Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: OPS.3.1 Outsourcing für Dienstleister

1. Einleitung

Immer mehr Institutionen entscheiden sich heutzutage, bestimmte Prozesse und Aktivitäten nicht mehr vollständig selbst zu erbringen, sondern diese an einen externen Dienstleister auszulagern. Diese Entscheidung wird in der Regel aufgrund der vielfältigen Möglichkeiten getroffen, die ein solches Outsourcing-Vorhaben mit sich bringen kann. So können je nach vorhandenen Rahmenbedingungen eventuell Kosten gespart, externe Ressourcen flexibel genutzt oder eine Entlastung der eigenen Ressourcen erreicht werden, um sich stärker auf die eigenen Kernkompetenzen konzentrieren zu können. Jene Chancen gehen jedoch stets mit zum Teil erheblichen Risiken einher (hohe Abhängigkeit von externen Dienstleistern, Verlust von Kontroll- und Steuerungsmöglichkeiten sowie Risiken für die Informationssicherheit), die eine Outsourcing-Dienstleistung nicht nur scheitern lassen, sondern im schlechtesten Fall auch die Existenz der auslagernden Institution gefährden können. Umso mehr ist es von Bedeutung, jeglichen Risiken, die mit der Outsourcing-Dienstleistung einhergehen, ausreichend zu begegnen. Um diese Zielsetzung angemessen umsetzen zu können, ist eine enge Zusammenarbeit zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden unerlässlich. Der Erfolg des Outsourcing-Vorhabens liegt dabei nicht nur im Interesse der auslagernden Institution. Vielmehr hat auch der Outsourcing-Dienstleister ein großes Interesse daran, dass die Outsourcing-Ziele des Kunden zu dessen vollsten Zufriedenheit erfüllt werden. Eine Verfehlung der an den Dienstleister gestellten Anforderungen kann mitunter hohe Vertragsstrafen und weitere juristische Auswirkungen zur Folge haben, die sich nicht nur finanziell erheblich auf den Dienstleister auswirken können, sondern auch dessen Reputation nachhaltig schädigen können.

Aufgrund dieser Risiken werden nachfolgend Maßnahmen beschrieben, die der Outsourcing-Dienstleister im Rahmen jeder Phase einer Outsourcing-Dienstleistung umsetzen sollte.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins OPS.3.1 *Outsourcing für Dienstleister* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein OPS.3.1 Outsourcing für Dienstleister

OPS.3.1.M1 Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung (B)

Der Outsourcing-Dienstleister muss gemeinsam mit dem Outsourcing-Kunden in einem Grobkonzept mögliche Interaktionsprozesse, Regelungen und Richtlinien festlegen, auf denen die Zusammenarbeit basiert. Das Grobkonzept definiert das Outsourcing-Management mit den Führungs- und Kontrollfunktionen sowie Schnittstellen zwischen den Parteien und zu anderen Prozessen (z. B. Notfallmanagement, Informationssicherheit und Datenschutz), um so eine transparente Outsourcing Governance in nachvollziehbarer Weise abzubilden und eine schnelle Reaktion auf Ereignisse zu ermöglichen.

Das Grobkonzept sollte ebenfalls die Betrachtung der folgenden Faktoren einschließen:

Ziele des Outsourcing-Vorhabens

Es ist zu definieren, welche Chancen und Ziele der Outsourcing-Kunde mit dem Vorhaben verbindet, welche Mehrwerte geschaffen werden sollen und wie der Projekterfolg gemessen werden kann. So sollen spezifische, messbare und realistische Ziele in einem vordefinierten Zeitrahmen erreicht werden. Um eine Aussage darüber treffen zu können, ob die Outsourcing-Dienstleistung erfolgreich verläuft, muss die Leistung des Outsourcing-Dienstleisters gegenüber dem Outsourcing-Kunden nachvollziehbar darstellbar sein.

Bei den Zielen eines Outsourcing-Vorhabens müssen insbesondere die Ziele mit Bezug auf Informationssicherheit berücksichtigt werden. Um diese Ziele messen zu können, eignen sich sogenannte Security Service Level Agreements (SLAs). Diese sollten im Sicherheitskonzept schriftlich fixiert und in regelmäßigen Abständen geprüft werden.

Für den Outsourcing-Dienstleister ist es in jedem Fall von Interesse, bei der Definition dieser Messgrößen mitzuwirken, da mittels dieser die Qualität seiner Leistungserbringung gemessen werden soll. Mögliche Messgrößen für quantifizierbare Leistungsbewertungen könnten sein:

- Meilensteine des Outsourcing-Vorhabens (z. B. Planung, Migration, Betrieb).
- Security Level Agreements (z. B. Angaben zur Verfügbarkeit).

Qualitäten des Outsourcing-Dienstleisters

Die Anforderungen an die von den Outsourcing-Dienstleistern erbrachten Services sind anwenderspezifisch und individuell. Eine Vorabbetrachtung der Erwartungen des Outsourcing-Kunden, z. B. hinsichtlich der Kapazitäten und Verfügbarkeiten der Services, kann vor dem Beginn der Vertragsverhandlungen Missverständnisse vermeiden.

