OPS.2: IT-Betrieb von Dritten

OPS.2.2: Cloud-Nutzung

1 Beschreibung

1.1 Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. 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.

Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen des Cloud-Diensteanbieters zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzer der nutzenden Institution, ist ein wichtiger Erfolgsfaktor.

Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance berücksichtigt werden (Cloud Governance). Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

1.2 Zielsetzung

Der Baustein beschreibt Anforderungen, durch die sich Cloud-Dienste sicher nutzen lassen. Er richtet sich an alle Institutionen, die solche Dienste bereits nutzen oder sie zukünftig einsetzen wollen.

1.3 Abgrenzung und Modellierung

Der Baustein OPS.2.2 *Cloud-Nutzung* ist immer auf eine konkrete Cloud-Dienstleistung anzuwenden. Nutzt eine Institution unterschiedliche Cloud-Diensteanbieter, so ist der Baustein für jeden Cloud-Diensteanbieter einmal anzuwenden. Die Schnittstelle zwischen den Cloud-Diensteanbietern ist ebenfalls Gegenstand des Bausteins und muss für alle Cloud-Dienstleistungen betrachtet werden.

In nahezu allen Bereitstellungsmodellen, abgesehen von der Nutzung einer Private Cloud On-Premise, stellen Cloud-Dienste eine Sonderform des Outsourcings (siehe Baustein OPS.2.1 *Outsourcing für Kunden*) dar. Die im Baustein OPS.2.2 *Cloud-Nutzung* beschriebenen Gefährdungen und Anforderungen werden daher häufig auch im Outsourcing angewendet. Bei Cloud-Diensten gibt es jedoch einige Besonderheiten, die sich ausschließlich in diesem Baustein wiederfinden. Der Baustein OPS.2.1 *Outsourcing für Kunden* ist daher nicht auf Cloud-Dienste anzuwenden.

Die in diesem Baustein beschriebenen Gefährdungen und Anforderungen gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Sicherheitsanforderungen, mit denen Anbieter ihre Cloud-Dienste schützen können, sind nicht Gegenstand dieses Bausteins. Gefährdungen und spezifische Sicherheitsanforderungen, die durch die Anbindung eines Cloud-Dienstes über entsprechende Schnittstellen (engl. API, Application Programming Interface) als relevant anzusehen sind, werden ebenfalls nicht in diesem Baustein betrachtet.

Abgrenzung zum klassischen IT-Outsourcing

Beim Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Institution ganz oder teilweise zu externen Dienstleistern ausgelagert. Dies ist ein etablierter Bestandteil heutiger Organisationsstrategien. Das klassische IT-Outsourcing ist meist so gestaltet, dass die komplette gemietete Infrastruktur exklusiv von einem Kunden genutzt wird (Single Tenant Architektur), auch wenn Outsourcing-Anbieter normalerweise mehrere Kunden haben. Zudem werden Outsourcing-Verträge meistens über längere Laufzeiten abgeschlossen.

Die Nutzung von Cloud-Diensten gleicht in vielen Punkten dem klassischen Outsourcing, aber es kommen noch einige Unterschiede hinzu, die zu berücksichtigen sind:

- Aus wirtschaftlichen Gründen teilen sich oft in einer Cloud mehrere Anwender eine gemeinsame Infrastruktur.
- Cloud-Dienste sind dynamisch und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. So können Cloud-basierte Angebote rascher an den tatsächlichen Bedarf des Anwenders angepasst werden.
- Die in Anspruch genommenen Cloud-Dienste werden in der Regel mittels einer Webschnittstelle durch den Cloud-Anwender selbst gesteuert. So kann er automatisiert die genutzten Dienste auf seine Bedürfnisse zuschneiden.
- Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geographisch sowohl im In- als auch im Ausland weit verstreut sein können.
- Der Anwender kann die genutzten Dienste und seine Ressourcen einfach über Web-Oberflächen oder passende Schnittstellen administrieren, wobei wenig Interaktion mit dem Provider erforderlich ist.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein OPS.2.2 *Cloud-Nutzung* von besonderer Bedeutung.

2.1 Fehlende oder unzureichende Strategie für die Cloud-Nutzung

Cloud-Dienste in einer Institution einzusetzen, ist eine strategische Entscheidung. Durch eine fehlende oder unzureichende Strategie für die Cloud-Nutzung ist es z. B. möglich, dass sich eine Institution für einen ungeeigneten Cloud-Dienst oder -Anbieter entscheidet. Auch könnte der ausgewählte Cloud-Dienst mit der eigenen IT, den internen Geschäftsprozessen oder dem Schutzbedarf nicht kompatibel sein. Dies kann sich organisatorisch, technisch oder auch finanziell negativ auf die Geschäftsprozesse

auswirken. Generell kann eine fehlende oder unzureichende Strategie für die Cloud-Nutzung dazu führen, dass die damit verbundenen Ziele nicht erreicht werden oder das Sicherheitsniveau signifikant sinkt.

