anwendbar sind.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Der Kunde muss durch geeignete Kontrollen vor Beginn der Nutzung des Cloud-Dienstes und bei jeder Änderung der Schnittstellen sicherstellen, dass die bereitgestellten Schnittstellen (und deren Sicherheit) entsprechend seines Schutzbedarfs angemessen sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die definierten Eingangs- und Ausgangsschnittstellen der Cloud-Dienste werden selten verändert. Somit reicht es für den Prüfer aus, diese Schnittstellen, die Kommunikation eventueller Änderungen und die zugehörige Dokumentation im Rahmen der zyklischen Prüfung zu testen.

In einer kontinuierlichen Prüfung könnte aber der Systemstatus der Schnittstellen abgefragt und kontinuierlich ausgewertet werden.

PI-02 Vertragliche Vereinbarungen zur Bereitstellung von Daten

Basiskriterium

In vertraglichen Vereinbarungen sind folgende Aspekte hinsichtlich der Beendigung des Auftragsverhältnisses definiert, soweit diese für den Cloud-Dienst anwendbar sind:

- Art, Umfang und Format der Daten, die der Cloud-Anbieter dem Cloud-Kunden übergibt,
- Definition der Frist, innerhalb derer der Cloud-Anbieter dem Cloud-Kunden die Daten verfügbar macht,
- Definition des Zeitpunktes, zu dem der Cloud-Anbieter die Daten für den Cloud-Kunden unzugänglich macht und löscht,
- Verantwortlichkeiten und Mitwirkungspflichten des Cloud-Kunden beim Bereitstellen der Daten.

Die Definitionen orientieren sich am Bedarf sachverständiger Personen potentieller Kunden, um die Eignung des Cloud-Dienstes hinsichtlich der Abhängigkeit vom Cloud-Anbieter sowie rechtlicher und regulatorischer Anforderungen zu beurteilen.

Zusatzkriterium

Die Ausgestaltung der Aspekte orientiert sich an rechtlichen und regulatorischen Anforderungen im Umfeld des Cloud-Anbieters. Die Anforderungen werden vom Cloud-Anbieter erhoben und regelmäßig, mindestens jährlich, auf Aktualität überprüft, und die vertraglichen Vereinbarungen entsprechend angepasst.

Ergänzende Informationen

Zum Kriterium

Art und Umfang der Daten sowie die Verantwortlichkeiten für die Bereitstellungen hängen vom Service-Modell des Cloud-Dienstes bzw. den bereitgestellten Diensten und Funktionen ab:

Bei IaaS und PaaS ist grundsätzlich der Cloud-Kunde verantwortlich, die im Cloud-Dienst gespeicherten Daten vor Beendigung des Auftragsverhältnisses außerhalb des Cloud-Dienstes zu sichern (vgl. komplementäres Kriterium).

Die Verantwortung des Cloud-Anbieters ist typischerweise auf die Bereitstellung von Daten zur Konfiguration der Infrastruktur bzw. der Plattform beschränkt, die der Cloud-Kunde innerhalb seiner Umgebung aufgebaut hat (z. B. Konfiguration der Netze, Images der virtuellen Maschinen und Container).

Bei SaaS ist der Cloud-Kunde typischerweise auf Export-Funktionen angewiesen, die der Cloud-Anbieter zur Verfügung stellt. Vom Cloud-Kunden erstellte Daten sollten dabei im gleichen Format zur Verfügung stehen, wie sie im Cloud-Dienst gespeichert wurden. Andere Daten, einschließlich relevanter Protokolldateien und Metadaten, sollten in einem anwendbaren Standardformat zur Verfügung stehen, z. B. CSV, JSON oder XML.

In Deutschland lassen sich gesetzliche Vorgaben zur Aufbewahrung beispielsweise der Abgabenordnung (§147 AO) und dem Handelsgesetzbuch (§ 257 HGB) entnehmen. Diese sehen eine Aufbewahrungspflicht von sechs oder zehn Jahren vor.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, die ihnen vertraglich zustehenden Daten beim Cloud-Anbieter am Vertragsende anzufragen oder über definierte Schnittstellen abzurufen (Art und Umfang der Daten entsprechen den vertraglichen Vereinbarungen, die vor Nutzung des Cloud-Dienstes festgelegt wurden) und für eine Aufbewahrung gemäß der für diese Daten geltenden gesetzlichen Anforderungen zu sorgen.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Der Cloud-Anbieter sollte ein standardisiertes Template für seine Verträge aufgesetzt haben. Danach sind alle Verträge nach dem gleichen Muster aufgebaut.

Dieses Template wird nur selten verändert. Daher ist hier eine kontinuierliche Prüfung nur bedingt zielführend. Es reicht somit aus, die Verträge und das zugehörige Template im Rahmen der zyklischen Prüfung zu testen.

PI-03 Sichere Datenlöschung

Basiskriterium

Die Verfahren des Cloud-Anbieters zur Löschung der Daten des Cloud-Kunden bei Beendigung des Auftragsverhältnisses stellen die Einhaltung der vertraglichen Vereinbarungen sicher (vgl. PI-02).

Die Löschung umfasst Daten in der Umgebung des Cloud-Kunden, Metadaten und Daten in der Datensicherung.

Die Löschverfahren verhindern eine Wiederherstellung mit forensischen Mitteln.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Geeignete Löschverfahren sind z. B. mehrfaches Überschreiben oder das Löschen des Schlüssels.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die rechtlichen und regulatorischen Rahmenbedingungen (z. B. gesetzliche Anforderungen an Aufbewahrung und Löschung) identifiziert sind und die Löschung ihrer Daten entsprechend initiiert wird.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die vollständige Löschung der Daten wird vom Cloud-Anbieter in Protokollen/Logs dokumentiert. Dabei sollten die Protokolle/Logs umfassen, welche Daten gelöscht wurden, damit nachvollziehbar ist, inwiefern Kundendaten, Metadaten und Daten in der Datensicherung gelöscht wurden.

Der Prüfer kann anschließend eine automatisierte Auswertung dieser Protokolle/Logs vornehmen. Zudem kann der Prüfer den Systemstatus des Verfahrens zur Löschung der Daten überprüfen.

Dass die Löschverfahren eine Wiederherstellung mit forensischen Mitteln verhindern, muss nicht kontinuierlich geprüft werden. Die eingesetzten Löschverfahren können im Rahmen der zyklischen Prüfung getestet werden.

6.11 Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)

Zielsetzung: *Sicherstellen der Informationssicherheit im Entwicklungszyklus von Informationssystemen.*

DEV-01 Richtlinien zur Entwicklung/Beschaffung von Informationssystemen

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die sichere Entwicklung des Cloud-Dienstes sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt.

Die Richtlinien und Anweisungen enthalten Vorgaben über den gesamten Lebenszyklus des Cloud-Dienstes und orientieren sich hinsichtlich der folgenden Aspekte an anerkannten Standards und Methoden:

- Sicherheit in der Software-Entwicklung (Anforderungen, Design, Implementierung, Tests und Überprüfungen)
- Sicherheit in der Software-Bereitstellung
- Sicherheit im Betrieb (Reaktion auf identifizierte Fehler und Schwachstellen)

Zusatzkriterium

Bei der Beschaffung werden Produkte vorgezogen, die nach den „Common Criteria for Information Technology Security Evaluation" (kurz: Common Criteria – CC) gemäß Prüftiefe EAL 4 (oder höher) zertifiziert wurden. Soweit bei verfügbaren zertifizierten Produkten abweichend unzertifizierte Produkte beschafft werden sollen, erfolgt eine Risikobeurteilung gemäß OIS-07.

Ergänzende Informationen

Zum Kriterium

Die Software-Bereitstellung kann z. B. mit Continuous Delivery-Verfahren erfolgen.

Als akzeptierte Standards und Methoden gelten z. B.

- ISO/IEC 27034. und
- OWASP Secure Software Development Lifecycle (S-SDLC).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Inhalte der Richtlinien und Anweisungen für die ordnungsgemäße Entwicklung oder Beschaffung von Informationssystemen werden nicht in hoher Frequenz verändert. Eine kontinuierliche Prüfung dieser Dokumentation ist somit nicht zielführend. Die Integration dieser Tests in die zyklische Prüfung erscheint hinreichend.

DEV-02 Auslagerung der Entwicklung

Basiskriterium

Bei ausgelagerter Entwicklung des Cloud-Dienstes (oder einzelner Systemkomponenten) sind Vorgaben hinsichtlich der folgenden Aspekte vertraglich zwischen Cloud-Anbieter und Auftragnehmer der ausgelagerten Entwicklung zu vereinbaren:

- Sicherheit in der Software-Entwicklung (Anforderungen, Design, Implementierung, Tests und Überprüfungen) gemäß anerkanntem Standard und Methoden;
- Abnahmeprüfung der Qualität der erbrachten Leistungen gemäß den vereinbarten funktionalen und nicht-funktionalen Anforderungen,
- Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um das Vorhandensein bekannter Schwachstellen auszuschließen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Ausgelagerte Entwicklung im Sinne des Basiskriteriums bezieht sich auf die Entwicklung einer dediziert für den Cloud-Dienst verwendeten Systemkomponente durch einen Auftragnehmer des Cloud-Anbieters. Die Entwicklung erfolgt gemäß den Prozessen des Auftragnehmers.

Die Anschaffung frei verfügbarer oder am Markt erhältlicher Software sowie die Einbindung externer Mitarbeiter in die Prozesse des Cloud-Anbieters sind keine Auslagerung im Sinne des Basiskriteriums.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine ausgelagerte Entwicklung der Cloud-Dienste eines Cloud-Anbieters und die zugehörige Vertragserstellung und Unterzeichnung wird nicht mit hoher Frequenz durchgeführt. Änderungen in den Vertragsstrukturen sind auch nicht der Regelfall. Somit ist eine kontinuierliche Prüfung in diesen Fällen wenig zielführend.

DEV-03 Richtlinien zur Änderung von Informationssystemen

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zur Verwaltung von Änderungen (Change Management) an Systemkomponenten des Cloud-Dienstes im Rahmen der Software-Bereitstellung sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt:

- Kriterien zur Risikobeurteilung, Kategorisierung und Priorisierung von Änderungen und damit verbundene Anforderungen an Art und Umfang durchzuführender Tests sowie erforderliche Genehmigungen für die Entwicklung/Implementierung der Änderung sowie der Freigaben zur Bereitstellung in der Produktionsumgebung durch autorisiertes Personal oder Systemkomponenten,,
- Anforderungen an die Durchführung und Dokumentation von Tests,
- Anforderungen an die Funktionstrennung bei Entwicklung, Test und Freigabe von Änderungen,
- Anforderungen zur sachgerechten Information der Cloud-Kunden über Art und Umfang der Änderung sowie daraus resultierende Mitwirkungspflichten gemäß den vertraglichen Vereinbarungen,
- Anforderungen an die Dokumentation von Änderungen in der System-, Betriebs- und Benutzerdokumentation,
- Anforderungen an die Durchführung und Dokumentation von Notfalländerungen, die dem gleichen Sicherheitsniveau wie normale Änderungen genügen müssen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Änderungen im Sinne des Basiskriteriums sind solche, die zu Änderungen an der Konfiguration, Funktionalität oder Sicherheit von Systemkomponenten des Cloud-Dienstes in der Produktionsumgebung führen können. Dies umfasst sowohl Änderungen an der Infrastruktur als auch am Quellcode.

