Bundesamt
für Sicherheit in der
Informationstechnik

Cloud Computing

Anforderungskatalog Cloud Computing (C5)

Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten

Inhaltsverzeichnis

1 Einleitung

1 Einleitung

1.1 Ausgangssituation

Cloud Computing ist ein neues Paradigma in der IKT-Branche (Informations- und Kommunikationstechnik). Es besteht darin, dass IT-Dienstleistungen dynamisch an den Bedarf des Kunden angepasst und abrechenbar über ein Netz zur Verfügung gestellt werden. Angebot und Nutzung erfolgen dabei ausschließlich über technische Schnittstellen und Protokolle. Im Übrigen gilt die Definition von Cloud Computing des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (ebenso die Abgrenzung zur IT-Auslagerung), wie sie auf der Webseite des BSI[1] beschrieben ist.

Cloud Computing basiert auf einem hohen Maß an Standardisierung der Hard- 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.

Eine mögliche Lösung besteht darin, dass die hohe Standardisierung des Cloud Computing mit einer hohen Standardisierung der Informationssicherheit kombiniert wird. An verfügbaren Standards zur Informationssicherheit im Bereich des Cloud Computing mangelt es nicht. Zu nennen sind beispielsweise die Standards ISO/IEC 27001 sowie ISO/IEC 27017, die Regelungen der CSA Cloud Controls Matrix und die Produkte des BSI wie die IT-Grundschutz-Kataloge und Sicherheitsprofile für Software-as-a-Service (SaaS).

Zwischen Sicherheitsexperten und Cloud-Dienstleistern existiert durchaus ein informeller Konsens darüber, welche Anforderungen sicheres Cloud Computing erfüllen muss. Einen allgemein anerkannten Anforderungskatalog hierzu gab es bisher jedoch noch nicht.

Es gibt auf dem Markt verschiedene Standards und Zertifizierungen, die von vielen Cloud-Anbietern mit großem Aufwand parallel genutzt und aufrechterhalten werden. Die Vielzahl an verschiedenen Zertifizierungen ist für Kunden jedoch schwer zu überschauen. Mit diesem Anforderungskatalog soll den Kunden eine Hilfestellung für einen besseren Überblick zu mehr Sicherheit gegeben und Mehrfachprüfungen vermieden werden.

1.2 Einheitliche Anforderungen auf Basis vorhandener Standards

Das BSI legt mit diesem Anforderungskatalog seine derzeitige Sichtweise zu diesem informellen Konsens dar, insbesondere auch um eine vertiefte fachliche Diskussion zu ermöglichen. Die Anforderungen wurden, wo immer es möglich war, aus bekannten Sicherheitsstandards entnommen und gegebenenfalls konkretisiert. Nur soweit es nötig erschien, erfolgte eine Ergänzung um eigene Anforderungen. Die Herkunft der Anforderungen wurde transparent dokumentiert, so dass für den Cloud-Anbieter ein Vergleich mit dem eigenen Sicherheitsniveau leicht möglich ist.

Wo dies für sinnvoll erachtet wurde, sind zu einzelnen Basisanforderungen zusätzlich auch weiterführende Anforderungen in den Anforderungskatalog aufgenommen worden. Die Basisanforderungen sollten, wenn es sich um sicheres Cloud Computing handelt, aus der fachlichen Sicht des BSI immer erfüllt sein. Im Übrigen obliegt es dem Cloud-Kunden für seinen konkreten Anwendungsfall zu entscheiden, ob diese Basisanforderungen ausreichen oder ob er zusätzliche, weiterführende Anforderungen an den Cloud-Anbieter stellt. Hierfür stellen die

1 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html

weiterführenden Anforderungen des Anforderungskatalogs einen sinnvollen Ausgangspunkt dar.

Es bleibt die Herausforderung, dem Cloud-Kunden über eine transparente Prüfung durch einen unabhängigen, vertrauenswürdigen Dritten nachzuweisen, dass die Anforderungen des Anforderungskataloges eingehalten werden. Vergleichbar zu den einzelnen Anforderungen selbst, soll auch diese Prüfung auf bestehende Standards und Zertifizierungen aufbauen und so einen möglichst geringen Mehraufwand für den Cloud-Anbieter generieren. Der Anforderungskatalog ist daher so aufgebaut, dass er für eine Prüfung durch Wirtschaftsprüfer gemäß eines internationalen Prüfungsstandards geeignet ist. Dies zielt auf eine Prüfung mit umfangreicher Berichterstattung zu den geprüften aufbau- und ablauforganisatorischen Sicherungs- und Überwachungsmaßnahmen (Kontrollen) und insbesondere unter Einschluss einer Aussage über deren Angemessenheit und Wirksamkeit.

Betreffend des Aufbaus und des Inhalts dieses Anforderungskatalogs wird auf den Abschnitt 2 dieses Dokuments verwiesen. Hinweise zur Durchführung einer Prüfung und Berichterstattung durch einen unabhängigen externen Prüfer sind Gegenstand des Abschnitts 3. Im Abschnitt 3.6 sind Anwendungshinweise für potenzielle Cloud-Kunden aufgeführt. Die ausformulierten Anforderungen sind in den Abschnitten 4 und 5 zu finden. Eine Referenzierung zu einer Auswahl bekannter Standards ist in einem separaten Hilfsdokument aufgeführt, das auf den Webseiten des BSI zu finden ist.

2 Aufbau und Inhalt des Anforderungskatalogs

2 Aufbau und Inhalt des Anforderungskatalogs

2.1 Aufbau des Anforderungskatalogs

Als Cloud-Dienste im Sinne dieses Anforderungskatalogs sind IT-Dienstleistungen zu verstehen, die einem Kunden durch ein Dienstleistungsunternehmen (Cloud-Anbieter, Anbieter oder Dienstleister) über ein Netz bereitgestellt werden. Das Anbieten, Nutzen und Abrechnen der Cloud-Dienste erfolgt dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Der Anforderungskatalog selbst gliedert sich in 17 Anforderungsbereiche (vgl. Abschnitt 2.2).

Jedem Anforderungsbereich ist eine Zielsetzung zugewiesen (vgl. Abschnitt 2.2). Die Zielsetzung gibt dem Cloud-Anbieter eine zusammenfassende Vorgabe, die er im zugehörigen Anforderungsbereich durch entsprechende Maßnahmen in seiner Aufbau- und Ablauforganisation sicher zu stellen hat.

Jeder Zielsetzung sind einzelne Anforderungen zugewiesen (vgl. Abschnitt 5). Die Anforderungen geben allgemeine Grundsätze, Verfahren und Maßnahmen zur Erfüllung der Zielsetzung vor. Hierbei wird zwischen Basisanforderungen und weiterführenden Anforderungen unterschieden. Die Basis- Anforderungen stellen die Gesamtheit der grundlegenden Anforderungen dar, die der Cloud-Anbieter zu erfüllen und im Rahmen einer Prüfung nach diesem Katalog mindestens nachzuweisen hat.

Ergänzend zu ausgewählten Basisanforderungen sind darüber hinaus weiterführende, optionale Anforderungen definiert. Diese sind dahingehend klassifiziert, ob sie insbesondere die Vertraulichkeit (C), die Verfügbarkeit (A) oder beide Eigenschaften (C/A) zugleich in Bezug auf die im Cloud-Dienst verarbeiteten Daten adressieren sollen. Es stellte sich heraus, dass es neben den Basisanforderungen keine wirksamen höherwertigen Anforderungen für Integrität (I) gibt, weshalb diese Kategorie hier fehlt. Die weitergehenden Anforderungen stellen einen Ausgangspunkt für Anforderungen dar, die Cloud-Kunden aufgrund ihres individuellen Anwendungsszenarios stellen könnten.

Die Ausgestaltung, Beschreibung, Einrichtung und nachvollziehbar wirksame Durchführung von geeigneten aufbau- und ablauforganisatorischen Sicherungs- und Überwachungsmaßnahmen (Kontrollen), mit denen die Anforderungen beim Cloud-Anbieter umgesetzt werden, liegen in der Verantwortung des Cloud-Anbieters. Die Gesamtheit der erforderlichen Maßnahmen ist Teil seines die Cloud-Dienste betreffenden internen Kontrollsystems. Die Ausgestaltung dieses internen Kontrollsystems richtet sich nach der Art des erbrachten Cloud-Dienstes, den Anforderungen der Cloud-Kunden und den unternehmerischen Zielen des Cloud-Anbieters sowie den damit verbundenen spezifischen Risiken.

Eine Besonderheit in diesem Anforderungskatalog stellen die so genannten Umfeldparameter dar, die den übrigen Anforderungen vorweg gestellt sind. Umfeldparameter adressieren die Transparenz über Randbedingungen nach denen der Cloud-Dienst erbracht wird (z. B. der Gerichtsstandort). Durch die Informationen aus der Prüfung dieser Umfeldparameter kann der Kunde über die grundsätzliche Eignung gemäß seiner internen Vorgaben entscheiden.

2.2 Inhaltliche Darstellung der Anforderungsbereiche

Vor den einzelnen Anforderungen (Abschnitt 5) sind in Abschnitt 4 Aspekte in Form von so genannten Umfeldparametern aufgenommen, welche die grundsätzlichen Rahmenbedingungen für eine Abfrage darstellen. Sie sind in der Nomenklatur und Struktur den übrigen Anforderungen ähnlich. In welchem Rahmen sich diese Parameter bewegen dürfen, entscheidet dabei der Kunde nach seinen eigenen unternehmensinternen Vorgaben.

Der Anforderungskatalog selbst gliedert sich in 17 Anforderungsbereiche (vgl. Tabelle 1).

Anforderungsbereich	Zielsetzung
Organisation der Informationssicherheit	Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation.
Sicherheitsrichtlinien und Arbeitsanweisungen	Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.
Personal	Sicherstellen, dass Mitarbeiter, Dienstleister und Lieferanten 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.
Asset Management	Identifizieren der organisationseigenen Assets und der Verantwortlichen und gewährleisten eines angemessenen Schutzniveaus.
Physische Sicherheit	Verhindern von unberechtigtem physischen Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.
Regelbetrieb	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.
Identitäts- und Berechtigungsmanagement	Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (in der Regel privilegierte Benutzer) und des Cloud-Kunden zur Vermeidung von unberechtigtem Zugriff.
Kryptographie und Schlüsselmanagement	Gewährleisten einer angemessenen und effektiven Verwendung von Kryptographie zum Schutz der Sicherheit von Informationen.
Kommunikationssicherheit	Sicherstellen des Schutzes von Informationen in Netzwerken und den entsprechenden informationsverarbeitenden Systemen.
Portabilität und Interoperabilität	Ermöglichen der Eigenschaft, den Dienst auf unterschiedlichen IT-Plattformen sicher betreiben zu können sowie die Möglichkeit zur sicheren Anbindung unterschiedlicher IT-Plattformen und Dienstbeendigung.

Anforderungsbereich	Zielsetzung
Beschaffung, Entwicklung und Änderung von Informationssystemen	Einhalten der Sicherheitsvorgaben bei Neuentwicklungen und Beschaffungen von Informationssystemen sowie Änderungen.
Steuerung und Überwachung von Dienstleistern und Lieferanten	Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.
Security Incident Management	Gewährleisten eines konsistenten und umfassenden Vorgehens zur Überwachung, Erfassung, Bewertung, Kommunikation und Eskalation von Sicherheitsvorfällen.
Sicherstellung des Geschäftsbetriebes und Notfallmanagement	Strategische Etablierung und Steuerung eines Business Continuity Managements (BCM). Planen, implementieren und testen von Notfallkonzepten, sowie Verankerung von Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebs.
Sicherheitsprüfung und -nachweis	Überprüfen und Nachhalten, dass die Maßnahmen zur Informationssicherheit in Übereinstimmung mit den organisationsweiten Richtlinien und Anweisungen implementiert und ausgeführt werden.
Compliance und Datenschutz	Vermeiden von Verstößen gegen gesetzliche oder vertragliche Verpflichtungen in Bezug auf Informationssicherheit.
Mobile Device Management	Gewährleistung der Sicherheit beim Einsatz mobiler Endgeräte im Verantwortungsbereich des Cloud-Anbieters für den Zugriff auf IT-Systeme zur Entwicklung und zum Betrieb des Cloud-Dienstes.

Tabelle 1: Anforderungsbereiche des Anforderungskatalogs mit zugewiesenen Zielsetzungen

2.3 Zugrundeliegende nationale und internationale Standards

Entsprechend der Zielsetzung wurden die einzelnen Anforderungen des Anforderungskatalogs inhaltlich auf Grundlage national und international etablierter Standards formuliert. Berücksichtigt wurden im Einzelnen:

» ISO/IEC 27001:2013

» CSA[2] – Cloud Controls Matrix 3.01 (CSA CCM)

» AICPA[3] – Trust Services Principles Criteria 2014 (TSP)

» ANSSI[4] Référentiel Secure Cloud v2.0 (version intermediaire validée du 20/03/2015, nicht veröffentlicht)

» IDW[5] ERS FAIT 5 (Entwurf einer Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing“, Stand vom 04.11.2014)

» BSI IT-Grundschutz Kataloge 14. EL 2014

» BSI SaaS Sicherheitsprofile 2014

Anbietern, die sich bei der Gestaltung ihrer Organisation und Prozesse bereits jetzt an einem oder mehreren dieser Standards orientieren, haben damit die Möglichkeit die Umsetzung des Anforderungskatalogs weitgehend durch eine individuelle Referenzierung ihrer Maßnahmen zu den Anforderungen des Anforderungskataloges zu dokumentieren. Der Anwender wird hierbei über ausführliche Referenzen zwischen den Anforderungen des vorliegenden Katalogs und den Anforderungen der genannten Standards in einem separaten Hilfsdokument unterstützt, das auf den Webseiten des BSI zu finden ist.

2 Cloud Security Alliance, eine Non-Profit-Organisation zur Verbreitung von Sicherheitsstandards im Cloud Computing

3 American Institute of Certified Public Accountants, amerikansicher Berufsverband der Wirtschaftsprüfer

4 Agence nationale de la sécurité des systèmes d'information, französische Behörde für die Sicherheit von Informationssystemen

5 Institut der Wirtschaftsprüfer, die Interessenvertretung der wirtschaftsprüfenden Berufsstände in Deutschland

3 Nachweis der Konformität der Anforderungen durch eine unabhängige Prüfung

3 Nachweis der Konformität der Anforderungen durch eine unabhängige Prüfung

3.1 Einführung

Die in diesem Dokument dargelegten Anforderungen können sowohl von Cloud-Anbietern als auch von Cloud-Kunden herangezogen werden. Der Anbieter kann sich hieran bei der sicheren Gestaltung seiner Prozesse ausrichten. Der Cloud-Kunde wird den Anspruch haben, zu verifizieren, ob der Cloud-Anbieter diese Anforderungen erfüllt. Eine Selbstauskunft für jeden einzelnen Kunden wäre für den Anbieter nicht effizient und für den Kunden zu wenig verbindlich. Zudem wäre eine einheitliche Auskunftstiefe – wenn ein Kunde mehrere Anbieter anfragt – nicht gegeben, so dass ein Kunde nur schwer zwischen verschiedenen Anbietern vergleichen könnte. Eine einheitliche Prüfung durch einen unabhängigen und sachverständigen Dritten, der für den Cloud-Anbieter einen einheitlichen Bericht zur Weitergabe an bestehende und potenzielle Kunden erstellt, ist nach Auffassung des BSI eine wirtschaftliche und sinnvolle Lösung dieses Problems.

Das BSI legt hierzu nachfolgend seine Auffassung dar, nach der ein Prüfer, unbeschadet seiner Eigenverantwortlichkeit, bei einer derartigen Prüfung vorzugehen hat und wie er darüber dem Anbieter und den Kunden des Cloud-Dienstes eine Berichterstattung zur Verfügung zu stellen hat.

Bei der Ausgestaltung der Prüfungsanforderungen wurde, wie bei der inhaltlichen Ausgestaltung der Anforderungen selbst, ebenfalls auf national und international etablierte Standards zurückgegriffen.

Im Einzelnen sind dies der internationale Prüfungsstandard ISAE[6] 3000 (Revised), der als allgemeine Grundlage zur Prüfungsdurchführung und Berichterstattung dient. Dieser wird um weitere Prüfungsstandards ergänzt, die – in sinngemäßer Anwendung – bei Einzelfragen der Prüfungsdurchführung und Berichterstattung genutzt werden sollen. Zu nennen sind ISAE 3402 oder der Prüfungsstandard (PS) 951 des Instituts der Wirtschaftsprüfer (IDW). Ferner sind hier die Regelungen zur Prüfung und Dokumentation nach Service Operation Controls (SOC) zu beachten.

Der Bezug auf die Vorgaben und Regelungen der nationalen und internationalen Wirtschaftsprüfung ist an dieser Stelle bewusst gewählt. Darüber sollen die besonderen Anforderungen an die Unabhängigkeit des Prüfers und an die Verbindlichkeit und Nachvollziehbarkeit der Prüfungsnachweise sichergestellt werden. Gleichzeitig erhalten Cloud-Anbieter, die sich bereits jetzt einer Prüfung nach der im Abschnitt 2.3 genannten Standards unterziehen, damit die Möglichkeit, bei ihnen bereits vorliegende Systemdokumentationen und gegebenenfalls auch Teile vorhandener Prüfungsergebnisse parallel wieder zu verwenden und damit auch Nachweise in Bezug auf die Anforderungen dieses Anforderungskataloges zu erbringen. Der zusätzliche Prüfungsaufwand soll damit reduziert werden.

Das BSI ist der Auffassung, dass die in den genannten Prüfungsstandards dargelegten Anforderungen an die Prüfung zum Zwecke aussagekräftiger Testate keinesfalls unterschritten werden dürfen. Im weiteren Verlauf dieses Abschnitts folgen einige grundlegende Erläuterungen.

6 International Standard on Assurance Engagements

3.2 Prüfungsstandards und Kriterien

3.2.1 ISAE 3000 (Revised) als Prüfungsstandard

Prüfung und Berichterstattung haben unter Anwendung des ISAE 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information" zu erfolgen.

ISAE 3000 (Revised) umfasst allgemeine Anforderungen an die Qualifikation und das Verhalten eines Prüfers (z. B. sachverständige Beurteilung und Skepsis) sowie an die Annahme, Planung und Durchführung eines Prüfungsauftrags. Darüber hinaus sind beispielsweise allgemeine Anforderungen an Prüfungskriterien enthalten, ohne dieses jedoch inhaltlich weiter zu spezifizieren. ISAE 3000 (Revised) ist somit als ein übergeordneter Prüfungsstandard zu verstehen, der den erforderlichen übergeordneten Rahmen setzt.