2.2 Abhängigkeit von einem Cloud-Diensteanbieter (Kontrollverlust)

Nutzt eine Institution externe Cloud-Dienste, ist sie mehr oder weniger stark vom jeweiligen Cloud-Diensteanbieter abhängig. Dadurch kann es passieren, dass die Institution die ausgelagerten Geschäftsprozesse und die damit verbundenen Informationen nicht mehr vollständig kontrollieren kann, insbesondere deren Sicherheit. Auch ist die Institution trotz möglicher Kontrollen ab einem gewissen Punkt darauf angewiesen, dass der Cloud-Diensteanbieter Sicherheitsmaßnahmen auch korrekt umsetzt. Macht er das nicht, sind Geschäftsprozesse und geschäftskritische Informationen unzureichend geschützt.

Zudem kann die Nutzung externer Cloud-Dienste dazu führen, dass in der Institution Know-how über Informationssicherheit und -technik verloren geht. Dadurch kann die Institution unter Umständen gar nicht mehr beurteilen, ob die vom Anbieter ergriffenen Schutzmaßnahmen ausreichend sind. Auch ein Anbieterwechsel ist so nur noch sehr schwer möglich. Der Cloud-Diensteanbieter könnte diese Abhängigkeit zum Beispiel auch ausnutzen, um Preiserhöhungen durchzusetzen oder die Dienstleistungsqualität zu senken.

2.3 Mangelhaftes Anforderungsmanagement bei der Cloud-Nutzung

Wenn sich eine Institution dafür entscheidet, einen Cloud-Dienst zu nutzen, sind daran in der Regel viele Erwartungen geknüpft. So erhoffen sich Mitarbeiter beispielsweise eine höhere Leistungsfähigkeit oder einen größeren Funktionsumfang der ausgelagerten Dienste, während die Institutionsleitung auf geringere Kosten spekuliert. Ein mangelndes Anforderungsmanagement vor der Cloud-Nutzung kann jedoch dazu führen, dass die Erwartungen nicht erfüllt werden und der Dienst nicht den gewünschten Mehrwert, z. B. hinsichtlich der Verfügbarkeit, liefert.

2.4 Verstoß gegen rechtliche Vorgaben

Viele Anbieter bieten ihre Cloud-Dienste in einem internationalen Umfeld an. Damit unterliegen sie oft anderen nationalen Gesetzgebungen. Häufig sehen Cloud-Kunden nur die mit dem Cloud Computing verbundenen Vorteile (z. B. Kostenvorteile) und schätzen die rechtlichen Rahmenbedingungen falsch ein, wie z. B. Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder Informationszugriff für Dritte. Dadurch könnten geltende Richtlinien und Vorgaben verletzt werden. Auch die Sicherheit der ausgelagerten Informationen könnte beeinträchtigt werden.

2.5 Fehlende Mandantenfähigkeit beim Cloud-Diensteanbieter

Beim Cloud Computing teilen sich meistens verschiedene Kunden eine gemeinsame Infrastruktur, wie z. B. IT-Systeme, Netze und Anwendungen. Werden die Ressourcen der verschiedenen Kunden nicht ausreichend sicher voneinander getrennt, kann ein Kunde eventuell auf die Bereiche eines anderen Kunden zugreifen und dort Informationen manipulieren oder löschen.

2.6 Unzulängliche vertragliche Regelungen mit einem Cloud-Diensteanbieter

Aufgrund von unzulänglichen vertraglichen Regelungen mit einem Cloud-Diensteanbieter können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Verantwortungsbereiche, Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann es passieren, dass der Cloud-Diensteanbieter unbeabsichtigt oder aufgrund fehlender Ressourcen Sicherheitsmaßnahmen nicht oder nur ungenügend umsetzt.

Auch wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können Nachteile für den Auftraggeber daraus resultieren. So nutzen Cloud-Diensteanbieter für ihre Services häufig die Dienste Dritter. Bestehen hier unzureichende vertragliche Vereinbarungen oder wurden die

Abhängigkeiten zwischen dem Dienstleister und Dritten nicht offengelegt, kann sich dies auch negativ auf die Informationssicherheit und die Serviceleistung der Institution auswirken.