Soweit einzelne Änderungen zur Software-Bereitstellung in einem neuen Release, Update, Patch oder einem vergleichbaren Softwareobjekt zusammengefasst werden, gilt dieses Softwareobjekt als Änderung im Sinne des Basiskriteriums, nicht aber die einzelnen darin enthaltenen Änderungen.

Änderungen an der bestehenden Netzkonfiguration müssen ebenfalls ein

geregeltes Verfahren durchlaufen, da sie für eine wirksame Mandantentrennung notwendig sind.

Personal oder Systemkomponenten werden gemäß den Vorgaben für Zugangs- und Zugriffsberechtigungen (vgl. IDM-01) im Rahmen eines geregelten Verfahrens (vgl. IDM-02) für Genehmigungen und Freigaben autorisiert.

Sachgerechte Informationen umfassen z. B. Beschreibungen neuer Funktionen.

Mitwirkungspflichten des Cloud-Kunden können z. B. definieren, dass der Cloud-Kunde bestimmte Tests durchzuführen hat.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Inhalte der Richtlinien und Anweisungen für die Verwaltung und Änderung an Systemkomponenten werden nicht in hoher Frequenz verändert. Eine kontinuierliche Prüfung dieser Dokumentation ist somit nicht zielführend. Es reicht aus, diese Tests in die zyklische Prüfung zu integrieren.

DEV-04 Programm zur Sicherheitsausbildung und Sensibilisierung bezüglich kontinuierlicher Software-Bereitstellung und zugehöriger Systeme, Komponenten oder Werkzeuge

Basiskriterium

Der Cloud-Anbieter betreibt ein Programm zur regelmäßigen, zielgruppenorientierten Sicherheitsausbildung und Sensibilisierung der internen und externen Mitarbeiter zu Standards und Methoden der sicheren Software-Entwicklung und Software-Bereitstellung sowie zum Umgang mit den dafür eingesetzten Werkzeugen. Das Programm wird regelmäßig in Bezug auf die gültigen Richtlinien und Anweisungen, die zugewiesenen Rollen und Verantwortlichkeiten sowie die genutzten Werkzeuge überprüft und angepasst.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Cloud-Anbieter kann die Überprüfung auf die gültigen Richtlinien und Anweisungen, die zugewiesenen Rollen und Verantwortlichkeiten sowie die genutzten Werkzeuge automatisiert vollziehen und durch Logs dokumentieren.

Diese Logs können durch den Prüfer automatisiert ausgewertet und somit einer kontinuierlichen Prüfung unterzogen werden.

DEV-05 Risikobewertung, Kategorisierung und Priorisierung von Änderungen

Basiskriterium

Änderungen werden gemäß den Richtlinien zum Change Management (vgl. DEV-03) einer Risikobeurteilung hinsichtlich potenzieller Auswirkungen auf die betroffenen Systemkomponenten unterzogen und entsprechend kategorisiert und priorisiert.

Zusatzkriterium

Autorisierten Personal oder autorisierten Systemkomponenten der Cloud-Kunden werden gemäß den vertraglichen Vereinbarungen aussagekräftige Information über Anlass, Zeitpunkt, Dauer, Art und Umfang der Änderung vorgelegt, um eine eigene Risikobeurteilung durchführen zu können, bevor die Änderung in der Produktionsumgebung bereitgestellt wird. Unabhängig der vertraglichen Vereinbarungen erfolgt dies für Änderungen, die aufgrund ihrer Risikobeurteilung die höchste Risikokategorie aufweisen.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Bewertung von Änderungen bei Releases kann durch den Cloud-Anbieter standardisiert und automatisiert erfolgen. Wird diese Bewertung in standardisierter und digitaler Form erbracht (Tickets/Logs), kann eine automatisierte Auswertung durch den Prüfer erfolgen und eine kontinuierliche Prüfung durchgeführt werden.

DEV-06 Testen der Änderungen

Basiskriterium

Änderungen am Cloud-Dienst werden im Rahmen der Software-Entwicklung und Software-Bereitstellung geeigneten Tests unterzogen.

Art und Umfang der Tests entsprechen der Risikobeurteilung. Die Durchführung erfolgt durch angemessen qualifiziertes Personal des Cloud-Anbieters oder durch automatisierte Testverfahren, die den anerkannten Regeln der Technik entsprechen. Cloud-Kunden werden gemäß den vertraglichen Anforderungen in die Tests eingebunden.

Der Schweregrad der in den Tests identifizierten Fehlern und Schwachstellen, welche für die Abnahme relevant sind, wird nach definierten Kriterien beurteilt und Maßnahmen zur zeitnahen Behebung oder Mitigation eingeleitet.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Eine Beurteilung der in Tests identifizierten Fehler und Schwachstellen kann z. B. gemäß Common Vulnerability Scoring System (CVSS) erfolgen.

Korrespondierende Kriterien für Kunden

Soweit Änderungen gemäß den vertraglichen Vereinbarungen vor der Bereitstellung in der Produktivumgebung durch die Cloud-Kunden zu testen sind, stellen diese durch geeignete Kontrollen sicher, dass die Tests angemessen durchgeführt werden, um Fehler zu identifizieren. Dies umfasst insbesondere die zeitgerechte Durchführung der Tests durch qualifiziertes Personal gemäß der vom Cloud-Anbieter vorgegebenen Rahmenbedingungen.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Werden die Tests automatisiert durchgeführt, können die Durchführung und zugehörige Ergebnisse in Protokollen/Logs dokumentiert werden. Diese Protokolle/Logs können anschließend kontinuierlich durch den Prüfer ausgelesen werden.

Maßnahmen zur Behebung identifizierter Schwachstellen können ebenso standardisiert festgehalten und durchgeführt werden, damit eine kontinuierliche Prüfung ermöglicht wird.

DEV-07 Protokollierung von Änderungen

Basiskriterium

Systemkomponenten und Werkzeuge zur Quellcode-Verwaltung und Software-Bereitstellung, mit denen Änderungen an Systemkomponenten des Cloud-Dienstes in der Produktionsumgebung durchgeführt werden, unterliegen einem Rollen- und Rechtekonzept gemäß IDM-01 und Autorisierungsmechanismen. Sie sind so zu konfigurieren, dass alle Änderungen protokolliert werden und diese somit auf die ausführenden Personen oder Systemkomponenten zurückgeführt werden können.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Änderungen am Rollen- und Rechtekonzept gemäß IDM-01 werden vom Cloud-Anbieter in Protokollen/Logs dokumentiert. Somit kann eine automatische und kontinuierliche Auswertung dieser durchgeführt werden. Hierbei werden Unregelmäßigkeiten aufgedeckt und ebenfalls protokolliert.

Der Prüfer kann eine kontinuierliche Prüfung durchführen indem er die Protokolle/Logs und protokollierten Unregelmäßigkeiten automatisiert auswertet.

DEV-08 Versionskontrolle

Basiskriterium

Verfahren zur Versionskontrolle sind eingerichtet, um Abhängigkeiten einzelner Änderungen nachzuvollziehen und in Folge aufgetretener Fehler oder identifizierter Schwachstellen betroffene Systemkomponenten in ihren vorherigen Zustand zurück zu versetzen.

Zusatzkriterium

Die Verfahren zur Versionskontrolle stellen durch geeignete Schutzmaßnahmen sicher, dass die Integrität und Verfügbarkeit der Daten von Cloud-Kunden nicht beeinträchtigt werden, wenn Systemkomponenten in ihren vorherigen Zustand zurückversetzt werden.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Verfahren zur Versionskontrolle des Cloud-Anbieters und gegebenenfalls auch ein Zurücksetzen in vorherige Zustände können automatisiert erfolgen. Dies ist in Logs zu dokumentieren.

Durch eine automatische Auswertung dieser Logs ist eine kontinuierliche Prüfung möglich.

DEV-09 Freigaben zur Bereitstellung in der Produktionsumgebung

Basiskriterium

Autorisiertes Personal oder Systemkomponenten des Cloud-Anbieters geben auf Basis definierter Kriterien (z. B. Testergebnisse und erforderliche Genehmigungen) Änderungen am Cloud-Dienst frei, bevor diese den Cloud-Kunden in der Produktionsumgebung bereitgestellt werden.

Cloud-Kunden werden gemäß den vertraglichen Anforderungen in die Freigabe eingebunden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Es gelten die Definitionen für Kriterium DEV-03.

Korrespondierende Kriterien für Kunden

Soweit Änderungen gemäß den vertraglichen Vereinbarungen vor der Bereitstellung in der Produktivumgebung durch die Cloud-Kunden freizugeben sind, stellen diese durch geeignete Kontrollen sicher, dass autorisiertes und qualifiziertes Personal die bereitgestellten Informationen entgegennimmt, die Auswirkungen im Rahmen des ISMS bewertet und gemäß der vom Cloud-Anbieter vorgegebenen Rahmenbedingungen über die Freigabe entscheidet.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Überprüfung, ob alle Tests vollständig durchgeführt wurden, erfolgreich waren und durch eine autorisierte Stelle genehmigt wurden kann durch den Cloud-Anbieter automatisiert erfolgen und in Form von Protokollen/Logs dokumentiert werden.

Diese Protokolle/Logs lassen sich anschließend durch den Prüfer automatisiert und kontinuierlich auswerten.

DEV-10 Trennung der Umgebungen

Basiskriterium

Produktionsumgebungen sind von Test- oder Entwicklungsumgebungen physisch oder logisch getrennt, um unautorisierte Zugriffe auf Daten der Cloud-Kunden, die Ausbreitung von Schadprogrammen oder Änderungen an Systemkomponenten zu verhindern. Daten aus Produktionsumgebungen werden nicht in Test- oder Entwicklungsumgebungen verwendet, um deren Vertraulichkeit nicht zu gefährden.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Da fundamentale Änderungen in Test- und Entwicklungsumgebungen, die die physische oder logische Trennung betreffen würden, nur selten vorgenommen werden, ist eine kontinuierliche Prüfung hier nicht zielführend. Die jeweiligen Umgebungen sind anfangs initial zu testen und anschließend bei Änderungen erneut zu überprüfen.

6.12 Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)

Zielsetzung: *Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.*

SSO-01 Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter

Basiskriterium

Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter (z. B. Dienstleister bzw. Lieferanten), deren Leistungen zur Bereitstellung des Cloud-Dienstes beitragen, sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt:

- Vorgaben für die Beurteilung der Risiken, die aus dem Bezug von Leistungen Dritter resultieren,
- Vorgaben für die Klassifizierung der Dritten auf Basis einer Risikobeurteilung durch den Cloud-Anbieter und der Feststellung, ob es sich um ein Subdienstleistungsunternehmen handelt (vgl. Ergänzende Information),
- Anforderungen an die Informationssicherheit bei der Verarbeitung, Speicherung oder Übertragung von Informationen durch Dritte, die sich an anerkannten Branchenstandards orientieren,
- Anforderungen an die Sensibilisierung und Schulung des Personals für Informationssicherheit,
- anwendbare rechtliche und regulatorische Anforderungen,
- Anforderungen an den Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen,
- Vorgaben für die vertragliche Vereinbarung dieser Anforderungen;
- Vorgaben für die Überwachung dieser Anforderungen,
- Vorgaben für die Weitergabe dieser Anforderungen auch an Dienstleister, die von den Dritten eingesetzt werden, soweit Leistungen dieser Dienstleister ebenso zur Bereitstellung des Cloud-Dienstes beitragen.