Der Standard unterscheidet Prüfungen mit einer hinreichenden Sicherheit („reasonable assurance") von Prüfungen mit einer gewissen Sicherheit („limited assurance"). Ferner werden sogenannte „attestation engagements" von sogenannten „direct engagements" unterschieden.[7]

Prüfungen zur Umsetzung der Anforderungen des hier vorgelegten Anforderungskataloges haben mit einer hinreichenden Sicherheit („reasonable assurance") als „attestation engagement" zu erfolgen. Bei einem „attestation engagement" geben die gesetzlichen Vertreter des Cloud-Anbieters (z. B. ein Vertreter der Unternehmensleitung des Cloud-Anbieters) respektive zeichnungsberechtigte Repräsentanten der für die Erbringung des Cloud-Dienstes verantwortlichen Organisationseinheit (nachfolgend „Management des Cloud-Anbieters") eine Erklärung über die Angemessenheit und – soweit einschlägig – die Wirksamkeit der zur Abdeckung der Anforderungen eingerichteten Maßnahmen ab. Gegenüber dem Cloud-Kunden signalisiert der Cloud-Anbieter hierüber die Verbindlichkeit, mit der er der Umsetzung der Anforderungen nachkommt. Für den Prüfer bildet die Erklärung (im internationalen Umfeld auch als „written assertion" oder „written statement" bezeichnet) den Ausgangspunkt für seine Prüfung.

3.2.2 Sinngemäße Anwendung weiterer Prüfungsstandards

Zu besonderen Fragen des Prüfungsvorgehens sowie der Dokumentation und Berichterstattung soll sinngemäß der ISAE 3402 „Assurance Reports on Controls at a Service Organization" herangezogen werden. Alternativ oder ergänzend kann sich der Prüfer sinngemäß auch auf die deutsche Variante dieses Standards (IDW PS 951 n. F. „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen") oder die US- amerikanischen Vorgaben der „Statements on Standards for Attestation Engagements" AT Section 801 bzw. AT Section 101 für den Anwendungsfall sogenannter SOC Prüfungen beziehen.

Alle diese Standards beschäftigen sich mit der Angemessenheit und Wirksamkeit von internen Prozessen und Kontrollen, die bei einem Dienstleister zur Erreichung spezifischer Vorgaben und Ziele eingesetzt werden. Bei ISAE 3402, IDW PS 951 n.F. und AT Section 801 stehen hierbei Prozesse und Kontrollen im Vordergrund, soweit diese für die Finanzberichterstattung der Kunden des Dienstleisters von Bedeutung sind. Im besonderen Anwendungsfall von SOC 2 Prüfungen gemäß AT Section 101 geht es um den Nachweis der Umsetzung der AICPA Trust Services Principles and Criteria (Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und/oder Datenschutz). Diese Prinzipien und Kriterien wurden im Übrigen auch bei der Erstellung dieses Anforderungskataloges berücksichtigt (vgl. Abschnitt 2.3).

Eine sinngemäße Anwendung dieser Prüfungsstandards bedeutet, dass der Prüfung inhaltlich die einzelnen Anforderungen dieses Anforderungskataloges als Kriterien zugrunde gelegt werden und dass die hier genannten Prüfungsstandards zu Einzelfragen betreffend Prüfungsplanung, Durchführung und Berichterstattung genutzt werden. Entsprechend können auch die in den Abschnitten 3.3 und 3.4 detaillierter dargelegten Anforderungen an die Prüfung unmittelbar auf diese Prüfungsstandards

7 Vgl. ISAE 3000, Textziffer 12.

zurückgeführt werden. Hiermit soll insbesondere erreicht werden, dass alle beteiligten Interessengruppen (Cloud-Anbieter, Prüfer sowie der Kunde des Anbieters als Adressat des Berichtes), die bereits über entsprechende Erfahrungen mit Prüfungen und/oder Berichten nach diesen Prüfungsstandards verfügen, diese Erfahrungen unmittelbar auch bei der Prüfung selbst und/oder bei der Auswertung der Berichterstattung einsetzen können.

Gleichwohl bestehen zu einigen Punkten, spezifische ergänzende Erwartungen des BSI. Sie betreffen beispielsweise die Qualifikation des Prüfers oder Einzelheiten zur Darstellung festgestellter Abweichungen in der Berichterstattung. Sie werden im Abschnitt 3.5 als „Gesondert und ergänzende Anforderungen des BSI“ zusammengefasst und erläutert.

3.2.3 Kriterien

Prüfungskriterien sollen allgemeinen übergeordneten Anforderungen entsprechen (vgl. sinngemäß z. B. ISAE 3000 (Revised), Textziffer A45 oder IDW PS 951 n.F., Textziffer 50):

» **Relevanz:** Kriterien müssen für die Beurteilung der durch den Cloud-Anbieter eingerichteten Grundsätze, Verfahren und Maßnahmen sowie für die Entscheidungsfindung maßgebend sein.

» **Vollständigkeit:** Kriterien sind vollständig, wenn keine für die Beurteilung der durch den Cloud-Anbieter eingerichteten Grundsätze, Verfahren und Maßnahmen sowie keine für die Entscheidungsfindung wesentlichen Gesichtspunkte ausgeklammert wurden.

» **Verlässlichkeit:** Kriterien sind verlässlich, wenn sie eine konsistente und nachvollziehbare Beurteilung der durch den Cloud-Anbieter eingerichteten Grundsätze, Verfahren und Maßnahmen zulassen.

» **Neutralität:** Kriterien sind neutral, wenn sie eine objektive Beurteilung der durch den Cloud-Anbieter eingerichteten Grundsätze, Verfahren und Maßnahmen sicherstellen.

» **Verständlichkeit:** Kriterien sind verständlich, soweit sie klare Schlussfolgerungen ermöglichen und dadurch Fehlinterpretationen vermieden werden.

Die Anforderungen des Anforderungskataloges orientieren sich an den im Abschnitt 2.3 aufgeführten Standards und Publikationen. Über diesen Bezug wird nach Ansicht des BSI sichergestellt, dass die darin enthaltenen Anforderungen geeignet sind, um als Grundlage für eine sachgerechte und nachvollziehbare Beurteilung der Cloud-Dienste durch die Cloud-Anbieter selbst und durch einen unabhängigen Prüfer herangezogen werden zu können.

3.3 Prüfungsgegenstand einschließlich Systembeschreibung

3.3.1 Prüfungsgegenstand

Gegenstand der Prüfung sind die zwei Dinge:

» Die Beschreibung des die Cloud-Dienste betreffenden internen Kontrollsystems (Systembeschreibung) und

» die in der Systembeschreibung mit Bezug auf die einzelnen Anforderungen dargestellten Kontrollen auf Basis einer vom Management des Cloud-Dienstleisters abzugebenden Erklärung.

Die Verantwortung für die Systembeschreibung und deren Inhalt liegt bei den gesetzlichen Vertretern des Anbieters. Die Erklärung des Managements umfasst die Angemessenheit und in der Regel auch die Wirksamkeit des in der Systembeschreibung dargestellten die Cloud-Dienste betreffenden internen Kontrollsystems. Hierbei eingeschlossen sind auch die Prozesse und Verfahren zur Einrichtung und Durchführung der dargestellten Kontrollen.

Bei einer Prüfung hinsichtlich des Anforderungskataloges werden zwei Typen der Prüfung und Berichterstattung unterschieden, wie dies auch bei ISAE 3402 oder IDW PS 951 n.F. der Fall ist.

» **Prüfung und Berichterstattung vom Typ 1:**
Der Prüfer hat zu beurteilen, ob die Systembeschreibung die tatsächliche Ausgestaltung und Einrichtung des die Cloud-Dienste betreffenden internen Kontrollsystems zu dem zu prüfenden Zeitpunkt sachgerecht darstellt und die dargestellten Kontrollen angemessen ausgestaltet sind. Eine Berichterstattung vom Typ 1 eignet sich beispielsweise im Falle einer Erstprüfung, um für neu entwickelte Cloud-Dienste zeitnah ein Prüfungsergebnis zu erhalten. Sie ist zum Nachweis der tatsächlichen Umsetzung über einen rückblickenden Zeitraum nicht geeignet.

» **Prüfung und Berichterstattung vom Typ 2:**
Der Prüfer führt, im Vergleich zur Prüfung und Berichterstattung nach Typ 1, zusätzliche Prüfungshandlungen zur Wirksamkeit der Kontrollen (Funktionsprüfunggen) durch. Hierfür soll der Prüfungszeitraum im Regelfall zwölf Monate, zumindest aber sechs Monate umfassen. Kürzere Prüfungszeiträume können in begründeten Ausnahmefällen (z. B. bei der Gründung des Cloud-Anbieters, Übernahme neuer Cloud-Dienste) in Betracht kommen und sind in der Berichterstattung zu begründen.

Nach Auffassung des BSI ist eine Prüfung und Berichterstattung vom Typ 2 erforderlich, um eine angemessene Aussagekraft zu erzeugen. Berichterstattungen vom Typ I sollten nur in den oben genannten und zu begründenden Ausnahmefällen erfolgen und keinesfalls mehrmals hintereinander in Betracht gezogen werden.

Der Anforderungskatalog unterscheidet Basisanforderungen und optionale, weitergehende Anforderungen (vgl. Abschnitt 2.1).

» Der Prüfung und Berichterstattung können entweder die Basisanforderungen allein oder die Basisanforderungen zusammen mit den weitergehenden Anforderungen zugrunde gelegt werden.

» Die Basisanforderungen (und soweit zutreffend die weitergehenden Anforderungen) müssen in jedem Fall vollständig und ohne Auslassungen adressiert werden. Zum Nachweis einer höheren Vertraulichkeit können weiterführende Anforderungen mit entsprechendem Vertraulichkeitsbezug (im Abschnitt 5, Spalte „C/A“ mit „C“, bzw. „C/A“ klassifiziert) berücksichtigt werden. Für den Nachweis über höhere Verfügbarkeit gilt entsprechendes. Welche weitergehenden Anforderungen als Kriterien in die Prüfung einbezogen waren, muss aus der Systembeschreibung des Cloud-Anbieters hervorgehen. Soweit alle weiterführenden Anforderungen mit Vertraulichkeits-Bezug (C und C/A) bzw. alle Anforderungen mit Verfügbarkeitsbezug (A und C/A) vollständig erfüllt werden, ist dies darüber hinaus in der Beschreibung des Prüfungsgegenstandes durch den Zusatz „Die Systembeschreibung adressiert vollumfänglich alle weitergehenden Anforderungen an [die Vertraulichkeit] / [(und) die Verfügbarkeit]“ zu kennzeichnen. Sofern einzelne Anforderungen aus Sicht des Cloud-Anbieters nicht anwendbar sind, ist dies in der Systembeschreibung entsprechend zu begründen. Der Zusatz in der Beschreibung des Prüfungsgegenstandes entfällt in diesem Fall.

3.3.2 Systembeschreibung des Cloud-Anbieters

Die Systembeschreibung der Cloud-Dienste wird vom Cloud-Anbieter erstellt. Der Mindestumfang der Systembeschreibung ergibt sich in sinngemäßer Anwendung des ISAE 3402 (oder des/der alternativ herangezogenen Standards, vgl. Abschnitt 3.2). Exemplarisch sind die folgenden Bestandteile zu nennen:

» Art und Umfang der erbrachten Cloud-Dienste,

» Grundsätze, Verfahren und Maßnahmen zur Erbringung (Entwicklung und/oder Betrieb) des Cloud-Dienstes, einschließlich der eingerichteten Kontrollen,

» Beschreibung der eingesetzten Infrastruktur-, Netzwerk- und Systemkomponenten für Entwicklung und Betrieb des Cloud-Dienstes, einschließlich der geographischen Lage der Datenverarbeitung und Speicherung,

» Regelung des Umgangs mit bedeutsamen Vorkommnissen und Verhältnissen, die Ausnahmen vom Regelbetrieb darstellen, wie beispielsweise der Ausfall von kritischen IT-Systemen,

» Rollen und Zuständigkeiten des Cloud-Anbieters und des Cloud-Kunden, einschließlich Mitwirkungspflichten und erforderlicher korrespondierender Kontrollen beim Cloud-Kunden,

» an Unterauftragnehmer vergebene oder ausgelagerte Funktionen.

Bei der Berichterstattung vom Typ 2 muss die Systembeschreibung alle wesentlichen Änderungen des die Cloud-Dienste betreffenden internen Kontrollsystems, die während des Berichtszeitraums vorgenommen wurden, hinreichend detailliert darstellen. Dies umfasst auch solche Änderungen, die sich aus einer zwischenzeitlich erfolgten Aktualisierung des Anforderungskatalogs ergeben haben (vgl. Abschnitt 3.5.4). In keinem Fall darf die Systembeschreibung Informationen auslassen bzw. verzerren, die für den Aufgabenbereich des die Cloud-Dienste betreffenden internen Kontrollsystems relevant sind. Das bedeutet jedoch nicht, dass sämtliche Aspekte darzustellen sind, die aus individueller Sicht einzelner auslagernder Unternehmen als wichtig erachtet werden können.

Zu beachten ist hierbei, dass die Systembeschreibung in der Regel für eine Vielzahl von auslagernden Unternehmen erstellt wird, dass aber die Prozesse in Teilen gleichwohl kundenindividuell ausgestaltet sein können.

Unter Umständen lagert der Cloud-Anbieter Teile seiner Geschäftsprozesse zur Entwicklung und/oder zum Betrieb des Cloud-Dienstes auf weitere Dienstleistungsunternehmen aus (Einsatz von Unterauftragnehmern). Dies muss in der Systembeschreibung (und auch im Zuge der Prüfung) entsprechend berücksichtigt werden. Hierfür werden die „Inclusive Methode“ und die „Carve-out Methode“ unterschieden.

» **Inclusive Methode:** Die Systembeschreibung umfasst auch die Art und den Umfang der ausgelagerten Teile sowie die beim Unterauftragnehmer angesiedelten Kontrollen, die dann zusammen mit den Kontrollen beim Cloud-Anbieter selbst ebenfalls Gegenstand der Prüfung sind.

» **Carve-out Methode:** Die Systembeschreibung umfasst keine detaillierte Beschreibung der ausgelagerten Funktionen. Die beim Unterauftragnehmer angesiedelten Kontrollen sind nicht Gegenstand der Prüfung. In diesem Fall erfolgt zumindest eine Prüfung der Kontrollen des Dienstleisters, die der Überwachung der Wirksamkeit der Kontrollen beim Unterauftragnehmer dienen (vgl. hierzu auch die Anforderungen DLL-01 und DLL-02 im Abschnitt 5). Am unkompliziertesten ist es in diesem Fall, wenn der Unterauftragnehmer nach den Vorgaben aus diesem Dokument geprüft ist (und regelmäßig geprüft wird) und dem Cloud-Anbieter einen Prüfbericht über die Wirksamkeit der ausgelagerten Kontrollen vorlegt, den dieser im Rahmen seiner Verfahren zur Steuerung und Überwachung seiner Unterauftragnehmer verarbeitet.

Der Cloud-Anbieter hat die anzuwendende Methode nach eigenem Ermessen auszuwählen. Diese Auswahl ist deutlich im Prüfbericht zu hinterlegen und dem (potenziellen) Cloud-Kunden transparent zu machen. Bei Anwendung der Carve-out Methode wird der Wirtschaftsprüfer beurteilen, ob der Umfang der Auslagerung in der Systembeschreibung zutreffend beschrieben ist (z. B. auf Basis des Vertrags und Prüfberichten über das dienstleistungsbezogene interne Kontrollsystem des Unterauftragnehmers) und die Wirksamkeit der ausgelagerten Kontrollen durch den Cloud-Anbieter gemäß der Anforderung DLL-02 überwacht wird.

Inwiefern Unterauftragnehmer die Anforderungen aus diesem Katalog erfüllen und wie die Umfeldparameter beim Unterauftragnehmer ausgestaltet sind, ist im Prüfbericht zu dokumentieren.

3.3.3 Verwertung von Nachweisen aus anderen Prüfungen

Die einzelnen Anforderungen dieses Anforderungskataloges basieren weitgehend auf national und international bekannten Standards. Sofern diese beim Cloud-Anbieter bereits als Referenz genutzt werden, wird er entsprechende Prozesse und Kontrollen bereits in seinem Betriebsablauf berücksichtigt haben. Diese Prozesse und Kontrollen bilden typischerweise auch die Grundlage für weitere Prüfungen, die beim Cloud- Anbieter typischerweise durch unabhängige externe Prüfer vorgenommen werden. Zu nennen sind in diesem Zusammenhang insbesondere Prüfungen nach ISAE 3402, IDW PS 951 und/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 Anforderungskatalog zu kombinieren. Hierdurch werden Prüfer und Cloud-Anbieter bei sich überschneidenden Kontrollen in die Lage versetzt, Teile der Systembeschreibungen und der Prüfungsergebnisse parallel sowohl für eine Berichterstattung nach z. B. ISAE 3402 und/oder SOC 2 als auch für die Berichterstattung nach diesem Anforderungskatalog zu nutzen. Dabei bietet es sich in der Regel an, der Prüfung nach diesem Anforderungskatalog jeweils den selben Prüfungszeitraum wie bei den anderen Prüfungen zugrunde zu legen.

Dies erlaubt, gleichermaßen bei der Umsetzung der Anforderungen dieses Anforderungskataloges, der Dokumentation der Maßnahmen in einer Systembeschreibung und bei der Prüfung selbst, unnötigen Mehraufwand zu reduzieren.

Sofern der Cloud-Anbieter weitergehende Zertifikate (z. B. nach ISO/IEC 27001, ISO 22301 oder Datenschutzzertifikate) anstrebt, bietet es sich an, die entsprechenden Auditoren ggf. in das Prüfungsteam mit aufzunehmen und die Prüfung, soweit möglich, gemeinsam durchzuführen. Auf diese Weise bietet sich die Möglichkeit, die Effizienz der Prüfungen insgesamt weiter zu optimieren. Die Referenztabelle in einem separaten Hilfsdokument zu diesem Anforderungskatalog kann zur Identifizierung von Überschneidungen zwischen den im Abschnitt 2.3 genannten Standards und diesem Anforderungskatalog dienen.