Der Outsourcing-Dienstleister sollte gegenüber dem Outsourcing-Kunden idealerweise Qualitäten präsentieren können. Zu den Qualitäten eines Outsourcing-Dienstleisters kann z. B. gehören, dass eine gültige ISMS-Zertifizierung vorliegt, die bereits den Anwendungsbereich des Outsourcing-Kunden

abdeckt. Aber auch Referenz-Kunden, die der Outsourcing-Kunde bei Bedarf vor Vertragsunterzeichnung kontaktieren kann, können sinnvoll sein, um die eigenen Qualitäten im Umgang mit Informationssicherheit zu präsentieren.

Abhängigkeiten von externen Drittparteien

In einer komplex vernetzten Geschäftswelt mit einem hohen Spezialisierungsgrad bestehen viele Abhängigkeiten. In der Regel setzt der Outsourcing-Dienstleister ebenfalls weitere Drittparteien ein, um z. B. Wartungen an verschiedenen Anlagen durchführen zu lassen. Diese Abhängigkeiten sollten von Seiten des Outsourcing-Dienstleisters dem Outsourcing-Kunden bereits vor der Vertragsunterzeichnung mitgeteilt werden.

Diese Interdependenzen bei der Serviceerbringung sollten in der nötigen Detailtiefe dargestellt werden, um auch hier mögliche Risiken zu erfassen und diese entsprechend behandeln zu können. Eine Unterbrechung der Service-Erbringung durch den Outsourcing-Dienstleister kann empfindliche Vertragsstrafen nach sich ziehen und der Reputation schaden. Zudem ist eine offene Kommunikation hinsichtlich möglicher Risiken Grundlage einer erfolgreichen Outsourcing-Beziehung.

Durch den Outsourcing-Dienstleister sind z. B. darzustellen:

- Kritische Geschäftsprozesse, die im Rahmen eines Outsourcings an Dritte vergeben sind:
- Insbesondere bestehende IT-Outsourcing-Verträge,
- Externe Datenhaltung (Dienstleister, Standorte).
- Telekommunikationsanbieter.
- Kooperation mit Dritten im Zusammenhang mit der Notfallvorsorge (z. B. Ausweicharbeitsplätze).

Sicherheitskultur

Ein wichtiger Faktor bei einer langfristigen Bindung im Rahmen einer Outsourcing-Dienstleistung ist die Beachtung der unterschiedlichen Sicherheitskulturen. Hierzu sollte die Sicherheitskultur sowohl des Outsourcing-Dienstleisters als auch des Outsourcing-Kunden reflektierend in den Blick genommen werden. Zu beachten sind beispielsweise:

- Gesellschaftlich-kulturelle Unterschiede und Gemeinsamkeiten, die auch die Organisationskultur prägen.
- Unternehmenswerte und -visionen.
- Führungs- und Entscheidungsstile.
- Formelle und informelle soziale Codes.
- Ethische Standards.
- Einstellung zu Risiken, Risikoappetit.

Insbesondere der sichere Umgang mit Daten und Informationen seitens der Mitarbeiter des Outsourcing-Dienstleisters sollten klar geregelt sein. Der Outsourcing-Kunde verlässt sich in erster Linie auf die Zuverlässigkeit des Outsourcing-Dienstleisters bei der Auswahl seiner Mitarbeiter. Der Outsourcing-Dienstleister sollte bei der Zuordnung von Aufgaben zu Mitarbeitern deshalb auf das Arbeitsklima in den jeweiligen Teams achten.

OPS.3.1.M2 Vertragsgestaltung mit den Outsourcing-Kunden (S)

Bei der Gestaltung von Outsourcing-Verträgen ist darauf zu achten, alle Aspekte eines Outsourcing-Verfahrens bei der Vertragsgestaltung durch SLAs zu berücksichtigen und gemeinsam mit dem Outsourcing-Kunden eine genaue Analyse der Aufgaben und Prozesse, die übernommen werden sollen, durchzuführen. Alle nicht im Vorhinein definierten Merkmale der Leistungserbringung führen meist zu Mehrkosten, insbesondere beim Outsourcing-Kunden. Das schädigt das Geschäftsverhältnis

zwischen den Vertragsparteien und schwächt die Verhandlungsposition des Outsourcing-Dienstleisters bei Vertragsverlängerungen.

Um diesem Umstand Rechnung zu tragen, sollten alle relevanten Leistungsbeschreibungen für die Outsourcing-Dienstleistung im Vertragswerk zu berücksichtigen und möglichst genau zu definieren. Dies ist insbesondere dahingehend von besonderer Bedeutung, dass eventuelle Diskrepanzen zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden hinsichtlich unterschiedlicher Vorstellungen der Leistungserbringung im Zuge des Outsourcing-Projektes bereits im Vorfeld verhindert werden können. Bei unrechtmäßigen Vorwürfen seitens des Outsourcing-Kunden in Hinsicht auf eine nicht oder nur mangelhaft erbrachte Leistung kann der Outsourcing-Kunde sich auf die entsprechende Leistungsbeschreibung im Rahmen des Vertragswerkes berufen.

Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen dabei immer von der jeweiligen Outsourcing-Dienstleistung ab. Je höher beispielsweise der Schutzbedarf der ausgelagerten IT-Systeme und Anwendungen des Outsourcing-Kunden ist, desto sorgfältiger und detaillierter muss der Vertrag zwischen Outsourcing-Kunden und Outsourcing-Dienstleister in Hinsicht auf die zu ergreifenden Sicherheitsmaßnahmen ausgehandelt werden. So hat der Outsourcing-Dienstleister über die Einhaltung der Anforderungen aus dem IT-Grundschutz-Kompendium hinaus oftmals zusätzliche Sicherheitsanforderungen aufgrund von einem erhöhten Schutzbedarf zu erfüllen (siehe unter anderem OPS.3.1.M3 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*.