Zusatzkriterium

Subdienstleistungsunternehmen des Cloud-Anbieters werden vertraglich dazu verpflichtet, regelmäßige Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit ihres dienstleistungsbezogenen internen Kontrollsystems vorzulegen. Die Berichterstattungen umfassen die korrespondierenden Kontrollen beim Subdienstleister, die erforderlich sind, um zusammen mit den Kontrollen des Cloud-Anbieters, die anwendbaren Basiskriterien des BSI C5 mit hinreichender Sicherheit zu erfüllen. Soweit keine Berichterstattungen vorgelegt werden können, vereinbart der Cloud-Anbieter entsprechende Informations- und Prüfungsrechte, um die Angemessenheit und Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems einschließlich der korrespondierenden Kontrollen durch qualifiziertes Personal zu beurteilen.

Ergänzende Informationen

Zum Kriterium

Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit eines dienstleistungsbezogenen internen Kontrollsystems sind z. B. Berichterstattungen gemäß ISAE 3402, IDW PS 951, SOC 2 oder BSI C5. Qualifiziertes Personal ist z. B. in der Internen Revision des Cloud-Anbieters oder bei vom Cloud-Anbieter beauftragten Sachverständigen Dritten wie z. B. Wirtschaftsprüfungsgesellschaften tätig und hält ggf. einschlägige Zertifizierungen wie "Certified Internal Auditor (CIA)". Die korrespondierenden Kontrollen beim Subdienstleister sind erforderlich, um zusammen mit den Kontrollen des Cloud-Anbieters die anwendbaren C5 Kriterien mit hinreichender Sicherheit zu erfüllen. Anwendbare rechtliche und

regulatorische Anforderungen können z. B. in den Bereichen Datenschutz, Recht am geistigen Eigentum oder Urheberrecht bestehen.

Sofern gesetzliche oder regulatorische Anforderungen eine von diesen Kriterien abweichende Regelung zur Steuerung von Subdienstleistern vorsehen, bleiben diese Regelungen von den C5-Kriterien unberührt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Hinsichtlich des Vorhandenseins der Dokumentation ist eine kontinuierliche Prüfung nicht zielführend, da die dazugehörigen Prozesse und Schritte einmalig im Rahmen einer zyklischen Prüfung getestet werden können.

Eine kontinuierliche Prüfung, ob Veränderungen an den Richtlinien vorgenommen wurden, ist möglich, sofern diese Änderungen durch den Cloud-Anbieter auswertbar dokumentiert werden. Jedoch ist eine automatisierte Prüfung auf Sinnhaftigkeit der Änderungen nur schwer umzusetzen.

Bezogen auf den Nachweis, dass eine Kommunikation/Bereitstellung stattgefunden hat, ist eine kontinuierliche Prüfung durchaus denkbar.

Der Cloud-Anbieter müsste hierfür die Kenntnisnahme systembasiert gestalten (z. B. mithilfe von Tickets oder Vermerken im jeweiligen Dienstleister-Vertrag).

SSO-02 Risikobeurteilung der Dienstleister und Lieferanten

Basiskriterium

Dienstleister und Lieferanten des Cloud-Anbieters werden einer Risikobeurteilung gemäß den Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter unterzogen, bevor sie zur Bereitstellung des Cloud-Dienstes beitragen. Die Angemessenheit der Risikobeurteilung wird während des Leitungsbezugs regelmäßig, mindestens jährlich, durch qualifiziertes Personal des Cloud-Anbieters überprüft.

Die Risikobeurteilung umfasst die Identifikation, Analyse, Bewertung, Behandlung und Dokumentation von Risiken hinsichtlich der folgenden Aspekte:

- Schutzbedarf der Informationen hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, die durch den Dritten verarbeitet, gespeichert oder übertragen werden,
- Auswirkungen einer Schutzbedarfsverletzung auf die Bereitstellung des Cloud-Dienstes,
- Abhängigkeit des Cloud-Anbieters vom Dienstleister oder Lieferanten hinsichtlich Umfang, Komplexität und Einzigartigkeit der bezogenen Leistung, einschließlich der Betrachtung möglicher Alternativen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine kontinuierliche Prüfung der Risikobeurteilung erscheint nicht zielführend, da lediglich deren regelmäßige Durchführung, jedoch nicht deren Inhalte, automatisiert überprüft werden könnte.

Zudem ist die angegebene Frequenz von mindestens einem Jahr durch die zyklische Prüfung abgedeckt. Risikobeurteilungen werden selten dynamisch vorgenommen und ändern sich daher eher selten unterjährig.

SSO-03 Verzeichnis der Dienstleister und Lieferanten

Basiskriterium

Der Cloud-Anbieter registriert Dienstleister und Lieferanten, die Leistungen zur Bereitstellung des Cloud-Dienstes beitragen. Folgende Informationen sind nachzuhalten:

- Firmenname
- Anschrift
- Lokationen der Verarbeitung und Speicherung von Daten
- Verantwortlicher Ansprechpartner beim Dienstleister/Lieferanten
- Verantwortlicher Ansprechpartner beim Cloud-Anbieter
- Beschreibung der Leistung
- Klassifizierung auf Basis der Risikobeurteilung
- Beginn des Leistungsbezugs
- Nachweise über die Einhaltung der vertraglich vereinbarten Anforderungen.

Die Angaben im Verzeichnis werden mindestens jährlich auf Vollständigkeit, Richtigkeit und Gültigkeit überprüft.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Zur Erfüllung des Basiskriteriums ist es nicht notwendig, ein einziges zentrales Verzeichnis zu führen.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine ad-hoc-Vollständigkeitsprüfung auf die angegebenen Kriterien kann automatisiert stattfinden, ebenso ein Abgleich geänderter Daten mit einschlägigen Unternehmensdatenbanken. Dies kann der Cloud-Anbieter einrichten.

Der Prüfer kann dann in der zyklischen Prüfung Abweichungen untersuchen.

Jedoch erscheint aufgrund der Frequenz und der reinen Vollständigkeitsanalyse eine kontinuierliche Prüfung als recht aufwändig.

SSO-04 Überwachung der Einhaltung der Anforderungen

Basiskriterium

Der Cloud-Anbieter überwacht die Einhaltung der Anforderungen an die Informationssicherheit sowie der anwendbaren rechtlichen und regulatorischen Anforderungen gemäß den Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter.

Die Überwachung umfasst eine regelmäßige Durchsicht der folgenden Nachweise, soweit diese von den Dritten gemäß den vertraglichen Vereinbarungen zur Verfügung zu stellen sind:

- Berichte über die Qualität der Leistungserbringung,
- Zertifikate über die Konformität der Managementsysteme mit internationalen Standards,
- Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit ihres dienstleistungsbezogenen internen Kontrollsystems,
- Aufzeichnungen zum Umgang der Dritten mit Schwachstellen, Sicherheitsvorfällen und Störungen.

Die Regelmäßigkeit der Durchführung entspricht der Klassifizierung der Dritten auf Basis der Risikobeurteilung des Cloud-Anbieters (vgl. SSO-02). Die Ergebnisse der Überwachung fließen in die Überprüfung der Risikobeurteilung ein.

Identifizierte Verstöße und Abweichungen werden gemäß dem Verfahren zum Umgang mit Risiken (vgl. OIS-07) einer Analyse, Bewertung und Behandlung unterzogen.

Zusatzkriterium

Die Verfahren zur Überwachung der Einhaltung der Anforderungen werden durch automatische

Verfahren hinsichtlich der folgenden Aspekte ergänzt:

- Konfiguration von Systemkomponenten
- Leistung und Verfügbarkeit von Systemkomponenten
- Reaktionszeit bei Störungen und Sicherheitsvorfällen
- Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung).

Identifizierte Verstöße und Abweichungen werden automatisch an das dafür zuständigen Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.-

Ergänzende Informationen

Zum Kriterium

Nachweise hinsichtlich der Überprüfung der Angemessenheit und Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems durch unabhängige Dritte sind z. B. Berichte nach ISAE 3402, IDW PS 951, SOC 2 oder BSI C5.

Der Cloud-Anbieter überprüft in den von Dritten zur Verfügung gestellten Nachweisen bspw. folgende Aspekte und berücksichtigt die Erkenntnisse ggf. wieder in seiner Risikobeurteilung, um ggf. mitigierende Maßnahmen zu ergreifen:

- den Geltungsbereich und die Gültigkeit bzw. den abgedeckten Zeitraum des Nachweises,
- bei Prüfberichten: Einschränkungen der Opinion, enthaltene Abweichungen/sonst. Beobachtungen inkl. Management-Antwort sowie zu berücksichtigende korrespondierende Kontrollen, welche der Cloud-Anbieter selbst einzurichten und wirksam durchzuführen hat,
- offengelegte Subdienstleister inkl. Änderungen (z. B. neuer Subdienstleister),
- angegebene Sicherheitsvorfälle.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie sich über Subdienstleister ihres Cloud-Anbieters informieren (z. B. anhand der Angaben im C5-Prüfbericht) und anhand des Schutzbedarfs ihrer im Cloud-Dienst verarbeiteten und gespeicherten Daten entscheiden, ob weitergehende eigene Maßnahmen zur Überwachung und Überprüfung dieser Subdienstleister durchzuführen sind.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche Überprüfung einiger der geforderten Nachweise wie etwa der durchgeführten Reviews und deren Ergebnisse kann erfolgen, sobald die dazugehörigen Schritte mithilfe eines Tools beim Cloud-Anbieter dokumentiert werden.

Jedoch kann eine inhaltliche Überprüfung wie beispielsweise die Überprüfung der Reaktion auf Risikobeurteilungen und Verstöße gegen Dienstleister-Vorgaben nur schwerlich erfolgen, da hierzu ein semantisches Verständnis aufgebaut werden müsste. Daraus resultiert, dass zumindest Teile des Kriteriums für eine kontinuierliche Prüfung geeignet sind.

SSO-05 Ausstiegsstrategie für den Bezug von Leistungen

Basiskriterium

Der Cloud-Anbieter hat Ausstiegsstrategien für den Bezug von Leistungen definiert und dokumentiert, bei denen die Risikobeurteilung der Dienstleister und Lieferanten hinsichtlich Umfang, Komplexität und Einzigartigkeit der bezogenen Leistung, eine sehr hohe Abhängigkeit ergab (vgl. ergänzende Informationen).