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

3.4 Prüfungsziel und Berichterstattung

3.4.1 Prüfungsziel

Beim Prüfungsziel ist zu unterscheiden, ob eine Berichterstattung nach Typ 1 oder Typ 2 (vgl. Abschnitt 3.3.1) vereinbart wurde. Je nach vereinbartem Typ fällt der Prüfer unterschiedliche Prüfurteile. Ziel der Prüfung ist es, dem Prüfer eine Aussage mit hinreichender Sicherheit (Prüfungsurteil) darüber zu ermöglichen, ob

» die Systembeschreibung des Anbieters die tatsächliche Ausgestaltung und Einrichtung des die Cloud-Dienste betreffenden internen Kontrollsystems zum zu prüfenden Zeitpunkt (Berichterstattung vom Typ 1) bzw. während des zu prüfenden Zeitraums (Berichterstattung vom Typ 2) sachgerecht darstellt,

» 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) im Hinblick auf die Erfüllung der Anforderungen des Anforderungskatalogs angemessen ausgestaltet sind,

» die in der Systembeschreibung dargestellten Kontrollen (nur im Falle der Prüfung und Berichterstattung vom Typ 2) während des zu prüfenden Zeitraums wirksam sind.

3.4.2 Berichterstattung des Prüfers

Die Berichterstattung über die Prüfung umfasst (in analoger Anwendung des ISAE 3402) die folgenden Bestandteile. Die Gliederung sollte sich entsprechend an diesen Bestandteilen orientieren:

1. Bescheinigung des unabhängigen Prüfers
   - » Auftrag und Prüfungsumfang,
   - » Verantwortung der gesetzlichen Vertreter des Anbieters der Cloud-Dienstes bzw. des für die Cloud-Dienste verantwortlichen Managements des Cloud-Anbieters,
   - » Unabhängigkeit und Qualitätssicherung des Prüfers/der Prüfungsgesellschaft, einschließlich Angaben zur fachlichen Qualifikation des Prüfers,
   - » Verantwortung des Prüfers,
   - » Inhärente Grenzen von Kontrollen bei Dienstleistungsunternehmen,
   - » Prüfungsurteil,
   - » Adressaten und Nutzung der Bescheinigung,
   - » Hinweis auf die Auftragsbedingungen.
2. Erklärung der gesetzlichen Vertreter des Anbieters des Cloud-Dienstes bzw. des für die Cloud-Dienste verantwortlichen Managements des Cloud-Anbieters (im internationalen Umfeld auch als „written assertion“ oder „written statement“ bezeichnet).
3. Beschreibung des die Cloud-Dienste betreffenden internen Kontrollsystems (als Teil der Systembeschreibung).
4. Darstellung der Anforderungen und der zugeordneten Kontrollen (Teil der Systembeschreibung), sowie Darstellung der durchgeführten Prüfungshandlungen und der einzelnen Prüfungsergebnisse des Prüfers.
5. Optional: sonstige Informationen, bereitgestellt durch den Dienstleister.

3.5 Gesonderte und ergänzende Anforderungen des BSI

3.5.1 Qualifikation des Prüfers

Die Beurteilung eines die Cloud-Dienste betreffenden internen Kontrollsystems auf Grundlage des Anforderungskataloges stellt nach Auffassung des BSI, aufgrund der damit verbundenen auch technisch geprägten Aspekte, besondere Anforderungen an die Qualifikation des Prüfers.

Neben den mit der Anwendung des ISAE 3000 (Revised) allgemein verbundenen Anforderungen an den Prüfer, werden an den Prüfer bzw. das von ihm eingesetzte Prüfungsteam daher folgende ergänzende Anforderungen gestellt.

Mindestens die Hälfte der Mitglieder des Prüfungsteams verfügt über mehr als 3 Jahre Berufserfahrung in der Wirtschaftsprüfung und darüber hinaus über zumindest 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)

In der Berichterstattung ist anzugeben, welche der hier genannten Berufsexamina/Zertifizierungen im Prüfungsteam vorlagen (z. B. im Abschnitt zur Unabhängig und Qualitätssicherung des Prüfers). Die zugehörigen Nachweise sind dem Auftraggeber für die Prüfung auf Anfrage vorzulegen.

3.5.2 Berichterstattung über bestehende bzw. festgestellte Abweichungen von den Anforderungen

Es liegt in der Natur des Prüfungsgegenstandes, dass es im Zuge der Prüfung zu „negativen" Prüfungsfeststellungen kommen kann. Unabhängig von der Frage, ob eine solche Feststellung insgesamt zu einer Einschränkung im Prüfungsurteil führt oder nicht, erwarten die Kunden des Cloud-Anbieters, dass dieser erkennbare Maßnahmen zur Fehlerbeseitigung und Optimierung seiner Systeme und Prozesse durchführt.

Vor diesem Hintergrund sind in die Berichterstattung folgende Zusatzinformationen aufzunehmen:

» Sofern der Mangel vom Dienstleister selbst erkannt wurde, ist anzugeben, wann und im Zuge welcher Maßnahmen des Dienstleisters der Mangel erkannt wurde.

» Sofern der Mangel bereits Gegenstand der Berichterstattung über einen vorhergehenden Prüfungszeitraum war, ist anzugeben, wann und im Zuge welcher Maßnahmen der Mangel erkannt wurde; verbunden mit einem gesonderten Hinweis, dass die Entdeckung in einem vorherigen Prüfungszeitraum erfolgte. Dies setzt voraus, dass der Prüfer auf Prüfberichte des Cloud-Anbieters aus vorangegangenen Prüfungszeiträumen zugreifen kann. Im Zweifelsfall hat sich der Prüfer dies im Zuge seiner Beauftragung als Prüfer gesondert zusichern zu lassen.

» In jedem Fall soll angegeben werden, welche Maßnahmen zur künftigen Behebung des Mangels vorgesehen sind und ab wann diese Maßnahmen voraussichtlich abgeschlossen bzw. wirksam eingerichtet sein werden.

Die Berichterstattung hierüber kann beispielsweise in einem gesondert gekennzeichneten Abschnitt der Systembeschreibung oder im optionalen Abschnitt der „Sonstige Informationen, bereitgestellt durch die gesetzlichen Vertreter des Dienstleisters" erfolgen.

3.5.3 Angaben zur Haftungsbegrenzung

Die Regelungen zur Haftung des Prüfers gegenüber dem Dienstleister und den sonstigen Empfängern der Berichterstattung können, auch in Abhängigkeit landesspezifischer, den Prüfer betreffende Regelungen, unterschiedlich ausgestaltet sein.

Nach Überzeugung des BSI sind Angaben zu Art und Höhe der Haftung des Prüfers für den Berichtsempfänger eine bedeutende Information. Vor diesem Hintergrund muss die Berichterstattung eine vorgesehene bzw. vereinbarte Haftungsbegrenzung erkennen lassen.

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

3.5.4 Umgang mit Aktualisierungen des Anforderungskataloges

Das BSI beabsichtigt, den Anforderungskatalog 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 des Anforderungskataloges verbundenen Anpassungen der Systeme und Prozesse sowie der Prüfungsdurchführung vorzunehmen.

Nach Auffassung des BSI müssen die Anpassungen 12 Monate nach Veröffentlichung der neuen Version umgesetzt sein. Abweichungen hiervon sind gegenüber dem Kunden und Prüfern zu begründen.

Wie im Abschnitt 3.3.2 dargelegt, sind alle im Verlauf eines Prüfungszeitraumes vorgenommenen wesentlichen Änderungen des die Cloud-Dienste betreffenden internen Kontrollsystems hinreichend detailliert in der Systembeschreibung darzustellen. Da die Umsetzung der Aktualisierungen des Anforderungskataloges innerhalb von

12 Monaten erfolgen soll, kann es im Verlauf eines Prüfungszeitraums vorkommen, dass sich die Beurteilung der Angemessenheit und der Wirksamkeit sowohl auf den Stand vor, als auch nach Umsetzung dieser Maßnahmen bezieht.

Soweit der Prüfungszeitraum in einem Zeitraum endet, der zwischen sechs und zwölf Monaten nach der Veröffentlichung der Aktualisierung des Anforderungskataloges liegt, muss der Cloud-Anbieter in der Systembeschreibung ergänzende Angaben auch zu den noch erforderlichen und noch nicht abgeschlossenen Umsetzungsmaßnahmen machen. Hieraus muss auch hervorgehen, wann diese Maßnahmen abgeschlossen bzw. wirksam eingerichtet sein sollen.

3.6 Anwendungshinweise an potenzielle Cloud-Kunden: Regelmäßige Prüfung und vertragliche Zusicherung

In den vorhergehenden Abschnitten wurden die grundlegenden Anforderungen an die Prüfung und Berichterstattung von Cloud-Diensten dargelegt. In den nachfolgenden Kapiteln folgen die konkreten Anforderungen. In diesem Abschnitt gibt das BSI Hinweise an potenzielle Cloud-Kunden, wie sie eventuell vorhandene Testate von Cloud-Anbietern nutzen sollten.

Zuerst gilt festzuhalten, dass die Sicherheit von Cloud-Diensten eine fortlaufende Aufgabe ist. Diese Einsicht hat sich auch im Testat widerzuspiegeln. Es muss daher regelmäßig – i. d. R. alle 12 Monate – erneuert werden.

Ferner gilt, dass das BSI auf die eigentliche Prüfung durch den Wirtschaftsprüfer keinen Einfluss hat und auch nicht selbst die Qualität des Cloud-Dienstes überprüft. Der Wirtschaftsprüfer erbringt seine Tätigkeit gegenüber dem Cloud-Anbieter, nicht gegenüber dem Kunden des Anbieters.

Der Kunde des Cloud-Anbieters sollte die Einhaltung der Anforderungen aus diesem Anforderungskatalog (inklusive der Anforderung an Prüfung, Prüfungsintervalle und Berichterstattung) als einen wesentlichen Bestandteil seiner Beauftragung ansehen und dies auch mit dem Anbieter vereinbaren. Dies gilt insbesondere für den Fall, wenn höherwertige Anforderungen durch den Cloud-Anbieter erfüllt werden sollen.

Ferner sollte der potenzielle Cloud-Kunde seine Entscheidung nicht nur auf ein vorhandenes, aktuelles Testat (unabhängig, ob es sich lediglich auf die Basisanforderungen oder auch auf höherwertige bezieht) nach diesem Anforderungskatalog gründen, sondern sollte sich den Prüfbericht regelmäßig vorlegen lassen.

4 Rahmenbedingungen des Cloud-Dienstes (Umfeldparameter)

4 Rahmenbedingungen des Cloud-Dienstes (Umfeldparameter)

Zielsetzung: Die grundsätzlichen organisatorischen und rechtlichen Rahmenbedingungen und Vorgaben sind für einen sachverständigen Dritten nachvollziehbar und zutreffend beschrieben, um die grundsätzliche Eignung des Cloud-Dienstes für die gewünschte Anwendung zu beurteilen.

UP-01 Systembeschreibung

Basisanforderung

Der Cloud-Anbieter macht in seiner Systembeschreibung nachvollziehbare und transparente Angaben zum Cloud-Dienst, die es einem sachverständigen Dritten erlauben, die grundsätzliche Eignung des Cloud-Dienstes für die gewünschte Anwendung zu beurteilen.

Die Systembeschreibung beschreibt die folgenden Aspekte:

» Art und Umfang der erbrachten Cloud-Dienste gemäß der Dienstgütevereinbarung (Service Level Agreements), die einem Vertrag mit den Cloud-Kunden typischerweise zugrunde liegt,

» Grundsätze, Verfahren und Maßnahmen zur Erbringung (Entwicklung und/oder Betrieb) des Cloud-Dienstes, einschließlich der eingerichteten Kontrollen,

» Beschreibung der eingesetzten Infrastruktur-, Netzwerk- und Systemkomponenten für Entwicklung und Betrieb des Cloud-Dienstes,

» Umgang mit bedeutsamen Vorkommnissen und Verhältnissen, die Ausnahmen vom Regelbetrieb darstellen, wie bspw. der Ausfall von kritischen IT-Systemen,

» Rollen und Zuständigkeiten des Cloud-Anbieters und des Cloud-Kunden, einschließlich Mitwirkungspflichten und korrespondierender Kontrollen beim Cloud-Kunden,

» an Unterauftragnehmer vergebene oder ausgelagerte Funktionen.

Ergänzende Informationen zur Basisanforderung

Die Beschreibung der Infrastruktur-, Netzwerk- und Systemkomponenten sollen so detailliert sein, dass der Cloud-Kunde einen guten und für Risikoabwägungen im Rahmen seines Sicherheitsmanagements notwendigen Überblick erhält ohne jedoch die Sicherheit des Cloud-Anbieters durch deren Darlegung zu gefährden.

UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung

Basisanforderung

Der Cloud-Anbieter macht in Dienstgütevereinbarungen (Service Level Agreements), seiner Verfahrensdokumentation oder vergleichbaren Dokumentationen nachvollziehbare und transparente Angaben zu seiner Gerichtsbarkeit sowie den Lokationen der Daten bei Datenspeicherung, -verarbeitung und -sicherung, die es einem sachverständigen Dritten erlauben, die grundsätzliche Eignung des Cloud-Dienstes für die Kundenanwendung zu beurteilen. Das betrifft auch die Verarbeitung, Speicherung und Sicherung von Daten des Cloud-Kunden durch Unterauftragnehmer des Cloud-Anbieters. Daten des Cloud-Kunden werden außerhalb der vertraglich vereinbarten Lokationen nur nach ausdrücklicher, schriftlicher Zustimmung des Cloud-Kunden verarbeitet, gespeichert und gesichert.

UP-03 Offenbarungs- und Ermittlungsbefugnisse

Basisanforderung

Der Cloud-Anbieter macht in Dienstgütevereinbarungen (Service Level Agreements), seiner Verfahrensdokumentation oder vergleichbaren Dokumentationen nachvollziehbare und transparente Angaben zu geltenden Offenbarungs- und Ermittlungsbefugnissen staatlicher Stellen, die Zugriff auf Daten des Cloud-Kunden ermöglicht. Die Angaben müssen einem sachverständigen Dritten erlauben, die grundsätzliche Eignung des Cloud-Dienstes für die Kundenanwendung zu beurteilen. Sofern der Cloud-Anbieter auf Dienste Dritter zugreift, hat er diese Angaben von diesen eingeholt.

Ergänzende Informationen zur Basisanforderung

Verbundene Unternehmen sind Mutter- oder Tochterunternehmen des Cloud-Anbieters im Sinne des § 271 Abs. 2 HGB. Offenbarungs- und Ermittlungsbefugnisse bestehen üblicherweise gegenüber Polizei und Staatsanwaltschaft sowie Geheimdienststellen.

UP-04 Zertifizierungen

Basisanforderung

Der Cloud-Anbieter macht in Dienstgütevereinbarungen (Service Level Agreements), seiner Verfahrensdokumentation oder vergleichbaren Dokumentationen nachvollziehbare und transparente Angaben zu vorhandenen und gültigen Zertifizierungen oder Bescheinigungen unabhängiger Dritter, die es einem sachverständigen Dritten erlauben, die grundsätzliche Eignung des Cloud-Dienstes für die Kundenanwendung zu beurteilen.

Ergänzende Informationen zur Basisanforderung

Folgende Zertifikate oder Bescheinigungen können dabei vorgelegt werden:

» ISO/IEC 27001 (ggf. auch auf der Basis von IT- Grundschutz)

» ISO 22301

» von den zuständigen Datenschutzbehörden akzeptierter Nachweis über die Einhaltung des Datenschutzes

» Prüfberichte nach ISAE 3402/SSAE 16/SOC1/ IDW PS 951

» Softwarebescheinigungen nach IDW PS 880

Wichtig ist hierbei der Zertifizierungsgegenstand bzw. bei Systemzertifizierung, welchen Bereich diese abdecken.

5 Zielsetzungen und Anforderungen

5 Zielsetzungen und Anforderungen

5.1 Organisation der Informationssicherheit

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

OIS-01 Managementsystem für Informationssicherheit

Basisanforderung

Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS), das sich an ISO-Standards der 2700x-Reihe orientiert.

» Die hierzu eingesetzten Instrumente und Methoden ermöglichen eine nachvollziehbare Lenkung der folgenden Aufgaben und Aktivitäten zur dauerhaften Aufrechterhaltung der Informationssicherheit: Planung, Umsetzung der Planung bzw. Durchführung des Vorhabens,

» Erfolgskontrolle bzw. Überwachung der Zielerreichung und

» Beseitigung von erkannten Mängeln und Schwächen sowie kontinuierliche Verbesserung.

Das ISMS umfasst auch die IT-Prozesse zur Entwicklung und Betrieb des Cloud-Dienstes.

Ergänzende Informationen zur Basisanforderung

Soweit durch den Cloud-Anbieter noch keine Zertifizierung des ISMS vorgelegt werden kann, dessen Erklärung zur Anwendbarkeit (Statement of Applicability) die IT-Prozesse zur Entwicklung und Betrieb des Cloud-Dienstes umfasst, können Angemessenheit und Wirksamkeit unter anderem durch Prüfung der folgenden Anforderungen beurteilt werden:

» OIS-01 Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung

» OIS-07 Identifikation, Analyse, Beurteilung und Behandlung von Risiken

» SA-01, SA-02 und SA-03 Richtlinien und Anweisungen

» SPN-01 Informieren der Unternehmensleitung

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS), das eine gültige Zertifizierung nach ISO/IEC 27001:2013 oder ISO 27001 auf Basis von IT-Grundschutz aufweist. Die Erklärung zur Anwendbarkeit (Statement of Applicability) umfasst die IT-Prozesse zur Entwicklung und Betrieb des Cloud-Dienstes.

OIS-02 Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung

Basisanforderung

Eine Sicherheitsleitlinie mit Sicherheitszielen und strategischen Vorgaben, wie diese Ziele erreicht werden sollen, ist dokumentiert. Die Sicherheitsziele leiten sich von den Unternehmenszielen und Geschäftsprozessen, relevanten Gesetzen und Verordnungen, sowie der aktuellen und zukünftig erwarteten Bedrohungsumgebung in Bezug auf Informationssicherheit ab. Die strategischen Vorgaben stellen grundlegende Rahmenbedingungen dar, die in weiteren Richtlinien und Anweisungen

näher spezifiziert werden (vgl. SA-01). Die Leitlinie wird von der Unternehmensleitung verabschiedet und an alle betroffenen internen und externen Parteien des Cloud-Anbieters (z. B. Cloud-Kunden, Unterauftragnehmer) kommuniziert.