Folgende aufgelistete Aspekte sollten aus Sicht des Outsourcing-Dienstleisters bei der Vertragsgestaltung geregelt werden, um die Leistungserbringung entsprechend klarer Vorgaben von Seiten des Outsourcing-Kunden gewährleisten zu können. Der Übersicht halber sind die beschriebenen Aspekte den jeweiligen Themenbereichen zugeordnet. Weitere Hinweise und Details können diversen Bausteinen des IT-Grundschutz-Kompendiums entnommen werden:

Infrastruktur (siehe z. B. Baustein INF.2 *Rechenzentrum*)

- Umfang der gemeinsam genutzten Infrastruktur.
- Anforderungen des Outsourcing-Kunden an die Absicherung der gemeinsam genutzten Infrastruktur.
- Verbleib der Eigentumsrechte aller Bestandteile der Infrastruktur.

Organisatorische Regelungen / Prozesse (siehe z. B. Baustein ORP.1 *Organisation*)

- Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements) sind vertraglich zu fixieren. Dies sollte bereits in der Phase der Vertragsgestaltung selbst berücksichtigt werden, da Sicherheitsanforderungen des Outsourcing-Kunden unter Umständen Schlüsse auf die vorhandenen Sicherheitsmaßnahmen zulassen.
- Festlegung von Kommunikationswegen und Ansprechpartnern.
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten.
- Integration der Dienstleistung in den Wertschöpfungsprozess des Outsourcing-Kunden.
- Arbeitsteilung bei der Serviceerbringung / Mitwirkungspflichten des Outsourcing-Kunden.
- Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen bei beiden Vertragsparteien.
- Regelmäßige Abstimmungsrunden.
- Vorgehensweise bei der Leistungsanpassung.
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses).auf welches IT-System zu? Wie sind die Zuständigkeiten und Rechte?
- Zugang-, Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Dienstleisters zu den Räumlichkeiten und IT-Systemen des Outsourcing-Kunden.

- Zugang-, Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Kunden zu den Räumlichkeiten und IT-Systemen des Outsourcing-Dienstleisters.
- physischer Aufbewahrungsort von Daten.

Personal (siehe z. B. Baustein ORP.2 *Personal*)

- Gestaltung der Arbeitsplätze von Mitarbeitern des Outsourcing-Dienstleisters, die zum Outsourcing-Kunden entsandt werden (z. B. die Einhaltung der Bildschirmarbeitsplatzrichtlinie).
- Festlegung und Abstimmung von Vertretungsregelungen bei beiden Vertragspartnern.
- Verpflichtung zu Fortbildungsmaßnahmen.

Notfallvorsorge (siehe z. B. Baustein DER.4 *Notfallmanagement*)

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit.
- Erforderliche Handlungen beim Eintreten eines Störfalls.
- Vom Outsourcing-Kunden geforderte Reaktionszeiten und Eskalationsstufen.
- Zeitnahe Information des Outsourcing-Kunden über eingetretene Sicherheitsvorfälle.
- Mitwirkungspflicht des Outsourcing-Kunden bei der Behebung von Notfällen.
- Art der Einbindung in Notfallübungen und zeitliche Abfolge von Notfallübungen des Outsourcing-Kunden.
- Anforderungen des Outsourcing-Kunden an die Art und den Umfang der Datensicherung.
- Vereinbarung, ob bzw. welche IT-Systeme redundant ausgelegt sein müssen.

Von besonderer Bedeutung können Regelungen für Fälle höherer Gewalt sein. Des Weiteren sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Outsourcing-Dienstleisters die Verfügbarkeit von Daten und IT-Systemen sichergestellt werden kann. Besonders wenn Outsourcing-Dienstleister und Outsourcing-Kunde unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Outsourcing-Kunden von derartigen Vorkommnissen gänzlich überrascht werden.

Juristische Rahmenbedingungen, Haftung

Die Eigentums- und Urheberrechte an IT-Systemen, Software und Schnittstellen sind festzulegen. Zudem ist die Weiterverwendung der vom Outsourcing-Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.

Es sind angemessene Kündigungsfristen zu vereinbaren. In diesem Zusammenhang sollte darauf geachtet werden, dass innerhalb der Kündigungsfristen ausreichend Zeit für den Outsourcing-Kunden bleibt, die ausgelagerten Prozesse wieder selbst zu übernehmen oder auf einen anderen Dienstleister zu übertragen (siehe OPS.3.1.M15 *Geordnete Beendigung eines Outsourcing-Verhältnisses*).

Oftmals sind Outsourcing-Kunden bestrebt, Sanktionen oder Schadensersatzpflichten für eine eventuelle Nichteinhaltung der Dienstleistungsqualität festzulegen. Aus Sicht des Outsourcing-Dienstleisters sind dahingehend folgende Aspekte zu berücksichtigen bzw. mit dem Outsourcing-Kunden zu regeln:

- Quantifizierbarkeit eines eingetretenen Schadens.
- Messbarkeit eines Imageschadens.
- Verfahren bei Insolvenz des Outsourcing-Dienstleisters.
- Verfahren bei Eintreten von katastrophalen Schäden.