Die Ausstiegsstrategien sind mit den Plänen zur betrieblichen Kontinuität abgestimmt und umfassen die folgenden Aspekte:

- Analyse der potenziellen Kosten, Auswirkungen, Ressourcen und zeitlichen Auswirkungen des Übergangs einer bezogenen Leistung auf einen alternativen Dienstleister oder Lieferanten,

- Definition und Zuweisung von Rollen, Verantwortlichkeiten und ausreichenden Ressourcen zur Durchführung der Aktivitäten für einen Übergang,
- Definition von Erfolgskriterien für den Übergang,
- Definition von Indikatoren für die Überwachung der Leistungserbringung, die bei inakzeptablen Ergebnissen den Ausstieg für den Bezug der Leistung einleiten sollten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Von einer sehr hohen Abhängigkeit ist insbesondere in folgenden Situationen auszugehen:

- die bezogene Leistung ist für die Bereitstellung des Cloud-Dienstes unabdingbar - liegt vor, wenn der Cloud-Anbieter:
  - den Cloud-Dienst aus Rechenzentren heraus bereitstellt, die von Dritten betrieben werden,
  - einen SaaS-Dienst bereitstellt und das IaaS oder PaaS eines anderen Cloud-Anbieters nutzt.
- Die Leistung kann nicht innerhalb eines Monats von einem alternativen Dienstleister oder Lieferanten bezogen werden, da sie:
  - am Markt einzigartig ist und kein anderer Anbieter lieferfähig ist;
  - vom Dienstleister oder Lieferanten und/ oder dem Cloud-Anbieter stark individualisiert wurde,
  - von keinem anderen Anbieter in der erforderlichen Dienstgüte geliefert werden kann,
  - spezifisches Wissen erfordert, das nur/überwiegend beim aktuellen Dienstleister oder Lieferanten und nicht beim Cloud-Anbieter vorliegt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: Nein

Das Vorhandensein individueller Ausstiegsstrategien ist kein praktikabler Prüfgegenstand für die kontinuierliche Prüfung.

6.13 Umgang mit Sicherheitsvorfällen (SIM)

Zielsetzung: *Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen.*

SIM-01 Richtlinie für den Umgang mit Sicherheitsvorfällen

Basiskriterium

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt, um eine schnelle, effektive und ordnungsgemäße Reaktion auf alle bekannten Sicherheitsvorfälle zu gewährleisten.

Der Cloud-Anbieter definiert Vorgaben zur Klassifizierung, Priorisierung und Eskalation von Sicherheitsvorfällen und schafft Schnittstellen zum Incident Management und zum Business Continuity Management.

Zusätzlich hat der Cloud-Anbieter ein "Computer Emergency Response Team" (CERT) eingerichtet, das zur koordinierten Lösung von konkreten Sicherheitsvorfällen beiträgt.

Von Sicherheitsvorfällen betroffene Kunden werden zeitnah und in angemessener Form darüber informiert.

Zusatzkriterium

Es gibt Anweisungen, wie bei einem Sicherheitsvorfall die Daten eines verdächtigen Systems beweisfest gesammelt werden können. Weiterhin existieren Analysepläne für typische Sicherheitsvorfälle sowie eine Auswertemethodik, so dass die gesammelten Informationen in einer eventuell späteren juristischen Würdigung ihre Beweiskraft nicht verlieren.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen des Cloud-Anbieters bezüglich sie betreffender Sicherheitsvorfälle erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine kontinuierliche Prüfung der dokumentierten Richtlinien und Anweisungen ist nicht zielführend, da diese sich eher selten ändern. Somit kann die Prüfung der Richtlinien und Anweisungen in der zyklischen Prüfung durchgeführt werden.

Ebenso ist die Einrichtung eines CERT nicht für eine kontinuierliche Prüfung geeignet, da es sich um eine organisatorische Einheit handelt, die nicht kontinuierlich geprüft werden muss.

Die zeitnahe Kommunikation von Sicherheitsvorfällen an betroffene Kunden kann durch einen kontinuierlichen Prüfungsansatz abgedeckt werden. Dazu kann der Cloud-Anbieter nicht nur die Sicherheitsvorfälle mittels Protokollen/Logs dokumentieren, sondern auch, dass diese dem Kunden beispielsweise via E-Mail kommuniziert wurden. Dass es zu jedem Sicherheitsvorfall eine Kommunikation an betroffene Kunden gab, kann somit durch den Prüfer automatisch und kontinuierlich ausgewertet werden.

Dieses Verfahren lässt sich mit dem Prüfungsansatz weiterführender Anforderungen des Security Incident Managements kombinieren.

SIM-02 Bearbeitung von Sicherheitsvorfällen

Basiskriterium

Qualifiziertes Personal des Cloud Anbieters führt, gegebenenfalls gemeinsam mit externen

Sicherheitsdienstleistern, für Ereignisse die einen Sicherheitsvorfall darstellen könnten, Klassifizierungen, Priorisierungen sowie Ursachenanalysen durch.

Zusatzkriterium

Der Cloud-Anbieter simuliert das Identifizieren, Analysieren und Abwehren von Sicherheitsvorfällen und Angriffen mindestens jährlich durch geeignete Tests und Übungen (z. B. Red Team-Übungen).

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Cloud-Anbieter dokumentiert alle Sicherheitsvorfälle in digitaler Form, die Informationen über die Klassifizierung, Priorisierung und Ursachenanalyse enthält. Die Ursachenanalyse sollte standardisiert erfolgen, um eine kontinuierliche Prüfung zu erleichtern.

Eine automatische und kontinuierliche Auswertung der Sicherheitsvorfälle kann anschließend durch den Prüfer vorgenommen werden, indem er die angefertigten Logs oder Tickets ausliest und testet, ob der Sicherheitsvorfall klassifiziert und priorisiert wurde und ob eine standardisierte Ursachenanalyse erfolgt ist. Die kontinuierliche Prüfung liefert somit eine Aussage darüber, ob Sicherheitsvorfälle korrekt erfasst, klassifiziert und einer Ursachenanalyse unterzogen werden.

SIM-03 Dokumentation und Berichterstattung über Sicherheitsvorfälle

Basiskriterium

Nach Verarbeitung eines Sicherheitsvorfalls wird die Lösung gemäß den vertraglichen Vereinbarungen dokumentiert und der Bericht zur abschließenden Kenntnisnahme oder ggf. als Bestätigung an betroffene Kunden übermittelt.

Zusatzkriterium

Der Kunde kann Lösungen entweder aktiv zustimmen oder der Lösung wird nach Ablauf eines bestimmten Zeitraumes automatisch zugestimmt.

Informationen zu Sicherheitsvorfällen oder bestätigten Sicherheitsverstößen werden allen betroffenen Kunden zur Verfügung gestellt.

Zwischen Cloud-Anbieter und Cloud-Kunden ist vertraglich geregelt, welche Daten dem Cloud-Kunden bei Sicherheitsvorfällen zur eigenen Analyse zur Verfügung gestellt werden.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen des Cloud-Anbieters bezüglich sie betreffender Sicherheitsvorfälle sowie deren Lösung erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

In den angefertigten Protokollen oder Tickets, die die Sicherheitsvorfälle dokumentieren (vergleiche SIM-03), beschreibt der Cloud-Anbieter zusätzlich den verfolgten Lösungsweg zur Beseitigung des Vorfalls. Des Weiteren wird vom Cloud-Anbieter auch die Kommunikation an den Kunden dokumentiert.

Der Prüfer kann automatisch und kontinuierlich auslesen, ob die dokumentierten Sicherheitsvorfälle gelöst wurden und ob ein Lösungsweg dokumentiert ist. Gleiches gilt für die Kommunikation der Vorfälle an betroffene Kunden. Falls dem nicht so ist, kann als Ausgabewert der kontinuierlichen Prüfung der

nicht gelöste Sicherheitsvorfall dokumentiert werden.

SIM-04 Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle

Basiskriterium

Der Cloud-Anbieter informiert Mitarbeiter und externe Geschäftspartner über ihre Verpflichtungen. Falls erforderlich willigen sie dazu ein oder verpflichten sich vertraglich dazu, alle Sicherheitsereignisse, die ihnen bekannt werden und direkt mit dem vom Cloud-Anbieter bereitgestellten Cloud-Dienst in Verbindung stehen, zeitnah an eine zuvor benannte zentrale Stelle des Cloud-Anbieters zu melden.

Der Cloud-Anbieter kommuniziert, dass "Falschmeldungen" von Ereignissen, die sich im Nachhinein nicht als Vorfälle herausstellen, keine negativen Folgen nach sich ziehen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass identifizierte Sicherheitsereignisse, deren Bearbeitung im Verantwortungsbereich des Cloud-Anbieters liegt, zeitnah an eine zuvor benannte zentrale Stelle gemeldet werden. Die Identifikation solche Sicherheitsereignisse wird durch geeignete Kontrollen unterstützt (vgl. korrespondierendes Kriterium zu OPS-10).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Der Cloud-Anbieter sollte seine Mitarbeiter sowie externe Geschäftspartner in einem standardisierten und digitalen Format über ihre Verpflichtungen informieren. Dies geschieht üblicherweise bei Eintritt in das Unternehmen beziehungsweise in die Geschäftsbeziehung.

Somit kann der Prüfer automatisch und kontinuierlich überprüfen, ob allen Mitarbeitern und externen Geschäftspartnern ihre Verpflichtungen kommuniziert werden, indem automatisch bei Vertragsschluss getestet wird, ob eine entsprechende Klausel im Vertrag enthalten ist.

SIM-05 Auswertung und Lernprozess

Basiskriterium

Mechanismen sind vorhanden, um Art und Umfang der Sicherheitsvorfälle messen und überwachen sowie wie an unterstützende Stellen melden zu können. Die aus der Auswertung gewonnenen Informationen werden dazu verwendet, wiederkehrende oder mit erheblichen Folgen verbundene Vorfälle zu identifizieren und Notwendigkeiten für erweiterte Schutzmaßnahmen festzustellen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Unterstützende Stellen können externe Dienstleister oder staatliche Stellen wie z. B. das BSI sein.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Erkenntnisse aus vergangenen Sicherheitsvorfällen, die Ihnen mitgeteilt wurden, und die daraus resultierenden Maßnahmen des Cloud-Anbieters in Ihr ISMS aufnehmen und bewerten, ob und wenn ja welche Maßnahmen sie auf ihrer Seite unterstützend ergreifen können.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die vorhandenen Mechanismen zur Messung von Art und Umfang der Sicherheitsvorfälle werden nur selten verändert. Daraus resultiert, dass eine

kontinuierliche Prüfung nicht zielführend ist. Zudem kann es sich in einigen Fällen um eine manuelle, durch Mitarbeiter ausgeführte Tätigkeit darstellen, wiederkehrende oder mit erheblichen Folgen verbundene Vorfälle zu identifizieren und zugehörige Schutzmaßnahmen zu entwickeln.

6.14 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)

Zielsetzung: *Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.*

BCM-01 Verantwortung durch die Unternehmensleitung

Basiskriterium

Die oberste Leitung des Cloud-Anbieters ist als Prozesseigentümer des Kontinuitäts- und Notfallmanagements benannt und trägt die Verantwortung für die Etablierung des Prozesses im Unternehmen und die Einhaltung der Leitlinien. Sie muss dafür sorgen, dass ausreichende Ressourcen für einen effektiven Prozess bereitgestellt werden.

Personen in der Unternehmensleitung und anderen relevanten Führungspositionen demonstrieren Führung und Engagement in Bezug auf dieses Thema, indem sie beispielsweise die Mitarbeiter dazu auffordern beziehungsweise ermutigen, zu der Effektivität des Kontinuitäts- und Notfallmanagements aktiv beizutragen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die Verantwortlichkeiten für Prozesse des Kontinuitäts- und Notfallmanagements werden initial benannt und anschließend nur selten verändert. Somit ist eine kontinuierliche Prüfung hier nicht zielführend.

Eine kontinuierliche Prüfung kann jedoch das Datum der letzten Revision der Leitlinien für das Kontinuitäts- und Notfallmanagement zurückgeben.

BCM-02 Richtlinien und Verfahren zur Business Impact Analyse

Basiskriterium

Richtlinien und Anweisungen zum Ermitteln von Auswirkungen etwaiger Störungen des Cloud-Dienstes oder des Unternehmens sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt.