Ergänzende Informationen zur Basisanforderung

Die hier geforderte Leitlinie ist eine Basisanforderung. Weiterführende Richtlinien und Anweisungen müssen sich an der Größe und Komplexität der Organisation des Cloud-Anbieters und der Art des angebotenen Cloud-Dienstes orientieren. Während in der Leitlinie kurz und prägnant die allgemeinen Sicherheitsziele und eine Strategie zur Erreichung dieser Ziele formuliert sein müssen, sind typischerweise keine organisatorischen und technischen Details enthalten. Es hat sich bewährt diese in weiteren Richtlinien und Anweisungen auf verschiedenen Ebenen näher zu regeln. Auf den unteren Ebenen steigt der Detaillierungsgrad, während sich die Änderungsintervalle verkürzen.

OIS-03 Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit

Basisanforderung

Zwischen Cloud-Anbieter und Cloud-Kunden geteilte Verantwortlichkeiten, Mitwirkungspflichten sowie die Schnittstellen zum Melden von Sicherheitsvorfällen und Störungen sind in Abhängigkeit des Cloud-Modells (Infrastructure-, Plattform- oder Software-as-a-Service) und den vertraglichen Verpflichtungen definiert, dokumentiert, zugewiesen und an alle betroffenen internen und externen Parteien (z. B. Cloud-Kunden, Unterauftragnehmer des Cloud-Anbieters) kommuniziert. Seitens des Cloud-Anbieters sind mindestens die folgenden Rollen (oder vergleichbare Äquivalente) in der Sicherheitsleitlinie oder zugehörigen Richtlinien beschrieben und entsprechende Verantwortlichkeiten zugewiesen:

» IT-Leiter (CIO)

» IT-Sicherheitsbeauftragter (CISO)

» Beauftragter für die Behandlung von IT-Sicherheitsvorfällen (z. B. CERT-Leiter)

Veränderungen an Verantwortlichkeiten und Schnittstellen werden intern und extern so zeitnah kommuniziert, dass alle betroffenen internen und externen Parteien (z. B. Cloud-Kunden) mit organisatorischen und technischen Maßnahmen angemessen darauf reagieren können, bevor die Änderung wirksam wird.

Ergänzende Informationen zur Basisanforderung

Dokumentationen und Stellenprofile, welche die Zuständigkeiten im Rahmen der Informationssicherheit definieren und festlegen sollten vorliegen. Die Angemessenheit der Zuweisung von Rollen und Verantwortlichkeiten auf eine oder mehrere Personen beim Cloud-Anbieter ist vor dem Hintergrund der Größe und Komplexität seiner Organisation zu beurteilen.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Der Cloud-Anbieter identifiziert sämtliche Risiken im Zusammenhang mit überlappenden oder inkompatiblen Zuständigkeiten und Verantwortungen.

OIS-04 Funktionstrennung

Basisanforderung

Organisatorische und technische Kontrollen sind eingerichtet, um die Trennung von Rollen und Verantwortlichkeiten („Separation of Duties“/ Funktionstrennung), die hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der Cloud-Kunden nicht miteinander vereinbar sind, zu gewährleisten. Kontrollen zur Funktionstrennung sind insbesondere in den folgenden Bereichen eingerichtet:

» Administration von Rollen, Genehmigung und Zuweisung von Zugriffsberechtigungen für Benutzer unter Verantwortung des Cloud-Anbieters,

» Entwicklung und Implementierung von Änderungen am Cloud-Dienst,

» Wartung der für den Cloud-Dienst relevanten physischen und logischen IT-Infrastruktur (Netzwerke, Betriebssysteme, Datenbanken) und der IT-Anwendungen, soweit diese gemäß der vertraglichen Vereinbarungen mit dem Cloud-Kunden im Verantwortungsbereich des Cloud-Anbieters liegen.

Operative und kontrollierende Funktionen sollten nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Kann aus organisatorischen oder technischen Gründen keine Funktionstrennung erreicht werden, sind angemessene kompensierende Kontrollen eingerichtet, um missbräuchliche Aktivitäten zu verhindern oder aufzudecken.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Der Cloud-Anbieter hat vorhandene Funktionstrennungskonflikte und die dazu eingerichteten kompensierenden Kontrollen nachvollziehbar dokumentiert (z. B. in einem Rollen- und Rechtekonzept), um eine Beurteilung über die Angemessenheit und Wirksamkeit dieser Kontrollen zu ermöglichen.

OIS-05 Kontakt zu relevanten Behörden und Interessenverbänden

Basisanforderung

Angemessene und für den Cloud-Anbieter relevante Kontakte zu Behörden und Interessenverbänden sind etabliert, um stets über aktuelle Bedrohungslagen und Gegenmaßnahmen informiert zu sein.

Ergänzende Informationen zur Basisanforderung

Relevante Kontakte sind beispielsweise:

» Bundesamt für Sicherheit in der Informationstechnik (BSI)

» OWASP Foundation

» CERT-Verbünde DFN-CERT, TF-CSIRT etc.

Optionale, weitergehenden Anforderungen (Vertraulichkeit und Verfügbarkeit)

Es sind Verfahren definiert und dokumentiert, um die erhaltenen Informationen an die internen und externen Mitarbeiter des Cloud-Anbieters zu kommunizieren und zeitnah und angemessen darauf zu reagieren.

OIS-06 Richtlinie für die Organisation des Risikomanagements

Basisanforderung

Richtlinien und Anweisungen über das grundsätzliche Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Risiken und insbesondere IT-Risiken sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt.

OIS-07 Identifikation, Analyse, Beurteilung und Behandlung von Risiken

Basisanforderung

Die Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Risiken, einschließlich der für den Cloud-Dienst relevanten IT-Risiken, werden mindestens jährlich durchlaufen, um interne und externe Veränderungen und Einflussfaktoren zu berücksichtigen. Die identifizierten Risiken werden gemäß der Maßnahmen des Risikomanagements nachvollziehbar dokumentiert, bewertet und mit mitigierenden Maßnahmen versehen.

Ergänzende Informationen zur Basisanforderung

Soweit es sich beim Cloud-Anbieter um eine Aktiengesellschaft (AG) oder eine Kommanditgesellschaft auf Aktien (KGaA) handelt, findet § 91 Abs. 2 AktG Anwendung. Demnach hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Soweit diese Maßnahmen bereits Gegenstand einer Prüfung

durch einen Wirtschaftsprüfer waren, können diese Ergebnisse berücksichtigt werden. Dabei ist sicherzustellen, dass die für den Cloud-Dienst relevanten Risiken (i. d. R. IT-Risiken) Gegenstand des überprüften Überwachungssystems sind. Durch Auslagern von Geschäftsprozessen zur Entwicklung und/oder zum Betrieb des Cloud-Dienstes auf weitere Dienstleistungsunternehmen, verbleibt die Verantwortung für diese Risiken beim Cloud-Anbieter. Sie sind durch angemessene Verfahren zur Auswahl, Steuerung und Überwachung der Dienstleistungsunternehmen zu adressieren (vgl. Anforderungen DLL-01 und DLL-02).

Optionale, weitergehenden Anforderungen (Vertraulichkeit und Verfügbarkeit)

Vorgaben der Unternehmensleitung für den Risikoappetit und die Risikotoleranzen des Cloud-Anbieters sind in der Richtlinie für das Risikomanagement oder einem vergleichbaren offiziellen Dokument enthalten. Die zeitgerechte Implementierung der mitigierenden Maßnahmen wird durch qualifiziertes Personal des Cloud-Anbieters überwacht. Die Unternehmensleitung wird mindestens quartalsweise und in angemessener Form über den Status der identifizierten Risiken und mitigierender Maßnahmen informiert.

5.2 Sicherheitsrichtlinien und Arbeitsanweisungen

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

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

Basisanforderung

Von der Sicherheitsleitlinie abgeleitete Richtlinien und Anweisungen zur Informationssicherheit oder verwandter Themen sind nach einer einheitlichen Struktur dokumentiert. Sie werden sach- und bedarfsgerecht an alle internen und externen Mitarbeiter des Cloud-Anbieters kommuniziert und bereitgestellt. Leitlinien werden versioniert und von der Unternehmensleitung des Cloud-Anbieters freigegeben.

Die Richtlinien und Anweisungen beschreiben mindestens die folgenden Aspekte:

» Ziele,

» Geltungsbereiche,

» Rollen und Verantwortlichkeiten, einschließlich Anforderungen an die Qualifikation des Personals und das Einrichten von Vertretungsregelungen,

» die Koordination unterschiedlicher Unternehmensbereiche,

» Sicherheitsarchitektur und -maßnahmen zum Schutz von Daten, IT-Anwendungen und IT-Infrastrukturen, die durch den Cloud-Anbieter oder von Dritten verwaltet werden sowie

» Maßnahmen zur Einhaltung rechtlicher und regulatorischer Anforderungen (Compliance).

Ergänzende Informationen zur Basisanforderung

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 Basisanforderungen gefordert und an den angegebenen Stellen inhaltlich näher spezifiziert:

» Risikomanagement (OIS-06)

» Verwaltung von Datenträgern (AM-07)

» Wartung von Infrastruktur und Geräten (PS-05)

» Datensicherung und Wiederherstellung (RB-06)

» Protokollierung und Überwachung (RB- 10/ RB-11)

» Identifizieren von und Umgang mit Schwachstellen (RB-19)

» Verwaltung von Zugangs- und Zugriffsberechtigungen (IDM-01)

» Kryptographie und Schlüsselmanagement (KRY-01)

» Kommunikationssicherheit (KOS-05)

» Portabilität und Interoperabilität (PI-03)

» Beschaffung und Entwicklung von Cloud-Diensten (BEI-01)

» Change Management (BEI-03)

» Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister und Lieferanten des Cloud-Anbieters (DLL-01)

» Sicherstellung des Geschäftsbetriebes und Notfallmanagement (BCM-02)

» Sicherheit mobiler Endgeräte (MDM-01)

SA-02 Überprüfung und Freigabe von von Richtlinien und Anweisungen

Basisanforderung

Die Richtlinien und Anweisungen zur Informationssicherheit werden mindestens jährlich durch mit dem Thema vertraute Fachkräfte des Cloud-Anbieters hinsichtlich ihrer Angemessenheit und Wirksamkeit überprüft.

Die Überprüfung berücksichtigt mindestens

» organisatorische Änderungen beim Cloud-Anbieter,

» die aktuelle und zukünftig erwartete Bedrohungsumgebung in Bezug auf Informationssicherheit sowie

» rechtliche und technische Änderungen im Umfeld des Cloud-Anbieters.

Überarbeitete Richtlinien und Anweisungen werden durch hierzu autorisierten Gremien oder Stellen des Cloud-Anbieters genehmigt, bevor diese Gültigkeit erlangen.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Die regelmäßige Überprüfung wird durch zentrale Stellen beim Cloud-Anbieter nachgehalten.

SA-03 Abweichungen von bestehenden Richtlinien und Anweisungen

Basisanforderung

Ausnahmen von Richtlinien und Anweisungen zur Informationssicherheit werden durch hierzu autorisierten Gremien oder Stellen des Cloud-Anbieters in dokumentierter Form genehmigt. Die Angemessenheit genehmigter Ausnahmen und die Beurteilung der daraus entstehenden Risiken wird mindestens jährlich durch mit den Themen vertraute Fachkräfte des Cloud-Anbieters vor dem Hintergrund der aktuellen und zukünftig erwarteten Bedrohungsumgebung in Bezug auf die Informationssicherheit überprüft.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Die Angemessenheit genehmigter Ausnahmen und die Beurteilung der daraus entstehenden Risiken wird mindestens jährlich durch einen unabhängigen Dritten dahingehend überprüft, ob sie ein tatsächliches Bild der aktuellen und zukünftig erwarteten Bedrohungsumgebung in Bezug auf die Informationssicherheit wiedergibt (vgl. SPN-01).

5.3 Personal

Zielsetzung: Sicherstellen, dass Mitarbeiter, Dienstleister und Lieferanten 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 Sicherheitsüberprüfung der Hintergrundinformationen

Basisanforderung

Die Vergangenheit aller internen und externen Mitarbeiter des Cloud-Anbieters mit Zugriff auf Daten der Cloud-Kunden oder der geteilten IT-Infrastruktur 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

» Anfrage eines polizeilichen Führungszeugnisses bei sensiblen Positionen im Unternehmen

Ergänzende Informationen zur Basisanforderung

Die Überprüfung kann durch einen spezialisierten Dienstleister unterstützt werden. Haben Mitarbeiter eines Dienstleisters Zugriff auf die Nutzerdaten muss der Dienstleister gem. DLL-01 und DLL-02 diese Anforderung erfüllen und transparent machen.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Besondere Genehmigungsverfahren im Einstellungsprozess für Mitarbeiter und Positionen bei denen Zugriff auf besonders sensible Informationen besteht, sind etabliert.

HR-02 Beschäftigungsvereinbarungen

Basisanforderung

Beschäftigungsvereinbarungen beinhalten die Verpflichtungen der internen und externen Mitarbeiter des Cloud-Anbieters auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen in Bezug zur Informationssicherheit (vgl. KOS-10). Die Sicherheitsleitlinie sowie die davon abgeleiteten Richtlinien und Anweisungen zur Informationssicherheit sind den Unterlagen zur Beschäftigungsvereinbarung beigefügt. Deren Einhaltung wird durch den Mitarbeiter schriftlich bestätigt, bevor Zugriff auf Daten der Cloud-Kunden oder die (geteilte) IT-Infrastruktur möglich ist.

HR-03 Programm zur Sicherheitsausbildung und Sensibilisierung

Basisanforderung

Ein Programm zur zielgruppenorientierten Sicherheitsausbildung und Sensibilisierung zum Thema Informationssicherheit existiert und ist verpflichtend für alle internen und externen Mitarbeiter des Cloud-Anbieters. Das Programm wird regelmäßig in Bezug auf die gültigen Richtlinien und Anweisungen, den zugewiesenen Rollen und Verantwortlichkeiten sowie den bekannten Bedrohungen aktualisiert und ist dann erneut zu durchlaufen.

Das Programm umfasst mindestens die folgenden Inhalte:

» die regelmäßige und dokumentierte Unterweisung hinsichtlich der sicheren Konfiguration und des sicheren Betriebs der für den Cloud-Dienst erforderlichen IT-Anwendungen und IT-Infrastruktur, einschließlich mobiler Endgeräte,

» der angemessene Umgang mit Daten der Cloud-Kunden,

» die regelmäßige und dokumentierte Unterrichtung über bekannte Bedrohungen und

» das regelmäßige und dokumentierte Training des Verhaltens beim Auftreten sicherheitsrelevanter Ereignisse.

Externe Dienstleister und Lieferanten des Cloud-Anbieters, die zur Entwicklung oder Betrieb des Cloud-Dienstes beitragen, werden vertraglich verpflichtet ihre Mitarbeiter und Unterauftragnehmer auf die spezifischen Sicherheitsanforderungen des Cloud-Anbieters hinzuweisen und ihre Mitarbeiter allgemein zum Thema Informationssicherheit zu schulen.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Das Programm berücksichtigt verschiedene Profile und umfasst weiterführende Informationen für Positionen und Mitarbeiter die umfangreiche Berechtigungen oder Zugriff auf sensible Daten haben. Externen Mitarbeiter von Dienstleistern und Lieferanten des Cloud-Anbieters, die zur Entwicklung oder Betrieb des Cloud-Dienstes beitragen, werden in den spezifischen Sicherheitsanforderungen des Cloud-Anbieters sowie allgemein zum Thema Informationssicherheit unterwiesen. Der Cloud-Anbieter überprüft stichprobenartig, dass Dienstleister und Lieferanten die Unterweisung angemessen durchgeführt haben. Ergebnisse der Prüfung werden nachvollziehbar dokumentiert.

HR-04 Disziplinarmaßnahmen

Basisanforderung

Ein Prozess für die Durchführung von Disziplinarmaßnahmen ist implementiert und an die Mitarbeiter kommuniziert, um die Konsequenzen

von Verstößen gegen die gültigen Richtlinien und Anweisungen, sowie rechtliche Vorgaben und Gesetze transparent zu machen.

HR-05 Beendigung des Beschäftigungsverhältnisses oder Änderungen der Verantwortlichkeiten

Basisanforderung

Interne sowie externe Mitarbeiter sind darüber informiert, dass die Verpflichtungen auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen in Bezug zur Informationssicherheit auch bei einem Wechsel des Aufgabengebietes oder der Auflösung des Beschäftigungsverhältnisses bestehen bleiben.

5.4 Asset Management

Zielsetzung: Identifizieren der organisationseigenen Assets und der Verantwortlichen und gewährleisten eines angemessenen Schutzniveaus.

AM-01 Asset Inventar

Basisanforderung

Die zur Erbringung des Cloud-Dienstes eingesetzten Assets (z. B. PCs, Peripheriegeräte, Telefone, Netzwerkkomponenten, Server, Installationsdokumentationen, Verfahrensanweisungen, IT-Anwendungen, Werkzeuge) sind identifiziert und inventarisiert. Durch angemessene Prozesse und Maßnahmen wird sichergestellt, dass dieses Inventar vollständig, richtig, aktuell und konsistent bleibt. Änderungen an den Einträgen im Inventar werden nachvollziehbar historisiert. Soweit hierzu keine wirksamen Automatismen eingerichtet sind, wird dies durch eine mindestens monatlich stattfindende manuelle Überprüfung der Inventardaten des Assets sichergestellt.

Ergänzende Informationen zur Basisanforderung

Zu Asset-Management siehe auch die ISO-Normen 55001 und 55002.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Der Cloud-Anbieter kann bei einem Ausfall von Assets, die für die Verfügbarkeit des Cloud-Dienstes von wesentlicher Bedeutung sind (z. B. zentrale Netzwerkkomponenten), zeitnah erkennen, welche Cloud-Kunden davon betroffen sind, um eine der Dienstgütevereinbarung entsprechende Reaktion aufgetretene Störungen sicherzustellen. Durch technische Maßnahmen ist sichergestellt, dass sich das Inventar der Assets in regelmäßigen Abständen automatisch aktualisiert.

AM-02 Zuweisung von Asset Verantwortlichen

Basisanforderung

Sämtliche inventarisierten Assets sind einem Verantwortlichen auf Seiten des Cloud-Anbieters zugewiesen. Die Verantwortlichen des Cloud-Anbieters sind über den kompletten Lebenszyklus der Assets dafür zuständig, dass diese vollständig inventarisiert und richtig klassifiziert sind.

AM-03 Nutzungsanweisungen für Assets

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den ordnungsgemäßen Umgang mit Assets sind gemäß SA-01 dokumentiert, kommuniziert und der jeweils aktuellsten Version bereitgestellt.