Weiterverlagerungen

Die Möglichkeiten zur Einbindung von Dritten, Subunternehmern und Unterauftragnehmern durch den Outsourcing-Dienstleister sind zu regeln. Allgemein empfiehlt es sich, dies nicht grundsätzlich auszuschließen, sondern sinnvolle Bedingungen festzulegen. Grundsätzlich sollte jede Weiterverlagerung nur dann zulässig sein, wenn alle Anforderungen erfüllt werden, die im Rahmen der bestehenden Outsourcing-Beziehung an den Dienstleister gestellt werden.

Mandantenfähigkeit

Die Anforderungen hinsichtlich einer Trennung von IT-Systemen und Anwendungen verschiedener Kunden des Outsourcing-Dienstleisters müssen in einem Mandantenkonzept geregelt werden (siehe OPS.3.1.M7 *Erstellung eines Mandantentrennungskonzeptes durch den Outsourcing-Dienstleister*). Anhand dieser Regelungen ist es dem Outsourcing-Dienstleister im weiteren Projektverlauf möglich, eine anforderungsgerechte Mandantentrennung zu gewährleisten.

Falls notwendig, muss die physische Trennung (d. h. dedizierte Hardware) vereinbart werden.

Falls notwendig, muss vereinbart werden, dass die vom Outsourcing-Dienstleister eingesetzten Mitarbeiter nicht für andere Outsourcing-Kunden eingesetzt werden dürfen. Es kann auch sinnvoll sein, diese auf Verschwiegenheit zu verpflichten, sodass die eingesetzten Mitarbeiter nicht mit anderen Mitarbeitern des Outsourcing-Dienstleisters anwenderbezogene Informationen austauschen dürfen.

Änderungsmanagement und Testverfahren

Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Outsourcing-Kunde immer in der Lage ist, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn beispielsweise gesetzliche Vorgaben geändert wurden. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert werden soll.

In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener IT-Systeme zu regeln. Nicht selten übernimmt der Outsourcing-Dienstleister selbst entwickelte IT-Systeme oder Software vom Outsourcing-Kunden, der damit die Fähigkeit verliert, diese in seinem Sinne weiterzuentwickeln. Der Evolutionspfad von IT-Systemen muss daher geregelt werden.

Der vom Outsourcing-Kunden geforderte Zeitrahmen für die Behebung von Fehlern und Störungen ist festzulegen.

In Hinsicht auf Testverfahren für neue Hard- und Software sind die von Seiten des Outsourcing-Dienstleisters einzuhaltenden Regelungen zu vereinbaren. Dabei sollten insbesondere folgende Aspekte geklärt werden:

- Regelungen für Updates und Systemanpassungen.
- Trennung von Test- und Produktionssystemen.
- Zuständigkeiten bei der Erstellung von Testkonzepten.
- Festlegen von zu benutzenden Testmodellen.
- Zuständigkeiten bei Outsourcing-Kunden und Outsourcing-Dienstleister für die Erstellung von Testkonzepten und die Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Outsourcing-Kunden, Abnahme- und Freigabeprozeduren).
- Informationspflicht und Absprache vor wichtigen Eingriffen ins IT-System (Negativbeispiel: Der Dienstleister spielt eine neue Version des Betriebssystems auf dem Server ein. Durch unerwartete Fehler dabei werden wichtige Anwendungen gestört, ohne dass der Kunde sich vorbereiten konnte).
- Genehmigungsverfahren für die Durchführung von Tests.
- Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit).

Kontrollen und Prüfungen

Die Dienstleistungsqualität und Informationssicherheit müssen regelmäßig kontrolliert werden. Der Dienstleister muss daher mit dem Kunden abstimmen, welche Auskunfts-, Einsichts-, Zugriff-,

Zutritts- und Zugangsrechte eingeräumt werden. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies ebenfalls im Vertrag geregelt werden.

Der Dienstleister muss allen Institutionen, die beim Kunden Prüfungen durchführen müssen (z. B. Aufsichtsbehörden), entsprechende Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) einräumen.

OPS.3.1.M3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (S)

Der Outsourcing-Kunde sollte ein eigenes Sicherheitskonzept für das Outsourcing-Vorhaben erstellen (siehe Baustein OPS.2.1 *Outsourcing für Kunden*). Dieses bildet die Grundlage für die Sicherheitsanforderungen an den Outsourcing-Dienstleister im Rahmen des gemeinsamen Outsourcing-Projektes. Der Outsourcing-Dienstleister sollte aufbauend darauf ein Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben erstellen und kontinuierlich fortschreiben. Die folgenden allgemeinen Aspekte sind darin zu berücksichtigen:

- Einflussbereich und Mitwirkungspflichten des Outsourcing-Kunden.
- Schnittstellen und Kommunikation zwischen den Outsourcing-Partnern, aber auch zwischen dem Anwendungsbereich des Outsourcing-Kunden wie auch den Anwendungsbereichen der anderen Kunden.
- Abgestimmter Informationsverbund mit klarer Abgrenzung zum Sicherheitskonzept des Outsourcing-Kunden.

Der Outsourcing-Kunde sollte alle schutzbedürftigen Informationen entsprechend ihrer strategischen Bedeutung für seine Institution klassifizieren und diesen Schutzbedarf dem Outsourcing-Dienstleister kommunizieren. Darauf aufbauend sollte eine gemeinsame Klassifikation erarbeitet werden. Die umzusetzenden Sicherheitsmaßnahmen basieren auf dieser Klassifikation.