Mindestens die folgenden Aspekte werden dabei berücksichtigt:

- mögliche Szenarien basierend auf einer Risikoanalyse,
- Identifizierung kritischer Produkte und Dienstleistungen,
- Identifizierung von Abhängigkeiten, einschließlich der Prozesse (inkl. dafür benötigter Ressourcen), Anwendungen, Geschäftspartner und Dritter,
- Erfassung von Bedrohungen gegenüber kritischen Produkten und Dienstleistungen,
- Ermittlung von Auswirkungen resultierend aus geplanten und ungeplanten Störungen und die Veränderung im Laufe der Zeit,
- Feststellung der maximal vertretbaren Dauer von Störungen,
- Feststellung der Prioritäten zur Wiederherstellung,
- Feststellung zeitlicher Zielvorgaben zur Wiederaufnahme kritischer Produkte und Dienstleistungen innerhalb des maximal vertretbaren Zeitraums (RTO),
- Feststellung zeitlicher Vorgaben zum maximal vertretbaren Zeitraum, in dem Daten verloren und nicht wiederhergestellt werden können (RPO),
- Abschätzung der zur Wiederaufnahme benötigten Ressourcen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Zu berücksichtigende Szenarien gemäß des Basiskriteriums sind beispielsweise der Ausfall von Personal, Gebäude, Infrastruktur und Dienstleistern.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Szenarien für einen Ausfall des Cloud-Dienstes bzw. des Cloud-Anbieters im Rahmen ihrer Business Impact Analyse hinreichend berücksichtigt werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Richtlinie kann sich zwar ad-hock verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

BCM-03 Planung der Betriebskontinuität

Basiskriterium

Basierend auf der Business Impact Analyse wird ein einheitliches Rahmenwerk zur Planung der betrieblichen Kontinuität und des Geschäftsplans eingeführt, dokumentiert und angewendet, um sicherzustellen, dass alle Pläne konsistent sind. Die Planung richtet sich nach etablierten Standards, was in einem "Statement of Applicability" nachvollziehbar festgeschrieben ist.

Pläne zur betrieblichen Kontinuität und Notfallpläne berücksichtigen dabei folgende Aspekte:

- Definierter Zweck und Umfang unter Beachtung der relevanten Abhängigkeiten,
- Zugänglichkeit und Verständlichkeit der Pläne für Personen, die danach handeln sollen,
- Eigentümerschaft durch mindestens eine benannte Person, die für die Überprüfung, Aktualisierung und Genehmigung zuständig ist,
- Festgelegte Kommunikationswege, Rollen und Verantwortlichkeiten einschließlich Benachrichtigung des Kunden,
- Wiederherstellungsverfahren, manuelle Übergangslösungen und Referenzinformationen (unter Berücksichtigung der Priorisierung bei der Wiederherstellung von Cloud-Infrastruktur Komponenten und Diensten sowie Ausrichtung an Kunden),
- Methoden zur Inkraftsetzung der Pläne;
- Kontinuierlicher Verbesserungsprozess der Pläne,
- Schnittstellen zum Security Incident Management.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die Konsistenz von Plänen gemäß des Basiskriteriums gilt es auch bei Nutzung verschiedenen Standorte einzuhalten.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass bei der Planung der betrieblichen Kontinuität und des Geschäftsplans, die Ergebnisse der Business Impact Analyse hinreichend berücksichtigt werden, um für die Auswirkungen eines Ausfalls des Cloud-Dienstes bzw. des Cloud-Anbieters vorzusorgen.

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Verfügbarkeit des Cloud-Dienstes, seine Wiederherstellungszeit gemäß BCM-Plan sowie des Datenverlusts des Cloud-Dienstes mit ihren eigenen Verfügbarkeitsanforderungen und tolerierbarem Datenverlust im Einklang ist.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Bei der Einführung des Rahmenwerks sowie des Geschäftsplans anhand einer Business Impact-Analyse handelt es sich um einen manuellen Prozess des Cloud-Anbieters.

Eine kontinuierliche Prüfung ist hier nur bedingt zielführend. Die Pläne können im Rahmen der zyklischen Prüfung getestet werden.

BCM-04 Verifizierung, Aktualisierung und Test der Betriebskontinuität

Basiskriterium

Die Business Impact Analyse sowie die Pläne zur betrieblichen Kontinuität und Notfallpläne werden regelmäßig (mindestens jährlich) oder nach wesentlichen organisatorischen oder umgebungsbedingten Veränderungen überprüft, aktualisiert und getestet. Tests beziehen betroffene Kunden (Tenants) und relevante Dritte mit ein. Die Tests werden dokumentiert und Ergebnisse werden für zukünftige Maßnahmen der betrieblichen Kontinuität berücksichtigt.

Zusatzkriterium

Zusätzlich zu den Tests werden auch Übungen durchgeführt, die u.a. Szenarien aus in der Vergangenheit bereits aufgetretenen Sicherheitsvorfällen hervorgegangen sind.

Ergänzende Informationen

Zum Kriterium

Tests finden in erster Linie auf operativer Ebene statt und richten sich an operative Zielgruppen. Dazu gehören z. B.:

- Test der technischen Vorsorgemaßnahmen
- Funktionstests
- Plan-Review

Übungen finden zusätzlich auf taktischer und strategischer Ebene statt. Dazu gehören

z. B.:

- Planbesprechung
- Stabsübung
- Stabsrahmenübung
- Kommunikations- und Alarmierungsübung
- Simulation von Szenarien
- Ernstfall- oder Vollübung.

Im Anschluss an eine durchgeführte Übung:

- Überprüfung und eventuelle Anpassung des vorhandenen Alarmierungsplanes.

Relevante Dritte sind insbesondere Dienstleister und Lieferanten des Cloud-Anbieters, die zur Bereitstellung des Cloud-Dienstes beitragen (vgl. auch Basiskriterien SSO-02 und SSO-05).

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Maßnahmen zur Vorsorge der Auswirkungen eines Ausfalls des Cloud-Dienstes bzw. des Cloud-Anbieters regelmäßig überprüft, aktualisiert, getestet und geübt werden. Der Cloud-Anbieter wird gemäß den vertraglichen Vereinbarungen in die Tests und Übungen eingebunden.

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Ergebnisse der BCM-Tests und Übungen des Cloud-Anbieters in das eigene BCM einfließen und hinsichtlich der Sicherstellung der betrieblichen Kontinuität des Kunden umfassend gewürdigt werden.

Bei Tests und Übungen, die den Kunden mit einbeziehen und daher eigene Maßnahmen auf Kundenseite bedingen, stellen Cloud-Kunden durch geeignete Kontrollen aus ihrem BCM sicher, dass die entsprechenden Maßnahmen zur Bewältigung gemäß Szenario geübt und getestet werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Umsetzung der Tests der Pläne zur betrieblichen Kontinuität in einem jährlichen Zyklus lässt eine kontinuierliche Prüfung über das gesamte Kriterium hinweg nicht zielführend erscheinen. Der Aufwand für Cloud-Anbieter und Prüfer, diesen Prozess automatisiert und kontinuierlich zu testen, wäre wahrscheinlich höher als der erwartete Nutzen.

Jedoch kann kontinuierlich überprüft werden, ob ein Test in der definierten Zeitspanne

durchgeführt wurde. Dazu muss der Cloud-Anbieter standardisiert dokumentieren, dass und wann ein Test durchgeführt wurde. Eine kontinuierliche Prüfung ist somit teilweise möglich.

6.15 Compliance (COM)

Zielsetzung: *Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung.*

COM-01 Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen

Basiskriterium

Die für die Informationssicherheit des Cloud-Dienstes relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen sowie die Verfahren des Cloud-Anbieters zur Einhaltung dieser Anforderungen sind ausdrücklich definiert und dokumentiert.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die Dokumentation des Cloud-Anbieters kann u.a. auf die folgenden Anforderungen Bezug nehmen:

- Anforderungen zum Schutz personenbezogener Daten (z. B. EU Datenschutz-Grundverordnung),
- Compliance-Anforderungen aufgrund vertraglicher Verpflichtungen mit Cloud-Kunden (z. B. ISO/IEC 27001, SOC 2, PCI-DSS),
- allgemein anerkannte Buchführungsgrundsätze (z. B. gemäß HGB oder IFRS),
- Anforderungen bzgl. des Datenzugriffs und der Prüfbarkeit digitaler Unterlagen (z. B. gemäß GDPdU),
- Sonstige Gesetzte (z. B. gemäß BSIG oder AktG).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Eine kontinuierliche Prüfung von Vertragsvorgaben und Regularien sowie deren Dokumentation erscheint nicht zielführend. Hier reicht der Test im Rahmen der zyklischen Prüfung aus.

Eine kontinuierliche Prüfung könnte dahingehend unterstützen, dass das Datum der letzten Prüfung des Kriteriums ausgegeben wird.

COM-02 Richtlinie für die Planung und Durchführung von Audits

Basiskriterium

Richtlinien und Anweisungen mit Vorgaben für die Planung und Durchführung von Audits sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und adressieren folgende Aspekte:

- Beschränkung auf Lesezugriff für Systemkomponenten gemäß der vereinbarten Prüfungsplanung und wie es für die Durchführung der Aktivitäten notwendig ist,
- Aktivitäten, die zu Störungen des Cloud-Dienstes oder Verstößen gegen vertragliche Anforderungen führen können, werden während der planmäßigen Wartungsfester oder außerhalb der Zeiten von Lastspitzen durchgeführt,
- Protokollierung und Überwachung der Aktivitäten.

Zusatzkriterium

Der Cloud-Anbieter gewährt seinen Cloud-Kunden vertraglich zugesicherte Informations- und Prüfrechte.

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass auf Störungen des Cloud-Dienstes durch solche Audits angemessen reagiert wird.

Soweit vertraglich zugesicherte Informations- und Prüfrechte vorliegen, stellen Cloud-Kunden durch geeignete Kontrollen sicher, dass diese Rechte gemäß eigenen Anforderungen ausgestaltet und wahrgenommen werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Eine Leitlinie kann sich zwar ad-hoc verändern, jedoch ist eine kontinuierliche Prüfung nur in dem Sinne zielführend, dass diese Prüfung das Datum der letzten Veränderung zurückgibt, indem der Cloud-Anbieter dies automatisch im System hinterlegt. Plausibilität oder Sinnhaftigkeit des Inhalts einer Leitlinie kann derzeit kaum automatisiert und kontinuierlich geprüft werden.

COM-03 Interne Audits des Informationssicherheitsmanagementsystems

Basiskriterium

Qualifiziertes Personal überprüft in regelmäßigen Abständen, mindestens jährlich, in internen Audits die Compliance des Informationssicherheitsmanagementsystems mit den relevanten und anwendbaren gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen (vgl. COM-01) sowie die Einhaltung der Richtlinien und Arbeitsanweisungen (vgl. SP-01) in dessen Geltungsbereich (vgl. OIS-01).

Identifizierte Schwachstellen und Abweichungen werden gemäß dem Verfahren zum Umgang mit Risiken (vgl. OIS-06) einer Risikobeurteilung unterzogen und Maßnahmen zur Behandlung definiert und nachverfolgt (vgl. OPS-18).