AM-04 Ab- und Rückgabe von Assets

Basisanforderung

Alle internen und externen Mitarbeiter des Cloud-Anbieters sind verpflichtet sämtliche Assets, die Ihnen in Bezug auf den Cloud-Dienst ausgehändigt wurden bzw. für die sie verantwortlich sind, zurückzugeben oder unwiderruflich zu löschen sobald das Beschäftigungsverhältnis beendet ist.

AM-05 Klassifikation von Informationen

Basisanforderung

Der Cloud-Anbieter verwendet eine einheitliche Klassifizierung von Informationen und Assets, die für Entwicklung und Erbringung des Cloud-Dienstes relevant sind.

Ergänzende Informationen zur Basisanforderung

Die Klassifizierung von Informationen und Assets sollte u. a. folgende Angaben berücksichtigen:

» Kritikalität für die Erbringung des Cloud- Dienstes

» Sensibilität gegenüber unautorisierter Offenlegung oder Modifizierung

» Datentyp

» Anwendbare Rechtsordnung des Assets

» Geographische Lokation

» Kontext

» Rechtliche Einschränkungen

» Vertragliche Einschränkungen

» Wert

AM-06 Kennzeichnung von Informationen und Handhabung von Assets

Basisanforderung

Zu dem umgesetzten Klassifizierungsschema von Informationen und Assets existieren Arbeitsanweisungen und Prozesse, um die Kennzeichnung von Informationen, sowie die entsprechende Behandlung von Assets zu gewährleisten. Gemeint sind hier nur die Assets, die Informationen speichern oder verarbeiten.

Ergänzende Informationen zur Basisanforderung

Kennzeichnung (engl. Labeling) von Informationen ist im Nachgang zur Klassifizierung durchzuführen und liegt i. d. R. in der Verantwortung der Asset Owner. Eine Methode zur Kennzeichnung könnte eine Regelung für Dokumente sein, dass die Vertraulichkeitsstufe auf jeder Seite des Dokuments an der jeweils gleichen Stelle angegeben ist. Methoden zur Behandlung von Assets sollen Regelungen beinhalten, wie Assets gemäß jeder Vertraulichkeitsstufe zu schützen sind.

AM-07 Verwaltung von Datenträgern

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den sicheren Umgang mit Datenträgern aller Art sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben stellen einen Bezug zur Klassifikation von Informationen her (vgl. AM-05). Sie umfassen die sichere Verwendung, den sicheren Transport sowie die unwiederbringliche Löschung und Vernichtung von Datenträgern.

Ergänzende Informationen zur Basisanforderung

Richtlinien und Anweisungen sollten folgende Aspekte berücksichtigen:

» Sichere und unwiderrufliche Löschung der Daten und Entsorgung/Vernichtung der Datenträger,

» Verschlüsselung von Wechseldatenträgern,

» Übertragung der Daten auf neue Datenträger bei Austausch eines Mediums.

AM-08 Überführung und Entfernung von Assets

Basisanforderung

Geräte, Hardware, Software oder Daten dürfen nur nach erfolgter Genehmigung durch autorisierten Gremien oder Stellen des Cloud-Anbieters in externe Räumlichkeiten überführt werden. Die Überführung findet auf sicherem Wege statt, entsprechend der Art des zu überführenden Assets.

5.5 Physische Sicherheit

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

PS-01 Perimeterschutz

Basisanforderung

Die Begrenzungen von Räumlichkeiten oder Gebäuden, die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur beherbergen, sind physisch solide und durch angemessene Sicherheitsmaßnahmen geschützt, die dem Stand der Technik entsprechen.

Ergänzende Informationen zur Basisanforderung

Mögliche Sicherheitsmaßnahmen könnten beispielsweise Zäune, Mauern, Sicherheitspersonal oder Videoüberwachung sein. Bei den äußeren Türen und Fenstern sollte einbruchhemmendes Material (z. B. nach DIN EN 1627 Widerstandsklasse RC 2) und entsprechende Schließvorrichtungen verbaut sein.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Das Sicherheitskonzept beinhaltet die Einrichtung von verschiedenen Sicherheitszonen, die durch Sicherheitslinien als überwachte und gesicherte Übergänge zwischen den Zonen getrennt sind.

PS-02 Physische Zutrittskontrolle

Basisanforderung

Zugänge zu Räumlichkeiten oder Gebäuden die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur beherbergen, sind durch physische Zutrittskontrollen gesichert und überwacht, um unbefugten Zutritt zu verhindern.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Die physischen Zutrittskontrollen erfordern eine Zwei-Faktor-Authentifizierung.

PS-03 Schutz vor Bedrohungen von außen und aus der Umgebung

Basisanforderung

Räumlichkeiten oder Gebäude die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur beherbergen, sind durch bauliche, technische und organisatorische Maßnahmen vor Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und andere Formen natürlicher und von Menschen verursachter Bedrohungen geschützt.

An zwei georedundanten Standorten sind mindestens die folgenden Maßnahmen getroffen:

Bauliche Maßnahmen:

» Einrichtung eines eigenen Brandabschnitts für das Rechenzentrum

» Verwendung feuerbeständiger Materialien gemäß DIN 4102-1 oder EN 13501 (Feuerwiderstandsdauer von mindestens 90 Minuten)

Technische Maßnahmen:

» Sensoren zum Überwachen von Temperatur und Luftfeuchtigkeit

» Aufschalten des Gebäudes an einer Brandmeldeanlage mit Meldung an die örtliche Feuerwehr

» Brandfrüherkennungs- und Löschanlage

Organisatorische Maßnahmen:

» Regelmäßige Brandschutzübungen und Brandschutzbegehungen, um die Einhaltung der Brandschutzmaßnahmen zu prüfen

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Es findet eine Überwachung der Umgebungsparameter statt. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an die dafür zuständigen Stellen weitergeleitet.

PS-04 Schutz vor Unterbrechungen durch Stromausfälle und andere derartige Risiken

Basisanforderung

Dem Ausfall von Versorgungsleistungen wie Strom, Kühlung oder Netzanbindungen wird durch geeignete Maßnahmen und Redundanzen, in Abstimmung mit den Maßnahmen zur Betriebssicherheit, vorgebeugt. Versorgungsleitungen für Strom und Telekommunikation, welche Daten transportieren oder Informationssysteme versorgen, sind vor Abhören und Beschädigung geschützt.

Ergänzende Informationen zur Basisanforderung

Geeignete Maßnahmen zur Ausfallvorsorge umfassen typischerweise:

» Redundante Stromversorgung und Klimaanlagen

» Einsatz von angemessen dimensionierten unterbrechungsfreien Stromversorgungen (USV) und Netzersatzanlagen (NEA)

» Redundante Netzwerkanbindung über unterschiedliche physische Anbindungen

Darüber hinaus sollte der Cloud-Anbieter ermitteln und kommunizieren, welche externen Temperaturen die Klimatisierung des Rechenzentrums wie lange aushalten (also z. B. 30 °C/14 Tage, 35 °C/6 Tage, 40 °C/4 Tage). Soweit mit Flusswasser gekühlt, sollte angegeben werden, bei welchen Wasserständen die Klimatisierung wie lange aufrechterhalten werden kann. Zum Nachweis über die Abhörsicherheit und dem Beschädigungsschutz können Verkabelungspläne und ein entsprechendes Schutzkonzept vorgelegt werden, das in Gesprächen mit dem Verantwortlichen

plausibilisiert wird. Bei einer Sichtprüfung ist u. a. auf 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 sowie auf unzulässige Einbauten und Veränderungen zu achten.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Es findet eine Überwachung der Versorgungsleistungen statt. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an die dafür zuständigen Stellen weitergeleitet. Der Cloud-Anbieter ermittelt und kommuniziert die Autark-Zeiten, die durch die getroffenen Maßnahmen bei Ausfall der Versorgungsleistungen oder beim Eintritt von außergewöhnlichen Ereignissen (z. B. Hitzeperioden, länger anhaltender Stromausfall) erreicht werden sowie die maximal tolerierbaren Zeiten für einen Ausfall der Versorgungsleistungen. Verträge für die Aufrechterhaltung der Notfallversorgung mit entsprechenden Dienstleistern sind abgeschlossen (z. B. für den Treibstoff der Notstromversorgung).

PS-05 Wartung von Infrastruktur und Geräten

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, welche die Wartung (insbesondere Fernwartung), Löschung, Aktualisierung und Wiederverwendung von Assets in der Informationsverarbeitung in ausgelagerten Räumlichkeiten oder durch externes Personal beschreiben.

Ergänzende Informationen zur Basisanforderung

Richtlinien und Anweisungen sollten folgende Aspekte berücksichtigen:

» die sichere Löschung von sensiblen Daten vor einer externen Reparatur oder Wartung,

» Analysen der Assets vor der Wiederverwendung um Manipulationen oder Fehlfunktionen zu vermeiden,

» Erneuerung von Assets, sofern Verfügbarkeit, Sicherheit, Integrität oder Vertraulichkeit gefährdet sein könnten.

5.6 Regelbetrieb

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.

RB-01 Kapazitätsmanagement – Planung

Basisanforderung

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.

Ergänzende Informationen zur Basisanforderung

Aus Wirtschaftlichkeitsgründen streben Cloud-Anbieter typischerweise eine hohe Auslastung der IT-Ressourcen (CPU, Arbeitsspeicher, Speicherplatz, Netzwerk) an. In Multi-Mandanten-Umgebungen müssen die vorhandenen Ressourcen zwischen den Cloud-Nutzern (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, müssen die Verfahren im Rahmen dieser Prüfung mindestens mündlich erläutert werden können.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

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

RB-02 Kapazitätsmanagement – Überwachung

Basisanforderung

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 der vertraglichen Vereinbarungen erbracht werden und die Einhaltung der Dienstgütevereinbarungen sichergestellt ist.

Ergänzende Informationen zur Basisanforderung

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.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

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

RB-03 Kapazitätsmanagement – Datenlokation

Basisanforderung

Der Cloud-Kunde ist in der Lage die Lokationen (Ort/Land) der Datenverarbeitung und -speicherung einschl. der Datensicherungen festzulegen.

Ergänzende Informationen zur Basisanforderung

Diese Anforderung ergänzt Anforderung UP-02, in der die Lokationen dokumentiert werden sollen. Erbringt ein Cloud-Anbieter seine Dienste an mehreren Standorten, dann fragt diese Anforderung danach, ob der Cloud-Anbieter genau festlegen kann, an welchem Standort der Dienst erbracht und die Daten prozessiert werden.

RB-04 Kapazitätsmanagement – Steuerung von Ressourcen

Basisanforderung

Der Cloud-Kunde ist bei IaaS/PaaS in der Lage die Aufteilung der ihm zur Verwaltung/Nutzung zugeordneten Systemressourcen (z. B. Rechen- oder Speicherkapazität) zu steuern und zu überwachen, um eine Überbelegung der Ressourcen zu vermeiden.

RB-05 Schutz vor Schadprogrammen

Basisanforderung

Die logischen und physischen IT-Systeme, die der Cloud-Anbieter zur Entwicklung- und Erbringung des Cloud-Dienstes verwendet sowie die Perimeter des Netzwerks, die dem Verantwortungsbereich des Cloud-Anbieters unterliegen, sind mit Viren-Schutz- und Reparaturprogrammen versehen, die eine signatur- und verhaltensbasierte Erkennung und Entfernung von Schadprogrammen ermöglichen. Die Programme werden gemäß den vertraglichen Vereinbarungen mit dem/n Hersteller/n, mindestens aber täglich aktualisiert.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Der Cloud-Anbieter erstellt regelmäßige Reports über die durchgeführten Überprüfungen, welche durch autorisierte Stellen 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.

RB-06 Datensicherung und Wiederherstellung – Konzept

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zum Vermeiden von Datenverlusten sind sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Diese sehen zuverlässige Verfahren für die regelmäßige Sicherung (Backup sowie ggf. Snapshots) und Wiederherstellung von Daten (Restore) vor. Umfang, Häufigkeit und Dauer der Aufbewahrung entsprechen den vertraglichen Vereinbarungen mit den Cloud-Kunden sowie den geschäftlichen Anforderungen des Cloud-Anbieters. Der Zugriff auf die gesicherten Daten ist auf autorisiertes Personal beschränkt. Wiederherstellungsprozeduren beinhalten Kontrollmechanismen die sicherstellen, dass Wiederherstellungen ausschließlich nach Genehmigung durch hierfür autorisierte Personen gemäß den vertraglichen Vereinbarungen mit den Cloud-Kunden oder den internen Richtlinien des Cloud-Anbieters erfolgen.

Ergänzende Informationen zur Basisanforderung

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. Kontrolle 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 Anforderungskatalog 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.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Die Datensicherung erfolgt in verschlüsselter Form, die dem aktuellen Stand der Technik entspricht.

RB-07 Datensicherung und Wiederherstellung – Überwachung

Basisanforderung

Die Ausführung der Datensicherung wird durch technische und organisatorische Maßnahmen überwacht. Störungen werden durch qualifizierte Mitarbeiter untersucht und zeitnah behoben, um die Einhaltung der vertraglichen Verpflichtungen gegenüber den Cloud-Kunden oder den geschäftlichen Anforderungen des Cloud-Anbieters in Bezug auf Umfang, Häufigkeit und Dauer der Aufbewahrung zu gewährleisten.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

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

RB-08 Datensicherung und Wiederherstellung – Regelmäßige Tests

Basisanforderung

Sicherungsdatenträger und Wiederherstellungsverfahren sind von qualifizierten Mitarbeitern regelmäßig mit dedizierten Testmedien zu prüfen. Die Tests sind so gestaltet, dass die Verlässlichkeit der Sicherungsdatenträger und die Wiederherstellungszeit mit hinreichender Sicherheit überprüft werden kann. Die Tests werden durch qualifizierte Mitarbeiter durchgeführt und die Ergebnisse nachvollziehbar dokumentiert. Auftretende Fehler werden zeitnah behoben.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

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

RB-09 Datensicherung und Wiederherstellung – Aufbewahrung

Basisanforderung

Zu sichernde Daten werden an einen Remote-Standort (z. B. weiteres Rechenzentrum des Cloud-Anbieters) übertragen oder auf Sicherungsdatenträgern an einem Remote-Standort transportiert. Soweit die Datensicherung über ein Netzwerk zum Remote-Standort übertragen wird, erfolgt dies in einer verschlüsselten Form, die dem Stand der Technik entspricht. Die Entfernung zum Hauptstandort ist hinreichend gewählt, dass dortige Katastrophen zu keinem Datenverlust am Remote-Standort führen und gleichzeitig gering genug, um die vertraglichen Verpflichtungen zu Wiederherstellungszeiten erfüllen zu können. Die Maßnahmen zur physischen und umgebungsbezogenen Sicherheit am Remote-Standort entsprechen dem Niveau am Hauptstandort.

RB-10 Protokollierung und Überwachung – Konzept

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um Ereignisse auf allen Assets, die zur Entwicklung oder Betrieb des Cloud-Dienstes verwendet werden, zu protokollieren und an zentraler Stelle aufzubewahren. Die Protokollierung umfasst definierte Ereignisse, welche die

Sicherheit und Verfügbarkeit des Cloud-Dienstes beeinträchtigen können, einschließlich einer Protokollierung des Aktivierens, Stoppens und Pausierens der verschiedenen Protokollierungen. Die Protokolle werden bei unerwarteten oder auffälligen Ereignissen durch autorisiertes Personal anlassbezogen überprüft, um eine zeitnahe Untersuchung von Störungen und Sicherheitsvorfällen sowie das Einleiten geeigneter Maßnahmen zu ermöglichen.

Ergänzende Informationen zur Basisanforderung

Sicherheitsrelevante Ereignisse sind u. a.

» An- und Abmeldevorgänge

» Erstellung, Änderung oder Löschung von Benutzern und Erweiterung der Berechtigungen

» Verwendung, Erweiterung und Änderungen von privilegierten Zugriffsberechtigungen

» Nutzung von temporären Berechtigungen

Da es sich bei den protokollierten Daten i. d. R. um personenbezogene Daten handelt, sind in dem Fall datenschutzrechtliche Anforderungen an die Aufbewahrung zu beachten und zu überprüfen. Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

RB-11 Protokollierung und Überwachung – Metadaten

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zur sicheren Handhabung von Metadaten (Nutzungsdaten) sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Sammlung und Benutzung von Metadaten erfolgt ausschließlich für Abrechnungszwecke, zum Beheben von Störungen und Fehlern (Incident Management) sowie zum Bearbeiten von Sicherheitsvorfällen (Security Incident Management). Eine kommerzielle Nutzung der Metadaten findet nicht statt. Metadaten sind unverzüglich zu löschen, wenn sie zur Erreichung des, gemäß dieser Anforderung legitimen, Zwecks nicht mehr erforderlich sind. Der Zeitraum, in dem Metadaten gespeichert werden, ist vom Cloud-Anbieter festgelegt. Er steht im angemessenen Zusammenhang mit den Zwecken, die mit der Sammlung der Metadaten verfolgt werden.

Ergänzende Informationen zur Basisanforderung

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 der Anforderung soll die Sammlung und Nutzung der Metadaten transparent und klar eingegrenzt werden.

RB-12 Protokollierung und Überwachung – Kritische Assets

Basisanforderung

Der Cloud-Anbieter führt eine Liste aller protokollierungs- und überwachungskritischen Assets und überprüft diese Liste regelmäßig auf deren Aktualität und Korrektheit. Für diese kritischen Assets wurden erweiterte Protokollierungs- und Überwachungsmaßnahmen definiert.

RB-13 Protokollierung und Überwachung – Aufbewahrung der Protokolle

Basisanforderung

Die erstellten Protokolle werden auf zentralen Protokollierungsservern aufbewahrt, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind. Protokolldaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks

nicht mehr erforderlich sind. Zwischen den Protokollierungsservern und den protokollierten 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).

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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 und der technisch Realisierbarkeit wird eine logische oder eine physikalische Trennung von Protokoll- und Nutzdaten vorgenommen.

RB-14 Protokollierung und Überwachung – Zurechenbarkeit

Basisanforderung

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

Ergänzende Informationen zur Basisanforderung

Das Protokoll sollte die folgenden Angaben enthalten:

» Benutzer ID

» Datum und Zeit

» Quelle & Ziel (z. B. Identität oder Name der betroffenen Daten, Systemkomponenten oder Ressourcen)

» durchgeführte Aktivitäten

» Angaben über Erfolg oder Fehlschlag des Zugriffs

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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.