Vertraglich festgelegte Sicherheitsanforderungen (siehe OPS.3.1.M2 *Vertragsgestaltung mit den Outsourcing-Kunden*) sind zu erfüllen und dem Outsourcing-Kunden auf dessen Anfrage auch adäquat nachzuweisen. Des Weiteren ist zu beachten, dass während der Migrationsphase Änderungsbedarf entstehen kann. Um darauf zu reagieren, müssen die Vertragsparteien sich zu konkreten Sicherheitsmaßnahmen abstimmen. Hierfür sollten vom Outsourcing-Dienstleister Ressourcen in der Planung berücksichtigt werden.

Die Umsetzung des Sicherheitskonzepts sollte regelmäßig überprüft werden.

OPS.3.1.M4 Festlegung der möglichen Kommunikationspartner (S)

Zwischen Outsourcing-Dienstleister und Outsourcing-Kunden sollte im Vorfeld abgestimmt, dokumentiert und vertraglich vereinbart werden, welche internen und externen Kommunikationsteilnehmer welche Informationen über das jeweilige Outsourcing-Projekt erhalten dürfen. Während des Outsourcing-Projektes ist diese Dokumentation regelmäßig und anlassbezogen auf ihre Aktualität hin zu prüfen. So sollte stets sichergestellt sein, dass die angegebenen Ansprechpartner die ihnen ursprünglich zugeordnete Funktion noch wahrnehmen.

Sollen Informationen an einen Kommunikationspartner außerhalb der Institution des Outsourcing-Dienstleisters übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Diesbezüglich müssen Möglichkeiten und Rahmenbedingungen im Vorfeld mit dem Kunden abgestimmt und vertraglich festgelegt werden.

Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat bzw. erhalten wird.

Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Hierfür ist es erforderlich, dass alle

schutzbedürftigen Informationen entsprechend ihrer strategischen Bedeutung für die Institution klassifiziert sind.

Mittels einer Kommunikationsmatrix können alle Kommunikationspartner entweder den Klassifizierungen oder den Informationen selbst zugeordnet werden. Das ermöglicht eine übersichtliche Darstellung der Informationsverteilung.

Des Weiteren sollten auch die zu nutzenden Kommunikationswege hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit geprüft und überwacht werden, da auch auf diesem Wege Informationen an unberechtigte Empfänger gelangen können.

Die Empfänger sind darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (siehe zum Beispiel BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenübertragung oder Datenträgeraustausch zu erhalten.

OPS.3.1.M5 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters (S)

Im Zuge einer Outsourcing-Dienstleistung ist es gegebenenfalls erforderlich, dass sich Mitarbeiter des Outsourcing-Dienstleisters im Rahmen ihrer Aufgabenerfüllung über einen längeren Zeitraum in den Räumlichkeiten des Outsourcing-Kunden aufhalten müssen.

Jene Mitarbeiter sollten ausreichend eingewiesen und über hausinterne Regelungen und Vorschriften des Outsourcing-Kunden zur Informationssicherheit sowie die organisationsweite Informationssicherheitspolitik unterrichtet werden. Geschieht dies nicht von Seiten des Outsourcing-Kunden aus, sollte der Outsourcing-Dienstleister darauf hinwirken. Es ist von beiderseitigem Interesse, dass allen Beteiligten entsprechende Regelungen und Vorschriften bekannt sind und angewendet werden.

Vor dem Einsatz der Mitarbeiter des Outsourcing-Dienstleisters sollten eventuelle, von Seiten des Outsourcing-Kunden gestellte, Anforderungen (Führungszeugnis, Qualifikationen etc.) an das einzusetzende Personal identifiziert und deren Erfüllung sichergestellt werden.

Zudem sollte der Outsourcing-Dienstleister mit Blick auf alle Mitarbeiter, die im Rahmen ihrer Aufgabenerfüllung Zugang zu vertraulichen Unterlagen und Daten des Outsourcing-Kunden erhalten, sicherstellen, dass diese sich schriftlich zur Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und Regelungen des Outsourcing-Kunden verpflichten, z. B. über eine Verschwiegenheitserklärung (siehe unter anderem Baustein ORP.5 *Anforderungsmanagement*).

Es muss Vertretungsregelungen in allen Bereichen geben. Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss insbesondere dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, sobald dies von den Abläufen her gefordert wird.

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt überprüft werden. Nachfolger müssen eingearbeitet werden, Unterlagen sind zurückzugeben und erteilte Berechtigungen sind wieder zu entziehen. Vor der Verabschiedung sollte noch einmal explizit auf Verschwiegenheitsverpflichtungen hingewiesen werden.

OPS.3.1.M6 Regelungen für den Einsatz von Fremdpersonal (S)

Auch Outsourcing-Dienstleister greifen ihrerseits häufig auf Dienstleister zurück, um bestimmte Teilaufgaben erledigen zu lassen. Wenn externe Mitarbeiter Zugang zu vertraulichen Unterlagen und Daten des Outsourcing-Kunden bekommen könnten, ist dies dem Outsourcing-Kunden mitzuteilen. Der ISB des Outsourcing-Kunden sollte dann prüfen, ob damit die gestellten Sicherheitsanforderungen weiterhin erfüllbar sind und ob sich dadurch weitere Sicherheitsanforderungen ergeben.