Zusatzkriterium

Interne Audits werden durch Verfahren zur automatischen Überwachung anwendbarer Vorgaben aus Richtlinien und Arbeitsanweisungen hinsichtlich der folgenden Aspekte ergänzt:

- Konfiguration von Systemkomponenten zur Bereitstellung des Cloud-Dienstes im Verantwortungsbereich des Cloud-Anbieters,
- Leistung und Verfügbarkeit dieser Systemkomponenten,
- Reaktionszeit bei Störungen und Sicherheitsvorfällen,
- Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung).

Identifizierte Schwachstellen und Abweichungen werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.

Die Einhaltung ausgewählter vertraglicher Anforderungen kann durch die Cloud-Kunden in Echtzeit eingesehen werden.

Ergänzende Informationen

Zum Kriterium

Qualifiziertes Personal ist z. B. in der Internen Revision des Cloud-Anbieters oder bei vom Cloud-Anbieter beauftragten Sachverständigen Dritten wie z. B. Wirtschaftsprüfungsgesellschaften tätig und hält ggf. einschlägige Zertifizierungen wie "Certified Internal Auditor (CIA)".

Bezüglich Compliance des ISMS vgl. Abschnitt 9.3 von ISO/IEC 27001.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die regelmäßige Durchführung einer internen Prüfung des ISMS kann als Teil eines Compliance Monitorings aufgesetzt werden. Hierzu müssen die Ergebnisse der internen Prüfung digital dokumentiert werden, ebenso die einzelnen Prüfschritte.

Eine kontinuierliche Prüfung dieser internen Prüfung erscheint derzeit nicht praktikabel, sondern kann erst nach dem Aufsetzen eines Compliance-Monitorings angedacht werden.

Die kontinuierliche Prüfung kann dann das Datum der jeweiligen letzten Prüfung als Ausgabewert liefern.

COM-04 Informationen über die Informationssicherheitsleistung und Managementbewertung des ISMS

Basiskriterium

Die oberste Leitung des Cloud-Anbieters wird in regelmäßigen Abständen über die Informationssicherheitsleistung im Anwendungsbereich des ISMS informiert, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.

Die Informationen fließen mindestens jährlich in die Managementbewertung des ISMS ein.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Die oberste Leitung ist eine natürliche Person oder Personengruppe, welche letztgültige Entscheidungen für die Institution trifft und hierfür die Verantwortung trägt. Bezüglich Managementbewertung des ISMS vgl. Abschnitt 9.3 von ISO/IEC 27001.

Die im Rahmen der Managementbewertung des ISMS zu behandelnden Aspekte sind im Abschnitt 9.3 von ISO/IEC 27001 aufgeführt.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die eigentliche Übermittlung der Informationen an das Management des Cloud-Anbieters kann durchaus protokolliert und dementsprechend automatisiert sowie kontinuierlich überprüft werden. Jedoch sind die Inhalte der Kommunikation sowie der Nachweis, dass diese auch vom Management bewertet und verarbeitet wurden, nach wie vor im Rahmen der Regelprüfung zu prüfen.

6.16 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)

Zielsetzung: *Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten.*

INQ-01 Juristische Beurteilung von Ermittlungsanfragen

Basiskriterium

Ermittlungsanfragen staatlicher Stellen werden einer juristischen Beurteilung durch qualifiziertes Personal des Cloud-Anbieters unterzogen.

Im Rahmen der Beurteilung wird festgestellt, ob sich die staatliche Stelle auf eine anwendbare sowie rechtsgültige Rechtsgrundlage stützt und welche weiteren Schritte einzuleiten sind.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass Art und Umfang staatlicher Ermittlungsanfragen und der damit einhergehenden Offenlegung eigener Daten, im eigenen Risikomanagement behandelt wurde und die Nutzung des Cloud-Dienstes erst stattfindet, wenn dieses Risiko als tragbar erachtet wurde.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Obwohl eine kontinuierliche Prüfung der Durchführung der Beurteilung sowie derer Dokumentation denkbar ist, erscheint dies wenig praktikabel. Vielmehr zielt das Kriterium auf die Qualifikation des prüfenden Personals sowie den dahinterliegenden Prozess ab, welche einer manuellen Prüfung unterliegen.

INQ-02 Information der Cloud-Kunden über Ermittlungsanfragen

Basiskriterium

Der Cloud-Anbieter informiert den oder die betroffenen Cloud-Kunden nach Eingang einer Ermittlungsanfrage einer staatlichen Stelle unverzüglich, soweit die anwendbare Rechtsgrundlage, auf die sich die staatliche Stelle stützt, dies nicht untersagt oder eindeutige Hinweise auf rechtswidrige Handlungen im Zusammenhang mit der Nutzung des Cloud-Dienstes vorliegen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Hiervon unberührt bleiben andere gesetzliche oder regulatorische Vorgaben, die eine frühzeitigere Information des Cloud-Kunden fordern.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass derartige Meldungen entgegengenommen und gemäß eigenen Vorgaben und Möglichkeiten rechtlich geprüft werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Zur internen Prozessüberwachung beim Cloud-Anbieter und Erleichterung der Prüfung ist eine kontinuierliche Prüfung des Zeitraums zwischen Eingang der Anfrage und Information der Kunden denkbar.

Da dies aber abhängig von lokalen Rechtsgrundlagen ist, kann der Aufwand, dies in den jeweiligen Regionen zu etablieren, recht hoch sein.

Sofern ein Vorgangsbearbeitungssystem beim Cloud-Anbieter implementiert ist, kann zumindest der Prozess in diesem System kontinuierlich geprüft werden.

INQ-03 Voraussetzungen für den Zugriff auf oder der Offenlegung von Daten bei Ermittlungsanfragen

Basiskriterium

Der Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen erfolgt nur unter der Voraussetzung, dass die juristische Beurteilung des Cloud-Anbieters ergab, dass eine anwendbare und rechtsgültige Rechtsgrundlage vorliegt und der Ermittlungsanfrage auf dieser Grundlage stattgegeben werden muss.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Sofern für den Ermittler eine eigene Rolle vergeben wird, um Zugriff auf die Daten zu erhalten, können die in der Anforderung genannten Voraussetzungen systemseitig erfasst und überprüft sowie an die Vergabe der Ermittler-Rolle geknüpft werden.

Hierauf kann eine kontinuierliche Abfrage erfolgen, dass die Rolle nur unter Vorliegen der systemseitig hinterlegten Voraussetzungen gewährt wurde. Abweichungen können gezielt manuell geprüft werden.

INQ-04 Begrenzung des Zugriffs auf oder der Offenlegung von Daten bei Ermittlungsanfragen

Basiskriterium

Die Verfahren des Cloud-Anbieters für das Einrichten des Zugriffs auf oder das Offenlegen von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen gewährleisten, dass diese nur Zugriff auf oder Einsicht in diejenigen Daten erhalten, die Gegenstand der Ermittlungsanfrage sind.

Soweit keine klare Eingrenzung der Daten möglich ist, anonymisiert oder pseudonymisiert der Cloud-Anbieter die Daten, so dass staatliche Stellen diese nur solchen Cloud-Kunden zuordnen können, die Gegenstand der Ermittlungsanfrage sind.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Es ist eine eigene Rolle für den Ermittler vorzusehen (s. auch INQ3). Hierbei ist denkbar, bestimmte Datentypen für diese Rolle nicht sichtbar, pseudonymisiert oder anonymisiert darzustellen, bzw. Daten der Kunden, die nicht Teil der Ermittlung sind, auszuschließen.

Dies erfordert einen manuellen Aufwand bei der Konfiguration und Vergabe der Ermittler-Rolle.

Unter dieser Voraussetzung ist dann aber eine kontinuierliche Prüfung, ob und inwiefern der Ermittler Zugriff auf Daten hatte, denkbar.

6.17 Produktsicherheit (PSS)

Zielsetzung: *Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.*

PSS-01 Leitlinien und Empfehlungen für Cloud-Kunden

Basiskriterium

Der Cloud-Anbieter macht Cloud-Kunden Leitlinien und Empfehlungen für die sichere Nutzung des bereitgestellten Cloud-Dienstes zugänglich. Die darin enthaltenen Informationen sind geeignet, die Cloud-Kunden bei der sicheren Konfiguration, Installation und Nutzung des Cloud-Dienstes zu unterstützen, soweit dies für den Cloud-Dienst anwendbar ist und im Verantwortungsbereich der Cloud-Kunden liegt.

Art und Umfang der bereitgestellten Informationen orientieren sich am Bedarf sachverständigen Personals der Cloud-Kunden, die Vorgaben zur Informationssicherheit machen, diese umsetzen oder die Umsetzung überprüfen (z. B. IT, Compliance, Interne Revision). Die Informationen in den Leitlinien und Empfehlungen für die sichere Nutzung des bereitgestellten Cloud-Dienstes adressieren insbesondere die folgenden Aspekte, soweit diese für den Cloud-Dienst anwendbar sind:

- Anleitungen bezüglich der sicheren Konfiguration
- Informationsquellen zu bekannten Schwachstellen und Aktualisierungsmechanismen
- Fehlerbehandlungs- und Protokollierungsmechanismen
- Authentisierungsmechanismen;
- Rollen- und Rechtekonzept, inkl. risikobehafteter Kombinationen
- Dienste und Funktionen zur Administration des Cloud-Dienstes durch privilegierte Benutzer.

Die Informationen werden so gepflegt, dass sie für den bereitgestellten Cloud-Dienst in der für die produktive Nutzung vorgesehenen Version anwendbar sind.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass aus den Informationen des Cloud-Anbieters Richtlinien, Konzepte und Maßnahmen zur angemessen sicheren Konfiguration und Nutzung (gemäß eigener Risikobewertung) des Cloud-Dienstes abgeleitet und eingehalten werden. Änderungen in den Informationen werden zeitnah auf ihre Auswirkung in diesen Dokumenten hin bewertet und ggf. notwendige Änderungen umgesetzt.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Bereitstellung von Informationen des Cloud-Anbieters für Cloud-Kunden ist nur bedingt kontinuierlich prüfbar. Der Cloud-Anbieter kann beispielsweise die Leitlinien und Empfehlungen über sein internes Kundenportal zur Verfügung stellen, was eine kontinuierliche Prüfung nur bedingt zielführend erscheinen lässt.

Hier ist lediglich eine Prüfung auf Vollständigkeit und letztes Änderungsdatum denkbar, wobei jedoch eine inhaltliche Prüfung der Änderungen derzeit nicht praktikabel erscheint. Hierzu wären semantische Auswertungen notwendig.

PSS-02 Identifikation von Schwachstellen des Cloud-Dienstes

Basiskriterium

Der Cloud-Anbieter überprüft den Cloud-Dienst durch geeignete Verfahren auf Schwachstellen,

die durch den Softwareentwicklungsprozess in den Cloud-Dienst einfließen können.

Die Verfahren zur Identifikation solcher Schwachstellen sind Bestandteil des Softwareentwicklungsprozesses und umfassen, je nach Risikobewertung, die folgenden Aktivitäten:

- Statische Code-Analyse
- Dynamische Code-Analysen
- Code Reviews durch qualifiziertes Personal des Cloud-Anbieters
- Einholen von Information über bestätigte Schwachstellen in Software-Bibliotheken, die von Dritten bereitgestellt und im eigenen Cloud-Dienst genutzten werden.

Der Schweregrad identifizierter Schwachstellen wird nach definierten Kriterien beurteilt und Maßnahmen zur zeitnahen Behebung oder Mitigation eingeleitet.