2.7 Mangelnde Planung der Migration zu Cloud-Diensten

Die Migration zu einem Cloud-Dienst ist fast immer eine kritische Phase. Durch mangelhafte Planungen können Fehler auftreten, die sich auf die Informationssicherheit innerhalb der Institution auswirken. Verzichtet eine Institution beispielsweise durch eine ungenügende Planungsphase leichtfertig auf eine stufenweise Migration, kann dies in der Praxis zu erheblichen Problemen führen. Gibt es im Vorfeld etwa keine Testphasen, Pilot-Benutzer oder einen zeitlich begrenzten Parallelbetrieb von bestehender Infrastruktur und Cloud-Diensten, können wichtige Daten verloren gehen oder Dienste komplett ausfallen.

2.8 Unzureichende Einbindung von Cloud-Diensten in die eigene IT

Es ist erforderlich, dass Cloud-Dienste angemessen in die IT-Infrastruktur der Institution eingebunden werden. Setzen die Zuständigen dies nur unzureichend um, kann es passieren, dass die Benutzer die beauftragten Cloud-Dienstleistungen nicht in vollem Umfang abrufen können. Die Cloud-Dienste liefern so eventuell nicht die erforderliche und vereinbarte Leistung oder auf sie kann gar nicht oder nur eingeschränkt zugegriffen werden. Dadurch können Geschäftsprozesse verlangsamt werden oder ganz ausfallen. Werden Cloud-Dienste falsch in die eigene IT eingebunden, können auch schwerwiegende Sicherheitslücken entstehen.

2.9 Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens

Unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses können gravierende Folgen für die Institution haben. Das ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht der Institution kritischer Fall unerwartet eintritt, wie beispielsweise die Insolvenz, der Verkauf des Cloud-Diensteanbieters oder schwerwiegende Sicherheitsbedenken. Ohne eine ausreichende interne Vorsorge sowie genaue Vertragsregelungen kann sich die Institution nur schwer aus dem abgeschlossenen Vertrag mit dem Cloud-Diensteanbieter lösen. In diesem Fall ist es schwierig bis unmöglich, den ausgelagerten Cloud-Dienst zeitnah beispielsweise auf einen anderen Diensteanbieter zu übertragen oder ihn wieder in die eigene Institution einzugliedern.

Auch kann eine unzureichend geregelte Datenlöschung nach Vertragsende dazu führen, dass unberechtigt auf die Informationen der Institution zugegriffen wird.

2.10 Unzureichendes Administrationsmodell für die Cloud-Nutzung

Werden Cloud-Dienste genutzt, verändert sich häufig das Rollenverständnis innerhalb des IT-Betriebs des Cloud-Kunden. So entwickeln sich Administratoren oft weg von klassischen Systemadministratoren hin zu Service-Administratoren. Wird dieser Prozess nicht ausreichend begleitet, kann sich dies negativ auf die Cloud-Nutzung auswirken, etwa, wenn die Administratoren nicht das nötige Verständnis für die Umstellungen mitbringen oder sie für ihre neue Aufgabe nicht oder nur unzureichend geschult sind. In der Folge sind eventuell die Cloud-Dienste nicht ordnungsgemäß administriert und so nur noch eingeschränkt verfügbar oder sie fallen ganz aus.

2.11 Unzureichendes Notfallvorsorgekonzept

Eine unzureichende Notfallvorsorge hat bei der Cloud-Nutzung schnell gravierende Folgen. Wenn der Cloud-Dienst oder Teile hiervon ausfallen, führen Versäumnisse bei den Notfallvorsorgekonzepten beim Cloud-Diensteanbieter sowie bei den Schnittstellen immer zu unnötig langen Ausfallzeiten mit entsprechenden Folgen für die Produktivität bzw. Dienstleistung des Auftraggebers. Daneben können mangelhaft abgestimmte Notfallszenarien zwischen Auftraggeber und Dienstleister zu Lücken in der Notfallvorsorge führen.

2.12 Ausfall der IT-Systeme eines Cloud-Diensteanbieters

Bei einem Cloud-Diensteanbieter können die dort betriebenen Prozesse, IT-Systeme und Anwendungen teilweise oder ganz ausfallen, wovon folglich auch der Cloud-Kunde betroffen ist. Werden die Mandanten unzureichend voneinander getrennt, kann auch ein ausgefallenes IT-System, das nicht dem Cloud-Kunden zugeordnet ist, dazu führen, dass der Cloud-Kunde seine vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Cloud-Diensteanbieter und -Kunde ausfällt oder wenn die genutzte Cloud-Computing-Plattform erfolgreich angegriffen wird.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragter, Institutionsleitung, Personalabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.2.2 *Cloud-Nutzung* vorrangig erfüllt werden:

OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung [Fachverantwortliche, Institutionsleitung, Datenschutzbeauftragter] (B)

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.

Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Diensteanbieter bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung [Fachverantwortliche] (B)

Auf Basis der Strategie für die Cloud-Nutzung MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle

Sicherheitsanforderungen an den Cloud-Diensteanbieter sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste internationaler Anbieter genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Cloud-Kunden [Fachverantwortliche] (B)

Für jeden Cloud-Dienst MUSS eine Service-Definition durch den Cloud-Kunden erarbeitet werden. Zudem SOLLTEN alle geplanten und genutzten Cloud-Dienste dokumentiert werden.

OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen [Fachverantwortliche] (B)

Basierend auf der Service-Definition für Cloud-Dienste MUSS der Cloud-Kunde alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifizieren und dokumentieren. Es MUSS klar erkennbar sein, wie die Verantwortungsbereiche zwischen Cloud-Diensteanbieter und -Kunde voneinander abgegrenzt sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein OPS.2.2 *Cloud-Nutzung*. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst [Fachverantwortliche] (S)

Bevor zu einem Cloud-Dienst migriert wird, SOLLTE durch den Cloud-Kunden ein Migrationskonzept erstellt werden. Dafür SOLLTEN zunächst organisatorische Regelungen sowie die Aufgabenverteilung festgelegt werden. Zudem SOLLTEN bestehende Betriebsprozesse hinsichtlich der Cloud-Nutzung identifiziert und angepasst werden. Es SOLLTE sichergestellt werden, dass die eigene IT ausreichend im Migrationsprozess berücksichtigt wird. Auch SOLLTEN die Verantwortlichen ermitteln, ob die Mitarbeiter der Institution zusätzlich geschult werden sollten.

OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten (S)

Bevor ein Cloud-Dienst genutzt wird, SOLLTE sorgfältig geplant werden, wie er in die IT der Institution eingebunden werden soll. Hierfür SOLLTE mindestens geprüft werden, ob Anpassungen der Schnittstellen, der Netzanbindung, des Administrationsmodells sowie des Datenmanagementmodells notwendig sind. Die Ergebnisse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (S)

Auf Grundlage der identifizierten Sicherheitsanforderungen (siehe OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) SOLLTE durch den Cloud-Kunden ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters [Institutionsleitung] (S)

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE durch den Cloud-Kunden ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung eines Cloud-Diensteanbieters SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt werden.

OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter [Institutionsleitung] (S)

Die vertraglichen Regelungen zwischen dem Cloud-Kunden und dem Cloud-Diensteanbieter SOLLTEN in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Informationen angepasst sein, die im Zusammenhang mit der Cloud-Nutzung stehen. Es SOLLTE geregelt werden, an welchem Standort der

Cloud-Diensteanbieter seine Leistung erbringt. Zusätzlich SOLLTEN Eskalationsstufen und Kommunikationswege zwischen der Institution und dem Cloud-Diensteanbieter definiert werden. Auch SOLLTE vereinbart werden, wie die Daten der Institution sicher zu löschen sind. Ebenso SOLLTEN Kündigungsregelungen schriftlich fixiert werden. Der Cloud-Diensteanbieter SOLLTE alle Subunternehmer offenlegen, die er für den Cloud-Dienst benötigt.

OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst [Fachverantwortliche] (S)

Die Migration zu einem Cloud-Dienst SOLLTE auf Basis des erstellten Migrationskonzeptes erfolgen. Während der Migration SOLLTE überprüft werden, ob das Sicherheitskonzept für die Cloud-Nutzung an potenzielle neue Anforderungen angepasst werden muss. Auch SOLLTEN alle Notfallvorsorgemaßnahmen vollständig und aktuell sein.

Die Migration zu einem Cloud-Dienst SOLLTE zunächst in einem Testlauf überprüft werden. Ist der Cloud-Dienst in den produktiven Betrieb übergegangen, SOLLTE abgeglichen werden, ob der Cloud-Diensteanbieter die definierten Anforderungen des Cloud-Kunden erfüllt.

OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst (S)

Für die genutzten Cloud-Dienste SOLLTE durch den Cloud-Kunden ein Notfallkonzept erstellt werden. Es SOLLTE alle notwendigen Angaben zu Zuständigkeiten und Ansprechpartnern enthalten. Zudem SOLLTEN detaillierte Regelungen hinsichtlich der Datensicherung getroffen werden. Auch Vorgaben zu redundant auszulegenden Management-Tools und Schnittstellensystemen SOLLTEN festgehalten sein.