Externe Mitarbeiter, die über einen längeren Zeitraum für den Outsourcing-Dienstleister tätig sind, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen

Regelungen zu verpflichten. Beim Einsatz von externen Mitarbeitern muss außerdem auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit in ihre Aufgaben eingewiesen werden. Sie sind – so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist – über hausinterne Regelungen und Vorschriften zur Informationssicherheit zu unterrichten.

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren. Ebenso sollte gewährleistet sein, dass sich diese mit den von ihnen eingesetzten IT-Anwendungen auskennen und auch die erforderlichen Sicherheitsmaßnahmen beherrschen.

Wenn im Rahmen der auszuführenden Aufgaben einmalig zum Einsatz kommendes Fremdpersonal (z. B. Wartungstechniker) hinzugezogen werden soll, so sollte dieses Fremdpersonal wie Besucher behandelt werden. Dazu sollten die gängigen Regelungen zum Besuchermanagement eingehalten werden. Es muss nachvollziehbar sein, welche Befugnisse das Fremdpersonal hat und der Einsatz sollte entsprechend dem Schutzbedarf angemessen eingewiesen und begleitet werden.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse, erhaltenen Unterlagen und Betriebsmittel erfolgen. Zudem sind dem Outsourcing-Kunden physische Zutrittsmittel zu übergeben (z. B. Schlüssel, Zugangskarten). Eventuell bestehende Verschwiegenheitsverpflichtungen bleiben auch nach der Zusammenarbeit mit dem Outsourcing-Kunden gültig und müssen demnach weiterhin eingehalten werden (siehe auch ORP.2 *Personal*).

OPS.3.1.M7 Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister (S)

Häufig werden von mehreren Institutionen zentrale IT-Infrastrukturen oder Dienste eines Outsourcing-Dienstleisters gemeinsam genutzt. Hierbei können auch Anwendungen gemeinsam betrieben und genutzt werden, wobei Datenhaltung und Datenverarbeitung z. B. infolge rechtlicher Anforderungen oder aufgrund von Betriebs- und Geschäftsgeheimnissen getrennt erfolgen müssen. In diesen Fällen wird häufig von mandantenfähigen Anwendungen gesprochen, wobei jeder nutzenden Institution ein Mandantenbereich, kurz Mandant, zugeordnet wird.

In jedem dieser Fälle ist durch ein geeignetes Mandantenkonzept sicherzustellen, dass die Anwendungen mandantenfähig betrieben werden. Dazu gehört, dass jeder Outsourcing-Kunde innerhalb seines Bereichs, also seines Mandantensystems, die fachlichen Vorgaben (z. B. bezogen auf Protokollierungsumfang und Speicherfristen) umsetzen sowie seinen Kontrollpflichten nachkommen kann. Das Mandantenkonzept ist durch den Outsourcing-Dienstleister zu erstellen und dem Outsourcing-Kunden zur Verfügung zu stellen. Dieser muss sich überzeugen, dass das Mandantenkonzept für seinen Schutzbedarf eine angemessene Sicherheit bietet, bevor solche IT-Systeme oder Dienste gemeinsam mit weiteren Kunden genutzt werden. Das Mandantenkonzept ist somit Bestandteil des Sicherheitskonzeptes, das für ein Outsourcingvorhaben zu stellen ist.

Auch unter datenschutzrechtlichen Gesichtspunkten sind Anforderungen an die Trennung von Mandanten zu beachten. Hinweise dazu gibt die "Orientierungshilfe Mandantenfähigkeit" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder.

Wenn eine Anwendung neu beschafft, erstellt oder wesentlich geändert wird, muss außerdem zunächst grundsätzlich sichergestellt sein, dass diese Anwendung Mandanten sauber trennen kann.

Ein Mandantenkonzept sollte mindestens folgende Punkte berücksichtigen:

- Geeignete Rechtsgrundlagen: Rechtliche Vorgaben dürfen einem gemeinsamen, mandantenfähigen Verfahrensbetrieb nicht entgegenstehen. Ferner muss sichergestellt werden, dass die technische Ausgestaltung der Mandantentrennung dem Schutzbedarf der Daten in den jeweiligen Mandanten entspricht.
- Abgeschlossenheit von Transaktionen: Datenverarbeitungsschritte, die in einem Mandanten durchgeführt werden, dürfen nicht dazu führen, dass die Daten in anderen Mandanten verändert werden oder lesend auf sie zugegriffen werden kann.
- Konfigurative Unabhängigkeit der Mandanten untereinander: Es sollten mindestens zwei administrative Ebenen vorhanden sein. Die erste Ebene dient der Mandantenadministration:

Hier werden Mandantensysteme eingerichtet und gelöscht, mandantenübergreifende konfigurative Einstellungen durchgeführt, die Rollen der Mandantenadministratoren zugewiesen, die mandantenübergreifende Protokollierung angestoßen und deren Revision durchgeführt. Die zweite Ebene dient der Administration eines Mandantensystems: Hier werden die Berechtigungen im Mandantensystem vergeben, mandanteninterne Konfigurationen durchgeführt, die mandanteninterne Protokollierung konfiguriert und die Protokollrevision durchgeführt.