Zusatzkriterium

Die Verfahren zur Identifikation solcher Schwachstellen umfassen darüber hinaus jährliche Code Reviews oder Security Penetration-Tests durch qualifizierte externe Dritte.

Ergänzende Informationen

Zum Kriterium

Bekannte Schwachstellen in fremdbezogenen Systemkomponenten (z. B. Betriebssysteme), die für die Entwicklung und Bereitstellung des Cloud-Dienstes verwendet werden, aber nicht den Softwareentwicklungsprozess des Cloud-Anbieters durchlaufen, sind Gegenstand des Kriterium OPS-23 (Umgang mit Schwachstellen, Störungen und Fehlern - Prüfung offener Schwachstellen).

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Der Cloud-Anbieter überprüft seine Cloud-Dienste automatisiert auf Schwachstellen. Diese Überprüfung wird in standardisierter, digitaler Form dokumentiert.

Anschließend kann der Prüfer in der digitalen Dokumentation prüfen, inwiefern der Cloud-Anbieter eine Überprüfung auf Schwachstellen durchgeführt hat. Zudem kann der Schweregrad ggf. identifizierter Schwachstellen in diese kontinuierliche Prüfung integriert werden, sofern die definierten Kriterien und deren Anwendung standardisiert und maschinenlesbar erfolgen.

Die Information zu identifizierten und/oder behobenen Schwachstellen kann zudem direkt den betroffenen Kunden übergeben und damit eine erhöhte Transparenz erzielt werden.

PSS-03 Online-Register bekannter Schwachstellen

Basiskriterium

Der Cloud-Anbieter betreibt oder verweist auf ein tagesaktuell gepflegtes Online-Register bekannter Schwachstellen, die den bereitgestellten Cloud-Dienst sowie vom Cloud-Anbieter bereitgestellte Assets betreffen, die Cloud-Kunden in ihrem Verantwortungsbereich selbst installieren, bereitstellen oder betreiben müssen.

Die Darstellung der Schwachstellen folgt dem Common Vulnerability Scoring System (CVSS). Das Online-Register ist für jeden Cloud-Kunden leicht einsehbar. Die enthaltenen Informationen bilden eine geeignete Grundlage für die Risikobeurteilung und etwaige Folgemaßnahmen auf Seiten der Cloud-Kunden.

Zu jeder Schwachstelle ist angegeben, ob für diese entsprechend Software-Aktualisierungen (z. B. Patch, Update) verfügbar sind, bis wann diese ausgerollt werden und ob dies durch den Cloud-Anbieter, den Cloud-Kunden oder beide gemeinsam erfolgt.

Zusatzkriterium

Vom Cloud-Anbieter bereitgestellte Assets, die Cloud-Kunden in ihrem Verantwortungsbereich selbst installieren, bereitstellen oder betreiben müssen, sind mit automatischen Aktualisierungsmechanismen ausgestattet. Nach einer Freigabe durch den jeweiligen Cloud-Kunden, können Softwareaktualisierungen darüber so ausgerollt werden, dass eine

Verteilung an alle betroffenen Benutzer ohne menschliche Interaktion möglich ist.

Ergänzende Informationen

Zum Kriterium

Vom Cloud-Anbieter bereitgestellte Assets, welche Cloud-Kunden in ihrem Verantwortungsbereich selbst installieren, bereitstellen oder betreiben müssen sind z. B. lokale Software Clients und Apps sowie Werkzeuge zur Integration des Cloud-Dienstes.

Falls der Cloud-Dienst auf andere Cloud-Dienste zurückgreift, so muss dieses Register auch die Schwachstellen dieser anderen Cloud-Dienste aufnehmen oder auf sie verweisen, damit dieses Kriterium erfüllt ist.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Informationen dieses Registers gemäß eigenen Anforderungen hinreichend schnell in das eigene Risikomanagement aufgenommen, bewertet und ggf. eigene Maßnahmen im eigenen Verantwortungsbereich ergriffen werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Prüfung prüft vor allem, ob die Informationen tagesaktuell erneuert werden. Die Verbreitung von Softwareaktualisierungen muss durch den Cloud-Anbieter dokumentiert werden (Protokolle). Diese Dokumentation kann anschließend durch den Prüfer automatisiert und kontinuierlich ausgewertet werden, um sicherzustellen, dass die auf Assets im Verantwortungsbereich der Cloud-Kunden eingesetzte Software stets die aktuell ist.

PSS-04 Fehlerbehandlungs- und Protokollierungsmechanismen

Basiskriterium

Der bereitgestellte Cloud-Dienst ist mit Fehlerbehandlungs- und Protokollierungsmechanismen ausgestattet. Mittels dieser können Cloud-Kunden sicherheitsrelevante Informationen über den Sicherheitsstatus Cloud-Dienstens sowie die von ihm bereitgestellten Daten, Dienste oder Funktionen abrufen.

Die Informationen sind so detailliert, dass Cloud-Kunden folgende Aspekte überprüfen können, soweit diese für den Cloud-Dienst anwendbar sind:

- auf welche Daten, Dienste oder Funktionen, die dem Cloud-Kunden im Cloud-Dienst zur Verfügung stehen, wann und von wem zugegriffen wurde (Protokoll/Audit Logs),
- Störungen beim Verarbeiten von automatischen oder manuellen Aktionen,
- Änderungen sicherheitsrelevanter Parameter der Konfiguration, der Fehlerbehandlungs- und Protokollierungsmechanismen, der Authentifizierung von Benutzern, der Autorisierung von Aktionen, der Kryptographie und der Kommunikationssicherheit.

Die protokollierten Informationen sind vor unautorisierten Zugriffen sowie Veränderungen geschützt und können vom Cloud-Kunden gelöscht werden.

Falls der Cloud-Kunde für die Aktivierung oder Art und Umfang der Protokollierung zuständig ist, stellt der Cloud-Anbieter geeignete Protokollierungsfunktionen bereit.

Zusatzkriterium

Cloud-Kunden können die sicherheitsrelevanten Informationen über dokumentierte Schnittstellen abrufen, die geeignet sind, diese Informationen im Rahmen ihres Security Information and Event Management (SIEM) weiter zu verarbeiten.

Ergänzende Informationen

Zum Kriterium

Bei einem SaaS-Dienst für den sicheren Datenaustausch wäre unter den Begriffen Daten, Dienste oder Funktionen beispielsweise die Protokollierung aller lesenden oder schreibenden Zugriffe auf die abgelegten Dateien sowie deren Metadaten zu verstehen.

Korrespondierende Kriterien für Kunden

Sofern der Cloud-Dienst mit Fehlerbehandlungs- und Protokollierungsmechanismen ausgestattet ist, müssen Cloud-Kunden diese aktivieren und gemäß definierten Anforderungen konfigurieren. Hierzu hat der Cloud-Kunde das eigene Informationssicherheits-Management geeignet einzubinden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Informationen über den Sicherheitsstatus der Cloud-Dienste sowie weitere bereitgestellte Daten können automatisiert und kontinuierlich ausgelesen werden, da diese den Cloud-Kunden in digitaler Form bereitgestellt werden müssen.

Dies ermöglicht eine kontinuierliche Prüfung.

PSS-05 Authentisierungsmechanismen

Basiskriterium

Der bereitgestellte Cloud-Dienst bietet Authentisierungsmechanismen, mit denen für Benutzer, IT-Komponenten oder Anwendungen im Verantwortungsbereich der Cloud-Kunden eine starke Authentisierung (z. B. durch zwei oder mehrere Faktoren) erzwungen werden kann.

Diese Authentisierungsmechanismen sind an allen Zugangspunkten eingerichtet, die Benutzern, IT-Komponenten oder Anwendungen eine Interaktion mit dem Cloud-Dienst ermöglichen.

Für privilegierte Benutzer, IT-Komponenten oder Anwendungen sind diese Authentisierungsmechanismen erzwungen.

Zusatzkriterium

Der Cloud-Dienst bietet eine Out-of-Band-Authentisierung (OOB), bei der die Faktoren über unterschiedliche Kanäle übertragen werden (z. B. Internet und Mobilfunknetz).

Ergänzende Informationen

Zum Kriterium

IT-Komponente im Sinne dieses Kriterium sind eigenständig einsetzbare Objekte mit Schnittstellen nach außen, die mit anderen IT-Komponenten verbunden werden können.

Zugangspunkte im Sinne dieser Anforderungen sind solche, die für Benutzer, IT-Komponenten oder Anwendungen über Netze erreichbar sind (für Benutzer z. B. die Anmeldemaske auf der öffentlich zugänglichen Internetseite des Cloud-Anbieters).

Die Mehr-Faktor-Authentisierung kann z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token erfolgen.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vom Cloud-Dienst angebotenen Authentisierungsmechanismen gemäß Vorgaben des Identitäts- und Berechtigungsmanagement des Kunden genutzt werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Implementierung von Authentisierungsmechanismen für Benutzer erfolgt über Konfigurationen, die nur in geringer Frequenz angepasst werden. Somit ist eine kontinuierliche Prüfung hier nur bedingt zielführend.

Dennoch ist eine Überwachung des Status des dahinterliegenden Authentifizierungssystems denkbar, wobei jedoch lediglich Abweichungen von Soll-Konfigurationen geprüft werden sollten. Ob diese Abweichungen ggf. gewünscht sind, muss nach wie vor in einer manuellen Prüfung geprüft werden.

PSS-06 Session Management

Basiskriterium

Zum Schutz von Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität bei Interaktionen mit dem Cloud-Dienst wird ein geeignetes Session Management eingesetzt, welches mindestens dem Stand der Technik entspricht und gegen bekannte Angriffe geschützt ist. Es sind Mechanismen implementiert, die nach erkannter Inaktivität einer Session diese invalidiert. Die Erkennung der Inaktivität kann durch Zeitmessung erfolgen. In

diesem Falle ist das Zeitintervall vom Cloud-Anbieter oder – soweit technisch möglich – durch den Cloud-Kunden konfigurierbar.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Bekannte Angriffe sind zum Beispiel Manipulation, Fälschung, Session-Übernahme, Denial-of Service Angriffe, Enveloping, Replay und Null Cipher Angriffe.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Schutzfunktionen des Session Managements des Cloud-Dienstes gemäß den Vorgaben aus ihrem eigenen ISMS nutzen. Außerdem legen sie die Zeitspanne, nach der eine Session ungültig wird, nach den Vorgaben aus ihrem eigenen ISMS fest.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Nutzung von Session Management wird durch Konfigurationen gesteuert. Diese Konfigurationen werden in geringer Frequenz verändert oder angepasst und somit für eine kontinuierliche Prüfung nur bedingt relevant.

Dennoch ist eine Überwachung des Status des dahinterliegenden Authentifizierungssystems denkbar, wobei jedoch lediglich Abweichungen von Soll-Konfigurationen geprüft werden sollten. Ob diese Abweichungen gegebenenfalls normalsind, muss nach wie vor in einer manuellen Prüfung geprüft werden.