RB-15 Protokollierung und Überwachung – Konfiguration

Basisanforderung

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten ist beschränkt auf ausgewählte und autorisierte Mitarbeiter des Cloud-Anbieters. Änderungen der Protokollierungen und Überwachungen werden vorab durch unabhängige und autorisierte Mitarbeiter überprüft und freigegeben.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten erfordert eine Multi-Faktor-Authentifizierung.

RB-16 Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software

Basisanforderung

Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware wird unabhängig überwacht. Bei einem Ausfall der Protokollierungs- und Überwachungssoftware werden die verantwortlichen Mitarbeiter umgehend informiert.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Die Protokollierungs- und Überwachungssoftware ist redundant vorhanden, um auch bei Ausfällen die Sicherheit und Verfügbarkeit der Kunden-Systeme zu überwachen.

RB-17 Umgang mit Schwachstellen, Störungen und Fehlern – Konzept

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um das zeitnahe Identifizieren und Adressieren von Schwachstellen über alle Ebenen des Cloud-Dienstes, die unter seiner Verantwortung stehen, zu gewährleisten. Die Maßnahmen umfassen unter anderem:

» Regelmäßiges Identifizieren und Analysieren von Schwachstellen (Vulnerabilities),

» Regelmäßiges Nachhalten von Maßnahmen zum Adressieren identifizierter Maßnahmen (z. B. Einspielen von Sicherheitsaktualisierungen gemäß interner Zielvorgaben).

RB-18 Umgang mit Schwachstellen, Störungen und Fehlern – Penetrationstests

Basisanforderung

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 den sicheren Betrieb des Cloud-Dienstes als kritisch definierten Infrastruktur-Komponenten, die im Rahmen einer Risiko-Analyse als solche identifiziert wurden. Art, Umfang Zeitpunkt/Zeitraum und Ergebnisse werden für einen sachverständigen Dritten nachvollziehbar dokumentiert. Feststellungen aus den Penetrationstests werden bewertet und bei mittlerer oder hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit des Cloud-Dienstes nachverfolgt und behoben. Die Einschätzung der Kritikalität und der mitigierenden Maßnahmen zu den einzelnen Feststellungen werden dokumentiert.

Ergänzende Informationen zur Basisanforderung

Die Schwachstellen sollten gemäß Schadenpotenzial klassifiziert sein und einen Zeitraum für die erforderliche Reaktion nennen. Als Orientierung kann die folgende Einstufung gemäß der SI-Publikation „Ein Praxis-Leitfaden für IS-Penetrationstests“ dienen:

» **Hoch:** Sofortige Reaktion

» **Mittel:** Kurzfristige Reaktion

» **Niedrig:** Mittelfristige Reaktion

» **Information:** Langfristige Reaktion

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

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

RB-19 Umgang mit Schwachstellen, Störungen und Fehlern – Integration mit Änderungs- und Incident Management

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den Umgang mit kritischen Schwachstellen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Maßnahmen sind mit den Aktivitäten des Änderungsverfahrens (Change Management) und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt.

RB-20 Umgang mit Schwachstellen, Störungen und Fehlern – Einbindung des Cloud-Kunden

Basisanforderung

Der Cloud-Kunde wird durch den Cloud-Anbieter regelmäßig und in einer angemessener Form, die den vertraglichen Vereinbarungen entspricht, über den Status der ihn betreffenden Störungen (Incidents) informiert oder in deren Behebung eingebunden. Sobald ein Incident aus Sicht des Cloud-Anbieters behoben wurde, wird der Cloud-Kunde über die getroffenen Maßnahmen informiert. Diese Information ist so detailliert, dass der Cloud-Kunde sie in seinem Sicherheitsmanagement verwenden kann.

RB-21 Umgang mit Schwachstellen, Störungen und Fehlern – Prüfung offener Schwachstellen

Basisanforderung

Die IT-Systeme, welche der Cloud-Anbieter für die Entwicklung und Erbringung des Cloud-Dienstes verwendet, werden mindestens monatlich automatisiert auf bekannte Schwachstellen (Vulnerabilities) geprüft. Im Falle von Abweichungen zu den erwarteten Konfigurationen (u. a. dem erwarteten Patch-Level) werden die Gründe hierzu zeitnah analysiert und die Abweichungen behoben oder gemäß des Ausnahme-Prozesses dokumentiert (vgl. SA-03).

Ergänzende Informationen zur Basisanforderung

Im Gegensatz zu Penetrationstests (vgl. RB-18), die manuell und nach einem individuellem Schema ablaufen, erfolgt die Prüfung auf offene Schwachstellen automatisiert, unter Verwendung sog. Vulnerability Management Werkzeuge.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Auf Kundenwunsch informiert der Cloud-Anbieter den Cloud-Kunden in angemessener Form über offene Schwachstellen. Die offenen Schwachstellen werden ohne Ausnahme zeitnah behoben.

RB-22 Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung

Basisanforderung

Systemkomponenten, welche für die Erbringung des Cloud-Dienstes verwendet werden, sind gemäß allgemein etablierter und akzeptierter Industriestandards gehärtet. Die herangezogenen Härtungsanleitungen werden ebenso wie der Umsetzungsstatus dokumentiert.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Auf Nachfrage sind die verwendeten Standards und die Maßnahmen zur Härtung der Systemkomponenten dem Cloud-Kunden mitzuteilen.

RB-23 Segregation der gespeicherten und verarbeiteten Daten der Cloud-Kunden in gemeinsam genutzten Ressourcen

Basisanforderung

Daten sind auf gemeinsam genutzten virtuellen und physischen Ressourcen (Speichernetz, Arbeitsspeicher) gemäß eines dokumentierten Konzepts sicher und strikt separiert, um die Vertraulichkeit und Integrität der gespeicherten und verarbeiteten Daten zu gewährleisten.

Ergänzende Informationen zur Basisanforderung

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 Masking) 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. Penetrationstests zur Validierung des Konzepts). Die Segregation übertragener Daten ist Gegenstand der Kontrolle KOS-05.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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

5.7 Identitäts- und Berechtigungsmanagement

Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i. d. R. privilegierte Benutzer) und des Cloud-Kunden zum Vermeiden von unberechtigtem Zugriff.

IDM-01 Richtlinie für Zugangs- und Zugriffsberechtigungen

Basisanforderung

Ein auf den Geschäfts- und Sicherheitsanforderungen des Cloud-Anbieters basierendes Rollen- und Rechtekonzept sowie eine Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt und adressieren die folgenden Bereiche:

- die Vergabe und Änderung (Provisionierung) von 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 („Separation of Duties“),
- Funktionstrennung in der Administration von Rollen, Genehmigung und Zuweisung von Zugriffsberechtigungen,
- regelmäßige Überprüfung vergebener Berechtigungen,
- Berechtigungsentzug (Deprovisionierung) bei Veränderungen des Arbeitsverhältnisses,
- Anforderungen an Genehmigung und Dokumentation der Verwaltung von Zugangs- und Zugriffsberechtigungen.

IDM-02 Benutzerregistrierung

Basisanforderung

Zugangsberechtigungen für Benutzer unter Verantwortung des Cloud-Anbieters (interne und externe Mitarbeiter) werden in einem formalen Verfahren erteilt. Organisatorische und/oder technische Maßnahmen stellen sicher, dass eindeutige Benutzerkennungen vergeben werden, die jeden Benutzer eindeutig identifizieren.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Der Cloud-Anbieter bietet Möglichkeiten des Self-Services für Cloud-Kunden an, um Benutzerkennungen eigenständig erteilen zu können.

IDM-03 Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen

Basisanforderung

Vergabe und Änderung von Zugriffsberechtigungen für Benutzer unter Verantwortung des Cloud-Anbieters erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Organisatorische und/oder technische Maßnahmen stellen sicher, dass die vergebenen Zugriffe die folgenden Anforderungen erfüllen:

» Zugriffsberechtigungen entsprechen dem Prinzip der geringsten Berechtigung („Least-Privilege-Prinzip“),

» Zugriffsberechtigungen werden nur so vergeben, wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“),

» die formale Genehmigung erfolgt durch eine autorisierte Person, bevor die Zugriffsberechtigungen eingerichtet werden (d. h. bevor der Benutzer auf Daten der Cloud-Kunden oder Komponenten der geteilten IT-Infrastruktur zugreifen kann),

» die technisch zugewiesenen Zugriffsberechtigungen die formale Genehmigung nicht übersteigen.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Der Cloud-Anbieter bietet Möglichkeiten des Self-Services für Cloud-Kunden an, um Zugriffsberechtigungen eigenständig vergeben und ändern zu können.

IDM-04 Berechtigungsentzug (Deprovisionierung) bei Veränderungen des Arbeitsverhältnisses

Basisanforderung

Zugriffsberechtigungen von Benutzern unter Verantwortung des Cloud-Anbieters (interne und externe Mitarbeiter) werden bei Änderungen im Beschäftigungsverhältnis (Kündigung, Versetzung, längerer Abwesenheit/Sabatical/Elternzeit) zeitnah, spätestens aber 30 Tage nach Inkrafttreten entzogen bzw. vorübergehend ruhe stellend gesetzt. Zugänge werden vollständig deaktiviert sobald das Beschäftigungsverhältnis erlischt.

IDM-05 Regelmäßige Überprüfung der Zugriffsberechtigungen

Basisanforderung

Zugriffsberechtigungen von Benutzern unter Verantwortung des Cloud-Anbieters (interne und externe Mitarbeiter) werden mindestens jährlich überprüft, um diese zeitnah auf Änderungen im Beschäftigungsverhältnis (Kündigung, Versetzung, längerer Abwesenheit/Sabatical/Elternzeit) anzupassen. Die Überprüfung erfolgt durch hierzu autorisierte Personen aus den Unternehmensbereichen des Cloud-Anbieters, die aufgrund ihres Wissens über die Zuständigkeiten die Angemessenheit der vergebenen Berechtigungen überprüfen können. Die Überprüfung sowie die sich daraus ergebenden Berechtigungsanpassungen werden nachvollziehbar dokumentiert.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Administrative Berechtigungen werden mindestens halbjährlich überprüft.

IDM-06 Administratorenberechtigungen

Basisanforderung

Vergabe und Änderung von Zugriffsberechtigungen für interne und externe Benutzer mit administrativen oder weitreichenden Berechtigungen unter Verantwortung des Cloud-Anbieters erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen (vgl. IDM-01) oder einer separaten Richtlinie. Die Zuweisung erfolgt personalisiert und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“). Organisatorische und/oder technische Maßnahmen stellen sicher, dass durch die Vergabe dieser Berechtigungen keine ungewollten, kritischen Kombinationen entstehen, die gegen das Prinzip der Funktionstrennung verstoßen (z. B. Zuweisen von Berechtigungen zur Administration der Datenbank wie auch des Betriebssystems). Soweit dies in ausgewählten Fällen nicht möglich ist, sind angemessene, kompensierende Kontrollen eingerichtet, um einen Missbrauch dieser Berechtigungen zu identifizieren (z. B. Protokollierung und Überwachung durch eine SIEM-Lösung (Security Information and Event Management)).

IDM-07 Geheimhaltung von Authentifizierungsinformationen

Basisanforderung

Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an interne und externe Benutzer des Cloud-Anbieters oder des Cloud-Kunden erfolgt, soweit dies organisatorischen oder technischen Verfahren des Cloud-Anbieters unterliegt, in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt. Soweit diese initial vergeben werden, sind diese nur temporär, höchstens aber 14 Tage gültig. Benutzer werden ferner gezwungen, diese bei der ersten Verwendung zu ändern. Der Zugriff des Cloud-Anbieters auf Authentifizierungsinformationen der Cloud-Kunden ist streng reglementiert, mit dem Cloud-Kunden kommuniziert und erfolgt nur, wenn es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“). Die Zugriffe werden dokumentiert und dem Cloud-Kunden mitgeteilt.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Die Benutzer unterschreiben eine Erklärung, in der sie versichern, dass sie persönliche (oder geteilte) Authentisierungsinformationen vertraulich behandeln und ausschließlich für sich (innerhalb der Mitglieder der Gruppe) behalten.

IDM-08 Sichere Anmeldeverfahren

Basisanforderung

Die Vertraulichkeit der Anmeldeinformationen von internen und externen Benutzern unter Verantwortung des Cloud-Anbieter sind durch die folgenden Maßnahmen geschützt:

» Identitätsprüfung durch vertrauenswürdige Verfahren,

» Verwendung anerkannter Industriestandards zur Authentifizierung und Autorisierung (z. B. Multi-Faktor-Authentifizierung, keine Verwendung von gemeinsam genutzten Authentifizierungsinformationen, automatischer Ablauf),

» Multi-Faktor-Authentifizierung für Administratoren des Cloud-Anbieters (z. B. durch Smart Card oder biometrische Merkmale) ist zwingend erforderlich.

IDM-09 Umgang mit Notfallbenutzern

Basisanforderung

Die Verwendung von Notfallbenutzern (für Aktivitäten, die mit personalisierten, administrativen Benutzern nicht durchgeführt werden können, vgl. IDM-06) ist dokumentiert, zu begründen und bedarf der Genehmigung durch eine autorisierte Person, die unter Berücksichtigung des Prinzips der Funktionstrennung zu erfolgen hat. Die

Freischaltung des Notfallbenutzers erfolgt nur so lange, wie es für die Aufgabenwahrnehmung notwendig ist.

Ergänzende Informationen zur Basisanforderung

Die Genehmigung kann auch nachträglich erfolgen, soweit dies begründet wird.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Mindestens monatlich wird ein manueller Abgleich zwischen den erfolgten Freischaltungen der Notfallbenutzer und den entsprechenden Genehmigungen durchgeführt. Auffälligkeiten werden untersucht, um Missbrauch dieser Benutzer festzustellen und zukünftig zu verhindern. Die Aktivitäten der Notfallbenutzer werden revisionssicher protokolliert. Die Protokollierung ist hinreichend detailliert, um es einem sachverständigen Dritten zu ermöglichen die Aktivitäten nachzuvollziehen.

IDM-10 Systemseitige Zugriffskontrolle

Basisanforderung

Der Zugriff auf Informationen und Anwendungs-Funktionen wird durch technische Maßnahmen eingeschränkt, mit denen das Rollen- und Rechtekonzept umgesetzt wird.

IDM-11 Passwortanforderungen und Validierungsparameter

Basisanforderung

Sicherheits-Parameter auf Netzwerk,- Betriebssystem- (Host und Gast), Datenbank-, und Anwendungsebene (soweit für den Cloud-Dienst relevant) sind angemessen konfiguriert, um unautorisierte Zugriffe zu verhindern. Soweit keine Zwei-Faktor-Authentifizierung oder die Verwendung von Einmalpasswörtern möglich ist, wird die Verwendung sicherer Passwörter auf allen Ebenen und Geräten (einschl. mobilen Endgeräten) unter Verantwortung des Cloud-Anbieters technisch erzwungen oder in einer Passwort-Richtlinie organisatorisch gefordert. Die Vorgaben müssen mindestens die folgenden Anforderungen erfüllen:

» Minimale Passwortlänge von 8 Zeichen,

» Mindestens zwei der folgenden Zeichentypen müssen enthalten sein: Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen,

» Maximale Gültigkeit von 90 Tagen, minimale Gültigkeit von 1 Tag,

» Passworthistorie von 6,

» Übertragung und Speicherung der Passwörter in einem verschlüsselten Verfahren, das dem aktuellen Stand der Technik entspricht.

Ergänzende Informationen zur Basisanforderung

Sicherheitsparameter umfassen z. B. die Verwendung sicherer Anmeldeverfahren (vgl. IDM-08), Sperre nach fehlgeschlagenen Anmeldungen, keine Mehrfachanmeldungen mit dem gleichen Benutzer, automatische Abmeldung/Sperre nach Inaktivität).

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Automatische Kontrollen sind implementiert, die sich an den folgenden Regelungen orientieren:

» es erfolgt eine Sperrung von 15 Minuten nach 5 fehlgeschlagenen Anmeldungen, mit jedem Fehlversuch steigt die Wartezeit,

» eine Mehrfachanmeldung des gleichen Benutzer ist nicht möglich,

» nach Anmeldung erfolgt eine automatische Sperre nach 15 Minuten Inaktivität,

» die minimale Passwortlänge für privilegierte Benutzer beträgt 14 Zeichen und für Benutzer ohne weitreichende Berechtigungen 8 Zeichen,

» es müssen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen enthalten sein,

» nach 90 Tagen wird der Passwortwechsel bei der nächsten Anmeldung erzwungen,

» die Passworthistorie beträgt 12.

IDM-12 Einschränkung und Kontrolle administrativer Software

Basisanforderung

Die Verwendung von Dienstprogrammen und Managementkonsolen (z. B. zur Verwaltung des Hypervisors oder virtuellen Maschinen), die weitreichenden Zugriff auf die Daten der Cloud-Kunden ermöglichen, ist auf autorisierte Personen beschränkt. Vergabe und Änderung entsprechender Zugriffsberechtigungen erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Der Zugriff wird durch starke Authentifizierungstechniken, einschließlich Multi-Faktor-Authentifizierung gesteuert (vgl. KOS-06).

IDM-13 Zugriffskontrolle zu Quellcode

Basisanforderung

Der Zugriff auf den Quellcode und ergänzende für die Entwicklung des Cloud-Dienstes relevante Informationen (z. B. Architektur-Dokumentation, Testpläne) sind restriktiv vergeben und werden überwacht, um die Einführung von nicht autorisierten Funktionen oder das Durchführen unbeabsichtigter Änderungen zu vermeiden.

5.8 Kryptographie und Schlüsselmanagement

Zielsetzung: Gewährleisten einer angemessenen und effektiven Verwendung von Kryptographie zum Schutz der Sicherheit von Informationen.

KRY-01 Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung

Basisanforderung

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

» die Nutzung von starker Verschlüsselungsverfahren (z. B. AES) und die Verwendung von sicheren Netzwerkprotokollen, die dem Stand der Technik entsprechen (z. B. TLS, IPsec, SSH),

» risikobasierte Vorschriften für den Einsatz von Verschlüsselung die mit Schemata zur Informationsklassifikation abgeglichen sind und den Kommunikationskanal, 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.

Ergänzende Informationen zur Basisanforderung

Der Stand der Technik bezüglich starker Verschlüsselungsverfahren und sichere Netzwerkprotokolle 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)“

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

Basisanforderung

Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung bei der Übertragung von Daten der Cloud-Kunden (z. B. über öffentliche Netze transportierte elektronische Nachrichten) sind etabliert.