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (S)

Alle für die eingesetzten Cloud-Dienste erstellten Dokumentationen und Richtlinien SOLLTEN durch den Cloud-Kunden regelmäßig aktualisiert werden. Der Cloud-Kunde SOLLTE außerdem periodisch kontrollieren, ob der Cloud-Diensteanbieter die vertraglich zugesicherten Leistungen erbringt. Auch SOLLTEN sich der Cloud-Diensteanbieter und der Cloud-Kunde nach Möglichkeit regelmäßig abstimmen. Ebenso SOLLTE geplant und geübt werden, wie auf Systemausfälle zu reagieren ist.

OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (S)

Der Cloud-Kunde SOLLTE sich vom Cloud-Diensteanbieter regelmäßig nachweisen lassen, dass die vereinbarten Sicherheitsanforderungen erfüllt sind. Der Nachweis SOLLTE auf einem international anerkannten Regelwerk basieren (z. B. IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance). Der Cloud-Kunde SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzt ein Cloud-Diensteanbieter Subunternehmer, um die Cloud-Dienste zu erbringen, SOLLTE er dem Cloud-Kunden regelmäßig nachweisen, dass diese die notwendigen Audits durchführen.

OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses [Fachverantwortliche, Institutionsleitung] (S)

Wenn das Dienstleistungsverhältnis mit einem Cloud-Diensteanbieter beendet wird, SOLLTE sichergestellt sein, dass dadurch die Geschäftstätigkeit oder die Fachaufgaben des Cloud-Kunden nicht beeinträchtigt wird. Der Vertrag mit dem Cloud-Diensteanbieter SOLLTE regeln, wie das Dienstleistungsverhältnis geordnet aufgelöst werden kann.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein OPS.2.2 *Cloud-Nutzung* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE alle Anforderungen definieren, die es ermöglichen, einen Cloud-Diensteanbieter zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem SOLLTE der Cloud-Kunde regelmäßig Portabilitätstests durchführen. Im Vertrag mit dem Cloud-Diensteanbieter SOLLTEN Vorgaben festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.

OPS.2.2.A16 Durchführung eigener Datensicherungen [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE prüfen, ob, zusätzlich zu den vertraglich festgelegten Datensicherungen des Cloud-Diensteanbieters, eigene Datensicherungen erstellt werden sollen. Zudem SOLLTE er detaillierte Anforderungen an einen Backup-Service erstellen.

OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung (H)

Wenn Daten durch einen Cloud-Diensteanbieter verschlüsselt werden, SOLLTE vertraglich geregelt werden, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Wenn eigene Verschlüsselungsmechanismen genutzt werden, SOLLTE ein geeignetes Schlüsselmanagement sichergestellt sein. Bei der Verschlüsselung SOLLTEN die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt werden.

OPS.2.2.A18 Einsatz von Verbunddiensten [Fachverantwortliche] (H)

Es SOLLTE geprüft werden, ob bei einem Cloud-Nutzungs-Vorhaben Verbunddienste (Federation Services) eingesetzt werden.

Es SOLLTE sichergestellt sein, dass in einem SAML (Security Assertion Markup Language)-Ticket nur die erforderlichen Informationen an den Cloud-Diensteanbieter übertragen werden. Die Berechtigungen SOLLTEN regelmäßig überprüft werden, sodass nur berechtigten Benutzern ein SAML-Ticket ausgestellt wird.

OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Mit externen Cloud-Diensteanbietern SOLLTE vertraglich vereinbart werden, dass in geeigneter Weise überprüft wird, ob das eingesetzte Personal qualifiziert und vertrauenswürdig ist. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI beschreibt in seiner Publikation „Anforderungskatalog Cloud Computing (C5)“ Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten.

Die Cloud Security Alliance (CSA) gibt in ihrer Publikationen „Security Guidance for Critical Areas of Focus in Cloud Computing“ Empfehlungen zur Nutzung von Cloud-Diensten.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-144 „Guidelines on Security and Privacy in Public Cloud Computing“ Empfehlungen zur Nutzung von Cloud-Diensten.

Die European Union Agency for Network and Information Security (ENISA) hat folgendes weiterführendes Dokument „Cloud Computing: Benefits, Risks and Recommendations for Information Security“ zum Themenfeld Cloud Computing veröffentlicht.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in Kapitel SC 2 – Cloud Computing – Vorgaben zur Nutzung von Cloud-Diensten.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein OPS.2.2 *Cloud-Nutzung* von Bedeutung.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.35 Nötigung, Erpressung oder Korruption

G 0.36 Identitätsdiebstahl

G 0.41 Sabotage

G 0.45 Datenverlust