PSS-07 Vertraulichkeit von Authentisierungsinformationen

Basiskriterium

Soweit Passwörter als Authentisierungsinformationen für den Cloud-Dienst eingesetzt werden, ist deren Vertraulichkeit durch folgende Verfahren sichergestellt:

- Benutzer können das Passwort initial selbst erstellen oder müssen ein initial vorgegebenes Passwort bei der ersten Anmeldung am Cloud-Dienst ändern. Ein initial vorgegebenes Passwort verliert nach maximal 14 Tagen seine Gültigkeit
- Beim Erstellen von Passwörtern wird das Einhalten der Anforderungen des Cloud-Anbieters (vgl. IDM-09) oder des Cloud-Kunden an Länge und Komplexität technisch erzwungen
- Der Benutzer wird über das Ändern oder Zurücksetzen des Passworts informiert
- Die serverseitige Speicherung erfolgt unter Anwendung kryptographisch starker Hash-Funktionen, die dem Stand der Technik entsprechen, in Kombination mit mindestens 32 Bit langen Salt-Werten.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Den Stand der Technik bezüglich kryptographisch starker Hash-Funktion ist in der jeweils aktuellen Fassung der Technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI festgelegt. In Version 2019-01 dieser Richtlinie waren dies:

- SHA-256, SHA-512/256, SHA-384, SHA-512
- SHA3-256, SHA3-384, SHA3-512.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass gemäß eigener Bewertung hinreichend sichere Passwörter (vgl. IDM-09) verwendet werden und dass die mit der eigenen Wahl verbundenen Risiken eines unautorisierten Zugriffs getragen werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: nein

Die Einhaltung von Sicherheitsrichtlinien bei der Passwortvergabe wird zentral konfiguriert und in geringer Frequenz angepasst. Eine

kontinuierliche Prüfung ist somit nur bedingt zielführend.

PSS-08 Rollen- und Rechtekonzept

Basiskriterium

Der Cloud-Anbieter macht Cloud-Kunden ein Rollen- und Rechtekonzept zum Verwalten von Zugangs- und Zugriffsberechtigungen zugänglich. Darin sind Rechteprofile für die vom Cloud-Dienst bereitgestellten Funktionen beschrieben.

Die Rechteprofile sind geeignet, den Cloud-Kunden eine Verwaltung der Zugangs- und Zugriffsberechtigungen gemäß des Prinzips der geringsten Berechtigung („Least-Privilege-Prinzip“) und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-Know-Prinzip“) zu ermöglichen und den Grundsatz der Funktionstrennung zwischen operativen und kontrollierenden Funktionen („Separation of Duties“) umzusetzen.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Bei IaaS wären in einem Rollen- und Rechtekonzept u.a. die Rechteprofile für folgende Funktionen des Cloud-Dienstes zu beschreiben:

- Verwaltung der Zustände virtueller Maschinen (Start, Pause, Stopp) sowie für deren Migration oder Überwachung
- Verwaltung der verfügbaren Images, mit denen virtuelle Maschinen erstellt werden können
- Verwaltung virtueller Netze (z. B. Konfiguration virtueller Router und Switches).

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass:

- die Vergabe von Berechtigungen an Benutzer in ihrem Verantwortungsbereich einer Autorisierung unterliegt.
- die Angemessenheit der vergebenen Berechtigungen regelmäßig überprüft wird und Berechtigungen bei notwendigen Änderungen (zum Beispiel Mitarbeiter-Austritt) zeitgerecht angepasst oder entzogen werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Das Vorhandensein eines Rollen- und Rechtekonzeptes in Form einer Konfiguration im System kann überwacht werden. Jedoch ist zu beachten, dass auf den Inhalt dieses Konzeptes bezogen lediglich Abweichungen von Soll-Konfigurationen geprüft werden können. Ob diese Abweichungen ggf. gewünscht sind, muss nach wie vor in einer manuellen Prüfung erfasst werden.

PSS-09 Autorisierungsmechanismen

Basiskriterium

Der Zugriff auf die vom Cloud-Dienst bereitgestellten Funktionen wird durch Zugriffskontrollen (Autorisierungsmechanismen) eingeschränkt, die überprüfen, ob Benutzer, IT-Komponenten oder Anwendungen zur Durchführung bestimmter Aktionen berechtigt sind.

Der Cloud-Anbieter validiert die Funktionsfähigkeit der Autorisierungsmechanismen bevor den Cloud-Kunden neue Funktionen bereitgestellt werden sowie bei Änderungen an den Autorisierungsmechanismen bestehender Funktionen (vgl. DEV-06). Der Schweregrad identifizierter Schwachstellen wird nach definierten Kriterien beurteilt, die auf branchenüblichen Metriken basieren (z. B. Common Vulnerability Scoring System), und Maßnahmen zur zeitnahen Behebung oder Mitigation eingeleitet. Nicht behobene Schwachstellen werden im Online-Register bekannter Sicherheitslücken (vgl. PSS-02) dargestellt.

Zusatzkriterium

Die Zugriffskontrollen sind attributbasiert, um granulare und kontextbezogene Überprüfungen anhand mehrerer Attribute eines Benutzers, einer IT-Komponente oder einer Anwendung zu ermöglichen (z. B. Rolle, Standort, Authentifizierungsverfahren).

Ergänzende Informationen

Zum Kriterium

-

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Änderungen an Autorisierungsmechanismen, sowie die Identifizierung von Schwachstellen wird standardisiert durch den Cloud-Anbieter dokumentiert. Diese Dokumentation kann automatisiert und kontinuierlich geprüft werden.

Insofern auch die Behebung der Schwachstellen und deren Priorisierung in standardisierter Form (nach standardisierten Kriterien) erfolgt, können diese Punkte in die kontinuierliche Prüfung integriert werden.

PSS-10 Software-defined Networking

Basiskriterium

Soweit der Cloud-Dienst Funktionen für Software-defined Networking (SDN) bietet, wird die Vertraulichkeit der Daten des Cloud-Kunden durch geeignete SDN-Verfahren sichergestellt.

Der Cloud-Anbieter validiert die Funktionsfähigkeit der SDN-Funktionen, bevor er den Cloud-Kunden neue SDN-Funktionen bereitstellt oder bestehende SDN-Funktionen ändert. Identifizierte Mängel werden risikoorientiert beurteilt und behoben.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Dieses Kriterium ist für das Servicemodell SaaS typischerweise nicht anwendbar.

Geeignete SDN-Verfahren zur Erhöhung der Vertraulichkeit sind zum Beispiel L2-Overlay Networking (Tagging) oder Tunneling/Encapsulation.

Korrespondierende Kriterien für Kunden

-

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Die Validierung bei Bereitstellung und Änderung von SDN-Funktionen sowie bei der Identifizierung von Mängeln, kann durch den Cloud-Anbieter standardisiert dokumentiert werden.

Diese Dokumentation kann durch den Prüfer kontinuierlich und automatisiert geprüft werden.

Das "Markieren" der Daten wird durch eine Konfiguration durchgeführt, die es zentral zu testen gilt. Eine kontinuierliche Prüfung aller übertragenen Datenpakete wäre hier nicht zielführend.

Der Status der Konfiguration kann gegen einen Soll-Wert kontinuierlich geprüft werden, eine inhaltliche Bewertung muss manuell erfolgen.

PSS-11 Images für virtuelle Maschinen und Container

Basiskriterium

Soweit Cloud-Kunden mit dem Cloud-Dienst virtuelle Maschinen oder Container betreiben, hat der Cloud-Anbieter folgende Aspekte sicherzustellen:

- Der Cloud-Kunde kann die Auswahl von Images von virtuellen Maschinen oder Containern gemäß seinen Vorgaben einschränken, so dass Benutzer dieses Cloud-Kunden nur die gemäß diesen Einschränkungen freigegebenen Images oder Container starten können.

- Falls der Cloud-Anbieter dem Cloud-Kunden Images von virtuellen Maschinen oder Containern zur Verfügung stellt, informiert er in geeigneter Weise den Cloud-Kunden über die gegenüber der Vorversion vorgenommenen Änderungen.
- Die vom Cloud-Anbieter bereitgestellten Images sind nach allgemein akzeptierten Branchenstandards gehärtet.

Zusatzkriterium

Beim Start und zur Laufzeit von Images virtueller Maschinen oder Container findet eine Integritätsprüfung statt, die Manipulationen am Image erkennt und dem Cloud-Kunden meldet.

Ergänzende Informationen

Zum Kriterium

Dieses Kriterium ist für das Servicemodell SaaS typischerweise nicht anwendbar.

Allgemein akzeptierte Branchenstandards sind z. B. der Security Configuration Benchmark des Center for Internet Security (CIS) oder die entsprechenden Bausteine im BSI IT-Grundschutz-Kompendium.

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Images von virtuellen Maschinen oder Containern, die sie mit dem Cloud-Dienst betreiben, den Vorgaben ihres Informationssicherheitsmanagements entsprechen und dass die Ergebnisse der Integritätsprüfung beim Start und zur Laufzeit entsprechend dieser Vorgaben verarbeitet werden.

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: teilweise

Die Bereitstellung von Funktionen der Cloud-Dienste für die Cloud-Kunden ist nur bedingt für eine kontinuierliche Prüfung geeignet.

Diese Funktionen müssen zwar zentral in regelmäßigen Abständen geprüft werden, aber nicht kontinuierlich. Daher reicht es aus, dies in die zyklische Prüfung zu integrieren.

Mithilfe eines Agentensystems wäre eine kontinuierliche Abfrage der Konfigurationen der einzelnen virtuellen Maschinen möglich, und damit ein Abgleich zum Soll-Image. Dies könnte auch On-Demand aufgesetzt sein und so Teil der Kontrolle werden, die die Integritätsprüfung übernimmt.

PSS-12 Lokationen der Datenverarbeitung und -speicherung

Basiskriterium

Der Cloud-Kunde ist in der Lage die Lokationen (Ort/Land) der Datenverarbeitung und -speicherung einschl. der Datensicherungen gemäß der vertraglich zur Verfügung stehenden Optionen festzulegen. Dies muss durch die Cloud Architektur sichergestellt sein.

Zusatzkriterium

-

Ergänzende Informationen

Zum Kriterium

Dieses Kriterium ergänzt die Rahmenbedingung BC-01.

Die Cloud Architektur muss in einer solchen Form vorliegen, dass sie die technische Ausgestaltung der IT Infrastruktur zur Bereitstellung des Cloud-Dienstes die mit dem Kunden vereinbarten Datenlokationsvorgaben ermöglicht

Korrespondierende Kriterien für Kunden

Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie sich im Zuge der Dienstleister-Auswahl sowie beim Konfigurieren des Cloud-Dienstes über die Lokationen der Datenverarbeitung sowie -speicherung informieren und, wenn die Wahl zwischen verschiedenen Lokationen besteht, diejenigen auswählen, die den eigenen Anforderungen entsprechen.

Je nach Anwendungsbereich und insbesondere bei einer Nutzung angebotener Dienste des Cloud-Anbieters außerhalb ihres Landes,

berücksichtigen Cloud-Kunden bei der Auswahl auch die für sie geltenden Gesetze (zum Beispiel bei der Verarbeitung personenbezogener Daten; Einhaltung der gesetzlichen Aufbewahrungspflichten für Geschäftsunterlagen etc.).

Hinweise zur kontinuierlichen Prüfung

Möglichkeit: ja

Eine kontinuierliche Erhebung der Lokation der Daten sowie des Landes, aus dem heraus der Service erbracht wird, kann beim Cloud-Anbieter automatisiert durchgeführt werden. Diese Informationen können dann dem Kunden bspw. auf seinem Dashboard oder auf Nachfrage zur Verfügung gestellt werden.