Ergänzende Informationen zur Basisanforderung

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 Netzwerke erfolgt. In diesem Fall kann die nicht-öffentliche Umgebung des Cloud-Anbieters grundsätzlich als vertrauenswürdig angesehen werden kann. Als starke Transportverschlüsselung, die dem Stand der Technik entspricht, wird aktuell das Protokoll TLS 1.2 in Kombination mit Perfect Forward Secrecy angesehen. Im übrigen gilt die Technische Richtlinie des BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“ in der jeweils aktuellen Fassung. Die Verwendung von SSL (einschließlich der Version 3.0) ist kein sicheres Verfahren.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Soweit Daten mit einem höheren Schutzbedarf übertragen werden, ist auch innerhalb der Infrastruktur des Cloud-Anbieters eine starke Verschlüsselung zu implementieren.

KRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung

Basisanforderung

Verfahren und technische Maßnahmen zur Verschlüsselung sensibler Daten der Cloud-Kunden bei der Speicherung sind etabliert. Ausnahmen gelten für Daten, die für die Erbringung des Cloud-Dienstes funktionsbedingt nicht verschlüsselt sein können. Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich dem Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt. Ausnahmen (z. B. Verwendung eines Generalschlüssels durch den Cloud-Anbieter) folgen einem geregelten Verfahren und sind mit dem Cloud-Kunden einvernehmlich abzustimmen.

Ergänzende Informationen zur Basisanforderung

Soweit es ein Verfahren zur Verwendung eines Generalschlüssels durch den Cloud-Provider gibt, ist die Angemessenheit des Verfahrens zu prüfen und deren Einhaltung für eine Stichprobe von Einsätzen zu überprüfen.

KRY-04 Sichere Schlüsselverwaltung

Basisanforderung

Verfahren und technische Maßnahmen zur sicheren Schlüsselverwaltung beinhalten mindestens die folgenden Aspekte:

» Schlüsselgenerierung für unterschiedliche kryptographische Systeme und Applikationen,

» Ausstellung und Einholung von Public-Key-Zertifikaten,

» Provisionierung und Aktivierung von Schlüssel für Kunden und beteiligte Dritte,

» Sicheres speichern eigener Schlüssel (nicht die der Cloud-Kunden oder sonstiger Dritter) einschließlich der Beschreibung wie autorisierte Nutzer den Zugriff erhalten,

» Ändern oder Aktualisieren von kryptographischen Schlüssel einschließlich Richtlinien die festlegen unter welchen Bedingungen und auf welcher Weise die Änderungen bzw. Aktualisierungen zu realisieren sind,

» Umgang mit kompromittierten Schlüssel,

» Entzug und Löschen von Schlüsseln, beispielsweise im Falle von Kompromittierung oder Mitarbeiterveränderungen,

» Speicherung der Schlüssel der Cloud-Nutzer nicht beim Cloud-Anbieter (d. h. beim Cloud-Nutzer oder einem vertrauenswürdigen Dritten).

5.9 Kommunikationssicherheit

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

KOS-01 Technische Schutzmaßnahmen

Basisanforderung

Basierend auf den Ergebnissen einer gemäß OIS-06 durchgeführten Risiko-Analyse, hat der Cloud-Anbieter technische Schutzmaßnahmen implementiert, die geeignet sind, um netzwerkbasierte Angriffe auf Basis anomaler Eingangs- oder Ausgangs-Traffic-Muster (z. B. durch MAC-Spoofing und ARP-Poisoning-Angriffe) und/oder Distributed-Denial-of-Service (DDoS) Angriffe zeitnah zu erkennen und darauf zu reagieren.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Intrusion Prevention / Intrusion Detection Systeme (IDS/IPS) sind in ein übergreifendes SIEM-System (Security Information and Event Management) integriert, sodass Ereignisse aus IDS/IPS mit anderen Ereignissen korreliert werden können, um daraus hervorgehend erforderliche (Gegen-) Maßnahmen initiieren zu können. Durch technische Maßnahmen wird sichergestellt, dass keine unbekannten (physischen oder virtuellen) Geräte dem (physischen oder virtuellen) Netzwerk des Cloud-Anbieters beitreten (bspw. durch MACSec gemäß IEEE 802.1X:2010), vgl. IDM-08).

KOS-02 Überwachen von Verbindungen

Basisanforderung

Physische und virtualisierte Netzwerkumgebungen sind so konzipiert und konfiguriert, dass die Verbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzen zu beschränken und überwachen sind. 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 Kontrollen für die Verwendung von Protokollen, die als unsicher angesehen werden.

KOS-03 Netzwerkübergreifende Zugriffe

Basisanforderung

Jeder Netzwerkperimeter wird von Sicherheitsgateways kontrolliert. Die Zugangsberechtigung für Netzübergreifende Zugriffe basiert auf einer Sicherheitsbewertung auf Grundlage der Kundenanforderungen.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Jeder Netzwerkperimeter wird von redundanten und hochverfügbaren Sicherheitsgateways kontrolliert. Die Zugangsberechtigung für netzübergreifende Zugriffe basiert auf einer Sicherheitsbewertung auf Grundlage der Kundenanforderungen.

KOS-04 Netzwerke zur Administration

Basisanforderung

Es existieren gesonderte Netzwerke zur administrativen Verwaltung der Infrastruktur und für den Betrieb von Managementkonsolen, die logisch oder physisch vom Netzwerk der Cloud-Kunden getrennt und durch Multi-Faktor-Authentifizierung vor unberechtigten Zugriffen geschützt sind (vgl. IDM-08). Netzwerke, die zum Zwecke der Migration oder dem erzeugen von virtuellen Maschinen dienen sind ebenfalls physisch oder logisch von anderen Netzwerken zu separieren.

KOS-05 Segregation des Datenverkehrs in gemeinsam genutzten Netzwerkumgebungen

Basisanforderung

Der Datenverkehr in gemeinsam genutzten Netzwerkumgebungen wird gemäß eines dokumentierten Konzepts zur logischen Segmentierung zwischen den Cloud-Kunden auf Netzwerkebene segregiert, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten.

Ergänzende Informationen zur Basisanforderung

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. Penetrationstests zur Validierung des Konzepts). Die Segregation gespeicherter und verarbeiteten Daten ist Gegenstand der Kontrolle RB-23. 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 oder Wechsel von einem ungesicherten Kommunikationskanal (HTTP) auf einen gesicherten Kommunikationskanal (HTTPS) gewechselt werden.

Bei IaaS/PaaS kann sich in der Grundstufe an den Anforderungen für einen höheren Schutzbedarf orientiert werden.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Bei IaaS/PaaS ist die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselter VLANs sichergestellt.

KOS-06 Dokumentation der Netztopologie

Basisanforderung

Die Architektur des Netzwerks ist nachvollziehbar und aktuell dokumentiert (z. B. in Form von Diagrammen), um im Wirkbetrieb Fehler in der Verwaltung zu vermeiden und um im Schadensfall eine zeitgerechte Wiederherstellung gemäß der vertraglichen Verpflichtungen zu gewährleisten. Aus der Dokumentation gehen die unterschiedlichen Umgebungen (z. B. Administrations-Netzwerk und geteilte Netzwerksegmente) und Datenflüsse hervor. Darüber hinaus werden die geografischen Lokationen angegeben, in denen die Daten gespeichert werden.

KOS-07 Richtlinien zur Datenübertragung

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zum Schutz der Datenübertragung vor unbefugtem Abfangen, Manipulieren, Kopieren, Modifizieren, Umleiten oder Vernichten (z. B. Einsatz von Verschlüsselung) sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben stellen einen Bezug zur Klassifikation von Informationen her (vgl. AM-05).

KOS-08 Vertraulichkeitserklärung

Basisanforderung

Die mit internen Mitarbeitern, externen Dienstleistern sowie Lieferanten des Cloud-Anbieters zu schließenden Geheimhaltungs- oder Vertraulichkeitserklärungen basieren auf den Anforderungen des Cloud-Anbieters zum Schutz vertraulicher Daten und betrieblicher Details. Die Anforderungen sind zu identifizieren, dokumentieren und in regelmäßigen Abständen (mindestens jährlich) zu überprüfen. Soweit sich aus der Überprüfung ergibt, dass die Anforderungen anzupassen sind, werden mit den internen Mitarbeitern, den externen Dienstleistern sowie den Lieferanten des Cloud-Anbieters neue Geheimhaltungs- oder Vertraulichkeitserklärungen abgeschlossen. Die Geheimhaltungs- oder Vertraulichkeitserklärungen sind vor Beginn des Vertragsverhältnisses bzw. vor Erteilung des Zugriffs auf Daten der Cloud-Nutzer durch interne Mitarbeiter, externe Dienstleister oder Lieferanten des Cloud-Anbieters zu unterzeichnen.

Ergänzende Informationen zur Basisanforderung

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.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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.

5.10 Portabilität und Interoperabilität

Zielsetzung: Ermöglichen der Eigenschaft den Dienst auf unterschiedlichen IT-Plattformen sicher betreiben zu können sowie die Möglichkeit zur sicheren Anbindung unterschiedlicher IT-Plattformen und Dienstbeendigung.

PI-01 Nutzung öffentlicher API's und Industriestandards

Basisanforderung

Um die Interoperabilität von Cloud-Diensten zu gewährleisten, stehen Daten über dokumentierte Eingangs- und Ausgangs-Schnittstellen und in anerkannten Industriestandards (z. B. das Open Virtualization Format für Virtual Appliances) zur Verfügung, um die Kommunikation zwischen verschiedenen Komponenten und die Migration von Applikationen zu unterstützten.

PI-02 Export von Daten

Basisanforderung

Bei Vertragsende kann der Cloud-Kunde die Daten, die ihm gemäß der vertraglichen Rahmenbedingungen zustehen, bei dem Cloud-Anbieter anfragen und erhält diese in weiterverarbeitbaren elektronischen Standardformaten wie z. B. CSV oder XML.

PI-03 Richtlinie zur Portabilität und Interoperabilität

Basisanforderung

Soweit keine individuellen Vereinbarungen zwischen Cloud-Anbieter und Cloud-Kunden die Interoperabilität und Portabilität der Daten regeln, sind Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um die diesbezüglichen Anforderungen und Verpflichtungen des Cloud-Kunden zu gewährleisten.

PI-04 Sicherer Datenimport und -export

Basisanforderung

Der Cloud-Anbieter verwendet sichere Netzwerkprotokolle für den Import und Export von Informationen, sowie die Verwaltung des Dienstes um die Integrität, Vertraulichkeit und Verfügbarkeit der transportierten Daten sicherzustellen.

PI-05 Sichere Datenlöschung

Basisanforderung

Sowohl beim Wechsel der Speichermedien zu Wartungszwecken als auch bei auf Verlangen des Cloud-Kunden oder Beendigung des Vertragsverhältnisses erfolgt eine vollständige Löschung der Inhaltsdaten des Cloud-Kunden, einschließlich der Datensicherungen und der Metadaten (sobald diese für die ordnungsgemäße Dokumentation der Abrechnung nicht mehr benötigt werden). Die hierzu eingesetzten Methoden (z. B. durch mehrfaches Überschreiben der Daten, löschen des Schlüssels) verhindern eine Wiederherstellung mit forensischen Mitteln.

Ergänzende Informationen zur Basisanforderung

Das Löschen von Metadaten und Protokolldateien ist Gegenstand der Anforderungen RB-11 und RB-13.

5.11 Beschaffung, Entwicklung und Änderung von Informationssystemen

Zielsetzung: Einhalten der Sicherheitsvorgaben bei Neuentwicklungen und Beschaffungen von Informationssystemen sowie Änderungen.

BEI-01 Richtlinien zur Entwicklung / Beschaffung von Informationssystemen

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die ordnungsgemäße Entwicklung und/oder Beschaffung von Informationssystemen für die Entwicklung oder den Betrieb des Cloud-Dienstes, einschließlich Anwendungen, Middleware, Datenbanken, Betriebssystemen und Netzwerkkomponenten sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. In den Richtlinien und Anweisungen sind mindestens die folgenden Aspekte beschrieben:

» Sicherheit in der Softwareentwicklungsmethodik in Übereinstimmung mit in der Industrie etablierten Sicherheitsstandards (z. B. OWASP für Webapplikationen),

» Sicherheit der Entwicklungsumgebung (z. B. getrennte Entwicklungs-/Test-/Produktivumgebungen),

» Programmierrichtlinien für jede verwendete Programmiersprache (z. B. bezüglich Buffer Overflows, verbergen interner Objektreferenzen gegenüber Benutzern),

» Sicherheit in der Versionskontrolle.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

Bei der Beschaffung werden Produkte vorgezogen, die nach den „Common Criteria for Information Technology Security Evaluation“ (kurz: Common Criteria – CC) gemäß Prüftiefe EAL 4 zertifiziert wurden. Werden bei verfügbaren zertifizierten Produkten abweichend unzertifizierte Produkte beschafft, ist dies zu dokumentieren und zu begründen.

BEI-02 Auslagerung der Entwicklung

Basisanforderung

Bei ausgelagerter Entwicklung des Cloud-Dienstes (oder Teilen davon) in Bezug auf Design, Entwicklung, Test und/oder Bereitstellung von Quellcode des Cloud-Dienstes ist ein hohes Maß an Sicherheit gefordert. Deshalb sind mindestens die folgenden Aspekte vertraglich zwischen Cloud-Anbieter und externen Dienstleister zu vereinbaren:

» Anforderungen an einen sicheren Software-Entwicklungsprozess (insbesondere Design, Entwicklung und Test),

» Bereitstellung von Nachweisen, dass eine ausreichende Prüfung vom externen Dienstleister durchgeführt wurde,

» Abnahmeprüfung der Qualität der erbrachten Leistungen gemäß den vereinbarten funktionalen und nicht-funktionalen Anforderungen,

» Das Recht, den Entwicklungsprozess und Kontrollen einer Prüfung, auch stichprobenartig, zu unterziehen.

BEI-03 Richtlinien zur Änderung von Informationssystemen

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für eine ordnungsgemäße Verwaltung von Änderungen (Change Management) an Informationssystemen für die Entwicklung oder den Betrieb des Cloud-Dienstes, einschließlich Anwendungen, Middleware, Datenbanken, Betriebssystemen und Netzwerkkomponenten sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Mindestens die folgenden Aspekte sind dabei zu berücksichtigen:

» Kriterien zur Klassifizierung und Priorisierung von Änderungen und damit verbundene Anforderungen an Art und Umfang durchzuführender Tests und einzuholender Genehmigungen,

» Anforderungen zur Benachrichtigung betroffener Cloud-Kunden gemäß den vertraglichen Vereinbarungen,

» Anforderungen an die Dokumentation von Tests sowie zur Beantragung und Genehmigung von Änderungen,

» Anforderungen an die Dokumentation von Änderungen in der System-, Betriebs- und Benutzerdokumentation.

Ergänzende Informationen zur Basisanforderung

Änderungen an der bestehenden Netzwerkkonfiguration müssen ebenfalls ein geregeltes Verfahren durchlaufen, da sie für eine wirksame Mandantentrennung notwendig sind.

BEI-04 Risikobewertung der Änderungen

Basisanforderung

Der Auftraggeber einer Änderung führt zuvor eine Risikobewertung durch. Alle möglicherweise von der Änderung betroffenen Konfigurationsobjekte werden auf potenzielle Auswirkungen hin bewertet. Das Ergebnis der Risikobewertung ist angemessen und nachvollziehbar zu dokumentieren.

BEI-05 Kategorisierung der Änderungen

Basisanforderung

Alle Änderungen werden basierend auf einer Risikobewertung kategorisiert (z. B. als geringfügige, erhebliche oder weitreichende Folgen), um eine angemessene Autorisierung vor Bereitstellung der Änderung in der Produktivumgebung einzuholen.

BEI-06 Priorisierung der Änderungen

Basisanforderung

Alle Änderungen werden basierend auf einer Risikobewertung priorisiert (z. B. als niedrig, normal, hoch, Notfall), um eine angemessene Autorisierung vor Bereitstellung der Änderung in der Produktivumgebung einzuholen.

BEI-07 Testen der Änderungen

Basisanforderung

Alle Änderungen am Cloud-Dienst werden Tests (z. B. auf Integration, Regression, Sicherheit und Benutzerakzeptanz) während der Entwicklung und vor der Bereitstellung in der Produktivumgebung unterzogen. Die Tests werden von angemessen qualifiziertem Personal des Cloud-Anbieters durchgeführt. Gemäß Dienstgütevereinbarung (SLA) werden Änderungen ebenfalls durch den/die dazu geeigneten Kunden (Tenants) getestet.

BEI-08 Zurückrollen der Änderungen

Basisanforderung

Es sind Abläufe definiert, um erforderliche Änderungen in Folge von Fehlern oder Sicherheitsbedenken zurückrollen zu können und betroffene Systeme oder Dienste im vorherigen Zustand wiederherzustellen.

BEI-09 Überprüfen von ordnungsgemäßer Testdurchführung und Genehmigung

Basisanforderung

Bevor eine Änderung in der Produktivumgebung veröffentlicht wird (Release), ist diese durch eine hierzu autorisierte Stelle oder ein entsprechendes Gremium dahingehend zu überprüfen, ob die geplanten Tests erfolgreich abgeschlossen und die erforderlichen Genehmigungen erteilt sind.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Mindestens vierteljährlich wird für eine angemessene Zufallsstichprobe von Änderungen in der Produktivumgebung (d. h. min. 10% aller in diesem Zeitraum abgeschlossenen Änderungen) überprüft, ob die internen Anforderungen in Bezug auf ordnungsgemäße Klassifizierung, Test und Genehmigung von Änderungen eingehalten wurden.

BEI-10 Notfalländerungen

Basisanforderung

Notfalländerungen sind als solche von dem Änderungsmanager zu klassifizieren, der die Änderungsdokumentation vor Übertragung der Änderung in die Produktivumgebung erstellt. Anschließend (z. B. innerhalb von 5 Werktagen) fügt der Änderungsmanager Begründung und Ergebnis der Übertragung der Notfalländerung zu der Änderungsdokumentation hinzu. Aus der Begründung muss hervorgehen, warum der reguläre Änderungsprozess nicht durchlaufen werden konnte und was die Folgen einer Verzögerung durch Einhaltung des regulären Prozesses gewesen wären. Die Änderungsdokumentation wird an die betroffenen Kunden weitergeleitet und gemäß der vertraglichen Vereinbarungen eine nachträgliche Freigabe durch die hierzu autorisierten Stellen eingeholt.