- Trennung von Berechtigungskontexten: Jeder Mandant hat seinen eigenen, abgeschlossenen Berechtigungskontext. Die Vergabe oder Veränderung von Berechtigungen durch die Administratoren der jeweiligen Mandanten darf sich nicht auf Berechtigungen in anderen Mandanten auswirken.
- Es muss eine administrative Ebene zur Mandantenadministration seitens des Betreibers geben, die aber keine Berechtigung zur Verarbeitung von Daten innerhalb eines Mandanten besitzen sollte.
- Trennung von Protokollierungskontexten: Protokollrevisoren eines Mandatensystems dürfen keinen Zugriff auf Protokolldaten anderer Mandantensysteme haben. Beispielsweise können Mandanten eigene Log-Dateien haben. Eine andere Lösung könnte sein, dass eine Institution über vom Dienstleister entsprechend eingerichtete Filter oder Report-Generatoren auf die Protokolldaten ihres Mandanten zugreifen kann.
- Beschränkung der mandantenübergreifenden Datenverarbeitung: Die Ebene der Mandantenadministration sollte grundsätzlich keine Verarbeitung von Daten innerhalb eines Mandanten außerhalb der Mandantenadministration zulassen. Der Datenaustausch zwischen Mandanten sollte über definierte und geeignet abgesicherte Schnittstellen erfolgen.

Die Umsetzung dieser Anforderungen kann auf vielfältige Weise erfolgen. Eine herausragende Rolle spielt dabei ein geeignetes Rollen- und Berechtigungskonzept innerhalb von Anwendungen. Darüber hinaus können auf der Infrastruktur- und Diensteebene hierzu verschiedene Methoden wie z. B. Virtualisierungstechniken eingesetzt werden:

- Einsatz verschiedener Datenbanken (auch Instanzen genannt) in einem gemeinsamen Datenbankmanagementsystem (DBMS).
- VPD (Virtual Private Database) auf der Diensteebene bei Datenbanken.
- Speicherung von mit einem Mandantenattribut versehenen Datensätzen in einer gemeinsamen Datenbank und gemeinsamen Tabellen, sodass die Mandantentrennung durch die Anwendung erfolgt.
- Virtuelle Maschinen auf der Systemebene.
- VLAN (Virtual LAN), VRF (Virtual Routing and Forwarding), VPN (Virtual Private Network) in der Netzinfrastruktur.

Der Outsourcing-Kunde sollte prüfen, ob die vom Outsourcing-Dienstleister gewählte Lösung zur Mandantentrennung effektiv ist.

OPS.3.1.M8 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner (S)

Immer mehr Unternehmen und Behörden schließen ihre bisher nach außen abgeschotteten Netze zu Netzverbünden zusammen, sogenannten Extranets. Bei der Anbindung des Netzes des Outsourcing-Dienstleisters an das Netz des Outsourcing-Kunden ist es erforderlich, dass eine detaillierte Vereinbarung (Data Connection Agreement, DCA) geschlossen wird, bevor eine Netzanbindung erfolgt.

Hierdurch müssen die jeweiligen Zugriffsrechte des Outsourcing-Dienstleisters und des Outsourcing-Kunden genau definiert werden. Ebenso wichtig ist dabei die Frage, welcher Anwenderkreis mit

welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf das Netz des Dienstleisters und umgekehrt erhalten soll.

Die Vereinbarung sollte folgende Bestandteile umfassen:

- Eine Beschreibung dessen, was die Vereinbarung insgesamt umfasst, inklusive einer Beschreibung der betroffenen Informationsverbünde.
- Eine Abstimmung über den jeweiligen Schutzbedarf und die Klassifikation von Daten (es muss ein gemeinsames Verständnis erzielt werden).
- Eine Festlegung der Verantwortlichen (Wer trägt die Verantwortung für die Einhaltung der Vertragsbedingungen?).
- Die Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse.
- Die erforderlichen Informationen zur Klassifizierung organisatorischer und technischer Probleme als solche sowie sicherheitsrelevanter Ereignisse.
- Informationen und Festlegungen zur netzinternen Verschlüsselung.
- Welche Dienste (z. B. SSH, HTTPS) zur Verfügung gestellt werden und welche nicht.
- Welche IT-Plattformen, Anwendungen und Datenformate eingesetzt werden.
- Ob sich aus der Netzanbindung Anforderungen an die Verfügbarkeit von Netz- oder IT-Komponenten beim jeweiligen Partner ergeben (Performance, maximale Ausfallrate).
- Wer was protokollieren darf bzw. muss, wo die Protokollierungsdaten abgelegt werden und wer auf die Protokollierungsdaten zugreifen darf (dies kann insbesondere in Notsituationen wichtig sein).
- Inwieweit ein regelmäßiger Austausch von Protokollierungsdaten erfolgen soll.
- Welche Sicherheitsmaßnahmen gewährleistet werden müssen und wie deren Einhaltung überprüft wird.
- Eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden.
- Eine Haftungs- bzw. Schadensersatzregelung (hierin sollten unter anderem die Bedingungen für die Trennung der Netzanbindung, Haftung bei Schadprogrammen oder Hackerangriffen, Vertragsstrafen bei nicht erfüllter Leistung bzw. Haftungsübernahme bei Inanspruchnahme für fremde Inhalte geklärt sein).
- Eine Regelung über Auskunftspflichten bei aufgetretenen Sicherheitslücken.
- Eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen).
- Eine Beschreibung, inwieweit weitere Vertragspartner in die Vereinbarung eingebunden werden, z. B. durch gemeinsame Nutzung von Applikationen oder als Dienstleister für einen der Vertragspartner.
- Die Laufzeit sowie Anpassungsmöglichkeiten der Vereinbarung (Technik entwickelt sich schnell weiter, d. h. auch die Vereinbarungen über deren Nutzung müssen ständig angepasst werden).