BEI-11 Systemlandschaft

Basisanforderung

Produktivumgebungen sind von Nicht-Produktivumgebungen physisch oder logisch getrennt, um unbefugten Zugriff oder Änderungen an Produktivdaten zu vermeiden. Produktivdaten werden nicht in Test- oder Entwicklungsumgebungen repliziert, um deren Vertraulichkeit zu wahren.

BEI-12 Funktionstrennung

Basisanforderung

Verfahren zum Change Management beinhalten rollenbasierte Autorisierungen, um eine angemessene Funktionstrennung bei Entwicklung, Freigabe und Migration von Änderungen zwischen den Umgebungen sicherzustellen.

5.12 Steuerung und Überwachung von Dienstleistern und Lieferanten

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

DLL-01 Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister und Lieferanten des Cloud-Anbieters

Basisanforderung

Richtlinien und Anweisungen zur Sicherstellung des Schutzes von Informationen auf die sonstige Dritte (z. B. Dienstleister bzw. Lieferanten des Cloud-Anbieters), die wesentliche Teile zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben dienen der Mitigierung von Risiken, die durch den potenziellen Zugriff auf Informationen der Cloud-Kunden entstehen können. Dabei werden mindestens die folgenden Aspekte berücksichtigt:

- Definition und Beschreibung von Mindest-Sicherheitsanforderungen in Bezug auf die verarbeiteten Informationen, die sich an anerkannten Industriestandards wie ISO/IEC 27001 orientieren,
- rechtliche und regulatorische Anforderungen, einschließlich Datenschutz, Recht am geistigen Eigentum, Copyright, Umgang mit Metadaten (vgl. RB-11) sowie eine Beschreibung wie diese gewährleistet werden (z. B. Standort der Datenverarbeitung und Haftung, vgl. Umfeldparameter),
- Anforderungen an das Incident- und Vulnerability-Management (insbesondere Benachrichtigungen und Kollaborationen während einer Störungsbehebung),
- Weitergabe und vertragliche Verpflichtung auf die Mindest-Sicherheitsanforderungen auch an Unterauftragnehmer, wenn diese nicht nur unwesentliche Teile zu Entwicklung oder Betrieb des Cloud-Dienstes beitragen (z. B. RZ-Dienstleister).

Die Definition der Anforderungen ist in das Risikomanagement des Cloud-Anbieters eingebunden. Gemäß der Anforderung OIS-07 werden sie regelmäßig auf ihre Angemessenheit hin überprüft.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Unterauftragnehmer des Cloud-Anbieters werden vertraglich dazu verpflichtet, dem Cloud-Anbieter Prüfungsrechte über die Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems sowie das Einhalten der vereinbarten Sicherheitsanforderungen einzuräumen. Der Unterauftragnehmer kann den Nachweis auch durch Vorlage entsprechender Bescheinigungen unabhängiger Dritter (z. B. in Form von Berichterstattungen nach ISAE 3402/IDW PS 951) erbringen. Dies schließt auch Unterauftragnehmer des Unterauftragnehmers ein.

DLL-02 Überwachung der Leistungserbringung und Sicherheitsanforderungen an Dienstleister und Lieferanten des Cloud-Anbieters

Basisanforderung

Verfahren zur regelmäßigen Überwachung und Überprüfung der vereinbarten Leistungen und Sicherheitsanforderungen von Dritten (z. B. Dienstleister bzw. Lieferanten des Cloud-Anbieters), die wesentliche Teile zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, sind etabliert.

Die Maßnahmen umfassen mindestens:

- regelmäßige Überprüfung von Dienstleistungsberichten (z. B. SLA Reportings), soweit diese von Dritten erbracht werden,

» Überprüfung von sicherheitsrelevanten Vorfällen, Betriebsstörungen oder Ausfällen und Unterbrechungen, die mit der Dienstleistung zusammenhängen,

» außerplanmäßige Überprüfungen nach wesentlichen Änderungen der Anforderungen oder des Umfelds. Die Wesentlichkeit ist durch den Cloud- Anbieter zu beurteilen und für Audits nachvollziehbar zu dokumentieren.

Festgestellte Abweichungen werden gemäß der Anforderung OIS-07 einer Risikoanalyse unterzogen, um diese zeitgerecht durch mitigierende Maßnahmen wirksam zu adressieren.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Schnittstellen für eine automatisierte Echtzeit-Überwachung der Dienstleistung (mindestens Kapazität, Verfügbarkeit sowie Behebung von Störungen) sind eingerichtet, um die Einhaltung der vereinbarten Dienstgütevereinbarungen zu überwachen und zeitnah auf Abweichungen reagieren zu können. Mindestens jährlich erfolgt eine Prüfung durch unabhängige, externe Prüfer oder qualifiziertes Personal des Cloud-Anbieters, um die Wirksamkeit der beim Dienstleister eingerichteten Kontrollen, die im Zusammenhang mit dem Vertragsverhältnis stehen sowie die vereinbarten Sicherheitsanforderungen zu überprüfen. Die Nachweisführung kann z. B. in Form von Berichterstattungen nach ISAE 3402/ IDW PS 951 erfolgen. Die zeitgerechte Adressierung von Prüfungsfeststellungen werden durch den Cloud-Anbieter nachgehalten.

5.13 Security Incident Management

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

SIM-01 Verantwortlichkeiten und Vorgehensmodell

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um eine schnelle, effektive und ordnungsgemäße Reaktion auf alle bekannten Sicherheitsvorfälle zu gewährleisten. Seitens des Cloud-Anbieters sind dabei mindestens die in OIS-03 aufgeführten Rollen zu besetzen, Vorgaben zur Klassifizierung, Priorisierung und Eskalation von Sicherheitsvorfällen zu definieren und Schnittstellen zum Incident Management sowie dem Business Continuity Management zu schaffen. 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.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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.

SIM-02 Klassifizierung von Kunden Systemen

Basisanforderung

Alle Kundensysteme sind gemäß der Vereinbarungen (SLA) zwischen Cloud-Anbieter und Cloud-Kunden bezüglich der Kritikalität zur Dienstleistungserbringung klassifiziert. Die Zuweisung der vereinbarten Klassifizierungen wird regelmäßig sowie nach wesentlichen Änderungen/Ereignissen für sämtliche Kundensysteme überprüft. Abweichungen werden nachverfolgt und zeitnah aufgelöst. Ferner geht aus der Klassifizierung hervor, welche Parameter bzgl. der Wiederverfügbarkeit eines Systems mit dem Cloud-Kunden vereinbart wurden.

SIM-03 Bearbeitung von Sicherheitsvorfällen

Basisanforderung

Ereignisse, die einen Sicherheitsvorfall darstellen könnten, werden durch qualifiziertes Personal des Cloud-Anbieters oder in Verbindung mit externen Sicherheitsdienstleistern klassifiziert, priorisiert und einer Ursachenanalyse unterzogen.

SIM-04 Dokumentation und Berichterstattung über Sicherheitsvorfälle

Basisanforderung

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.

Optionale, weitergehende Anforderungen (Vertraulichkeit)

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.

SIM-05 Security Incient Event Management

Basisanforderung

Protokollierte Vorfälle werden zentral aggregiert und konsolidiert (Event-Korrelation). Regeln zur Erkennung von Beziehungen zwischen Vorfällen und zur Beurteilung gemäß Kritikalität sind implementiert. Die Behandlung dieser Vorfälle erfolgt gemäß dem Security Incident Management Prozess.

SIM-06 Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle

Basisanforderung

Mitarbeiter und externe Geschäftspartner werden über ihre Verpflichtungen informiert. Falls erforderlich willigen sie dazu ein oder verpflichten sich vertraglich dazu, alle Sicherheitsereignisse zeitnah an eine zuvor benannte zentrale Stelle zu melden. Zusätzlich wird darüber informiert, dass „Falschmeldungen“ von Ereignisses, die sich im Nachhinein nicht als Vorfälle herausstellen, keine negativen Folgen nach sich ziehen.

SIM-07 Auswertung und Lernprozess

Basisanforderung

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.

Ergänzende Informationen zur Basisanforderung

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

5.14 Sicherstellung des Geschäftsbetriebs und Notfallmanagement

Zielsetzung: Strategische Etablierung & Steuerung eines Business Continuity Managements (BCM). Planen, implementieren und testen von Notfallkonzepten sowie verankern von Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebs.

BCM-01 Verantwortung durch die Unternehmensleitung

Basisanforderung

Die Unternehmensleitung (bzw. ein Mitglied der Unternehmensleitung) 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 im Bezug auf dieses Thema, in dem sie beispielsweise die Mitarbeiter dazu auffordern beziehungsweise ermutigen, zu der Effektivität des Kontinuitäts- und Notfallmanagements aktiv beizutragen.

BCM-02 Richtlinien und Verfahren zur Business Impact Analyse

Basisanforderung

Richtlinien und Anweisungen zum Ermitteln von Auswirkungen etwaiger Störungen des Cloud-Dienstes oder des Unternehmens sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt.

Mindestens die folgenden Aspekte werden dabei berücksichtigt:

» mögliche Szenarien basierend auf einer Risikoanalyse (z. B. Ausfall von Personal, Gebäude, Infrastruktur und Dienstleister),

» Identifizierung kritischer Produkte und Dienstleistungen,

» Identifizierung von Abhängigkeiten, einschließlich der Prozesse (inkl. dafür benötigter Ressourcen), Anwendungen, Geschäftspartner und Dritter,

» Erfassung von Bedrohungen gegenüber kritischer Produkte 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.

BCM-03 Planung der Betriebskontinuität

Basisanforderung

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 (z. B. der verschiedenen Standorte des Cloud-Anbieters) 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.

BCM-04 Verifizierung, Aktualisierung und Test der Betriebskontinuität

Basisanforderung

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 (z. B. kritische Lieferanten) mit ein. Die Tests werden dokumentiert und Ergebnisse werden für zukünftige Maßnahmen der betriebliche Kontinuität berücksichtigt.

Ergänzende Informationen zur Basisanforderung

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

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Zusätzlich zu den Tests werden auch Übungen durchgeführt, die u. a. Szenarien aus in der Vergangenheit bereits aufgetretenen Sicherheitsvorfällen hervorgegangen sind.

BCM-05 Rechenzentrumsversorgung

Basisanforderung

Die Versorgung der Rechenzentren (z. B. Wasser, Elektrizität, Temperatur- und Feuchtigkeitskontrolle, Telekommunikation und Internetverbindung) ist abgesichert, überwacht und wird regelmäßig gewartet und getestet, um eine durchgängige Wirksamkeit zu gewährleisten. Sie ist mit automatischen Ausfallsicherungen und anderen Redundanzen konzipiert. Die Wartung wird in Übereinstimmung mit den von den Lieferanten empfohlenen Wartungsintervallen und Vorgaben sowie ausschließlich von autorisiertem Personal durchgeführt. Wartungsprotokolle einschließlich vermuteter oder festgestellter Mängel werden für den Zeitraum der zuvor vertraglich vereinbarter Frist aufbewahrt. Nach dieser Frist werden die Wartungsprotokolle ordnungsgemäß und dauerhaft vernichtet.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Simulierte Ausfälle der Versorgung der Rechenzentren wird in die Übungen (vgl. BCM-03) mit eingebunden.

5.15 Sicherheitsprüfung und -nachweis

Zielsetzung: Überprüfen und nachhalten, dass die Maßnahmen zur Informationssicherheit in Übereinstimmung mit den organisationsweiten Richtlinien und Anweisungen implementiert und ausgeführt werden.

SPN-01 Informieren der Unternehmensleitung

Basisanforderung

Die Unternehmensleitung wird durch regelmäßige Berichte über den Stand der Informationssicherheit auf Grundlage der Sicherheitsprüfungen informiert und ist verantwortlich für die zeitnahe Behebung von daraus hervorgegangenen Feststellungen.

SPN-02 Interne Überprüfungen der Compliance von IT-Prozessen mit internen Sicherheitsrichtlinien und Standards

Basisanforderung

Qualifiziertes Personal (z. B. Interne Revision) des Cloud-Anbieters oder durch den Cloud-Anbieter beauftragte sachverständige Dritte überprüfen jährlich die Compliance der internen IT-Prozesse mit den entsprechenden internen Richtlinien und Standards sowie der für den Cloud-Dienst relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität, werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Die Prüfung wird mindestens halbjährlich durchgeführt. Die Prüfung umfasst auch die Einhaltung der Anforderungen dieses Anforderungskatalogs.

SPN-03 Interne Überprüfungen der Compliance von IT-Systemen mit internen Sicherheitsrichtlinien und Standards

Basisanforderung

Qualifiziertes Personal (z. B. Interne Revision) des Cloud-Anbieters oder durch den Cloud-Anbieter beauftragte sachverständige Dritte überprüfen mindestens jährlich die Compliance der IT-Systeme, soweit diese ganz oder teilweise im Verantwortungsbereich des Cloud-Anbieters liegen und für die Entwicklung oder den Betrieb des Cloud-Dienstes relevant sind, mit den entsprechenden internen Richtlinien und Standards sowie der für den Cloud-Dienst relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität, werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Auf Anfrage der Cloud-Kunden stellt der Cloud-Anbieter Informationen über die Ergebnisse, Auswirkungen und Risiken dieser Prüfungen und Beurteilungen in angemessener Form zur Verfügung. Der Cloud-Anbieter verpflichtet seine Unterauftragnehmer zu solchen Prüfungen und lässt sich die Prüfberichte im gleichen Turnus vorlegen und verwertet sie bei seinen Überprüfungen.

5.16 Compliance und Datenschutz

Zielsetzung: Vermeiden von Verstößen gegen gesetzliche oder vertragliche Verpflichtungen in Bezug auf Informationssicherheit.

COM-01 Identifizierung anzuwendender gesetzlicher, vertraglicher und datenschutzrechtlicher Anforderungen

Basisanforderung

Rechtliche, regulative und gesetzlich vorgeschriebene Anforderungen, sowie die Vorgehensweise, um diese Vorgaben einzuhalten sind durch den Cloud-Anbieter für den Cloud-Dienst anwendungsbezogen zu identifizieren, dokumentieren und regelmäßig zu aktualisieren.

Ergänzende Informationen zur Basisanforderung

Die Dokumentation des Cloud-Anbieters kann u. a. auf die folgenden regulatorischen Anforderungen Bezug nehmen:

» allgemein anerkannte Buchführungsgrundsätze (z. B. gemäß HGB oder IFRS)

» Anforderungen bzgl. des Datenzugriffs und der Prüfbarkeit digitaler Unterlagen (z. B. gemäß GDPdU)

» Anforderungen zum Schutz personenbezogener Daten (z. B. gemäß BDSG oder EU Datenschutzrichtlinie)

» Anforderungen der Regierung (z. B. gemäß BSIG oder AktG)

COM-02 Planung unabhängiger, externer Audits

Basisanforderung

Unabhängige Überprüfungen und Beurteilungen von Systemen oder Komponenten die zur Erbringung der Cloud-Dienste beitragen, sind vom Cloud-Anbieter so geplant, dass die folgenden Anforderungen erfüllt werden:

» Es erfolgt ausschließlich lesender Zugriff auf Software und Daten.

» Aktivitäten, die möglicherweise die Verfügbarkeit der Systeme oder Komponenten beeinträchtigen und so zu einem Verstoß des SLAs führen könnten, werden außerhalb der regulären Geschäftszeiten bzw. nicht zu Zeiten von Lastspitzen durchgeführt.

» Die durchgeführten Aktivitäten werden protokolliert und überwacht.

Optionale, weitergehende Anforderungen (Verfügbarkeit)

Der Cloud-Anbieter hat Vorkehrungen für außerplanmäßige Audits getroffen.

COM-03 Durchführung unabhängiger, externer Audits

Basisanforderung

Prüfungen und Beurteilungen von Prozessen, IT-Systemen und IT-Komponenten, soweit diese ganz oder teilweise im Verantwortungsbereich des Cloud-Anbieters liegen und für die Entwicklung oder den Betrieb des Cloud-Dienstes relevant sind, werden mindestens jährlich durch unabhängige Dritte (z. B. Wirtschaftsprüfer) durchgeführt, um Nichtkonformitäten mit rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen zu identifizieren. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Auf Anfrage der Cloud-Kunden stellt der Cloud-Anbieter Informationen über die Ergebnisse, Auswirkungen und Risiken dieser Prüfungen und Beurteilungen in angemessener Form zur Verfügung. Falls notwendig, können außerplanmäßige Überprüfungen durch unabhängige Dritte durchgeführt werden.

5.17 Mobile Device Management

Zielsetzung: Gewährleistung der Sicherheit beim Einsatz mobiler Endgeräte im Verantwortungsbereich des Cloud-Anbieters für den Zugriff auf IT-Systeme zur Entwicklung und zum Betrieb des Cloud-Dienstes.

MDM-01 Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des Cloud-Anbieters

Basisanforderung

Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die ordnungsgemäße Verwendung mobiler Endgeräte im Verantwortungsbereich des Cloud-Anbieters, die Zugriff auf IT-Systeme zur Entwicklung und zum Betrieb des Cloud-Dienstes ermöglichen, sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Darin werden mindestens folgende Aspekte beachtet, soweit diese auf die Situation des Cloud-Anbieters anwendbar sind:

» Verschlüsselung der Geräte und der Datenübertragung,

» verstärkter Zugriffsschutz,

» erweitertes Identitäts- und Berechtigungsmanagement,

» Verbot von Jailbreaking/Rooting,

» Installation nur von freigegebenen Anwendungen aus als vertrauenswürdig eingestuften „App Stores“,

» Bring-Your-Own-Device (BYOD) – Mindestanforderungen an private Endgeräte.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit)

Es erfolgt eine zentrale Verwaltung und Überwachung mittels MDM-Lösungen, einschließlich Möglichkeit zur Fernlöschung. Es erfolgt eine

Standort-Plausibilisierung der Zugriffe. Eine Inventarisierungsliste mobiler Endgeräte mit Zugriff auf den Cloud-Dienst (u. a. mit Informationen über Betriebssystem und Patch-Status, zugeordneter Mitarbeiter, Freigabe bzgl. BYOD) wird geführt (vgl. AM-01).

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: cloudsecurity@bsi.bund.de
Internet: www.bsi.bund.de/C5

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
Telefon: +49 (0) 22899 9582-0
Telefax: +49 (0) 22899 9582-5400

Stand
September 2017

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelbild: Fotolia

Artikelnummer
BSI-Cloud17/202

www.bsi.bund.de