Verantwortlich für die Erstellung der Vereinbarung sollten die Personen sein, die auch für die Einhaltung der getroffenen Regelungen verantwortlich sind. Muss aufgrund von Problemen die Verbindung der Netze zeitweise getrennt werden, sollten jedoch alle betroffenen Personen miteinbezogen werden, da sich deren Anforderungen stark unterscheiden können, jedoch berücksichtigt werden sollten.

Eine Netzanbindung an Netze Dritter sollte nur aktiviert werden, wenn bei beiden Partnern alle für den vereinbarten Schutzbedarf angemessenen Sicherheitsmaßnahmen umgesetzt wurden und keine erkennbaren Sicherheitsmängel mehr vorliegen. Outsourcing-Dienstleister sollten sich auch von dem Sicherheitsniveau der Outsourcing-Kunden überzeugen, beispielsweise durch einen IT-Grundschutz-Check oder Stichproben vor Ort. Wird die gemeinsame IT-Infrastruktur durch eine Sicherheitslücke des Outsourcing-Kunden kompromittiert, wird sich im Nachhinein der Outsourcing-Dienstleister ebenfalls mit dem Vorwurf der Nachlässigkeit konfrontiert sehen. Zudem sollte eine sofortige Beseitigung aller identifizierten Sicherheitsmängel angestrebt werden. Im Echtbetrieb ist die Verfügbarkeit eines lauffähigen Produktes meist deutlich höher priorisiert, als die Behebung etwaiger Sicherheitsmängel, die dann zu dauerhaften Schwachstellen werden können.

Dem Outsourcing-Kunden und möglichen Dritten sollten nur die Dienste zur Verfügung gestellt werden, die zum einen vertraglich vereinbart worden sind und zum anderen unbedingt erforderlich sind. Auf welche Bereiche des eigenen Netzes Dritten Zugriff gewährt wird, muss abhängig gemacht werden von der Art der bestehenden Beziehungen zwischen den Vertragspartnern und vom gegenseitigen Vertrauen zwischen diesen. Bei ausländischen Partnern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie, Datenschutz und Urheberrecht.

Sollte es zu Sicherheitsvorfällen kommen, bei deren Behebung die Verbindung getrennt werden muss, muss klar definiert sein, wer dies wann tun darf. Es ist ebenfalls zu klären, welche Personen über diesen Vorgang zu informieren sind und welche Eskalationsschritte vorgesehen sind.

OPS.3.1.M9 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern (S)

Für den regelmäßigen Datenaustausch zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden sollten Vereinbarungen getroffen werden, die dessen reibungslosen und sicheren Ablauf sicherstellen.

Solche Vereinbarungen sollten insbesondere die folgenden Bestandteile umfassen:

- Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Herausforderungen und insbesondere für sicherheitsrelevante Ereignisse
- Festlegung der erforderlichen technischen und organisatorischen Rahmenbedingungen, also beispielsweise darüber,
    - welche Anwendungen und Datenformate unterstützt werden und
    - welche Verfügbarkeit und welche Reaktionsgeschwindigkeit bei den Partnern zu gewährleisten ist (wie häufig sind Nachrichten zu lesen und wie schnell sind sie zu beantworten).
- Festlegung der Sicherheitsmaßnahmen, welche beim Datenaustausch gewährleistet werden müssen, z. B.
    - Überprüfung der Daten auf Schadsoftware vor und nach dem Austausch,
    - Schutz der Daten vor Transportschäden und unbefugtem Zugriff bei der Übermittlung (verschlossene Behältnisse, Checksummen, Verschlüsselung, Signaturen),
    - Regelung des Schlüsselmanagements,
    - Löschung der Daten auf der Senderseite frühestens nach der Bestätigung des korrekten Empfangs (falls die Löschung erforderlich ist).
- Eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden.
- Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen).

- Verpflichtung auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen

Weitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in Baustein CON.9 *Informationsaustausch*.

OPS.3.1.M10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb

Nachdem ein Outsourcing-Vorhaben umgesetzt wurde, muss die Informationssicherheit auch im laufenden Betrieb gewährleistet werden. Um dies sicherzustellen, müssen Outsourcing-Kunden und Outsourcing-Dienstleister angemessen kooperieren. So hat der Outsourcing-Kunde ein Betriebskonzept zu erstellen, in dem alle relevanten Sicherheitsaspekte berücksichtigt werden. Outsourcing-Dienstleister sollten Outsourcing-Kunden insbesondere hinsichtlich der folgenden Aspekte unterstützen:

- Regelmäßige Aktualisierung der Dokumentationen und Richtlinien.
- Prüfung der geltenden Sicherheitskonzepte (sind diese noch aufeinander abgestimmt und ist das gewünschte Sicherheitsniveau noch gewährleistet?). Insbesondere sollte der Outsourcing-Dienstleister den Outsourcing-Kunden über wichtige Änderungen in seinem Einflussbereich informieren.
- Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister, in dem beschrieben ist, auf welche Weise die Mandantentrennung im Rahmen des Betriebs von IT-Systemen und Anwendungen sichergestellt wird. Der Outsourcing-Dienstleister hat dabei sicherzustellen, dass Störungen bei anderen Kunden nicht die Abläufe und IT-Systeme des Outsourcing-Kunden beeinträchtigen. Zudem ist sicherzustellen, dass Daten des Outsourcing-Kunden unter keinen Umständen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden.
- Durchführung der vereinbarten Audits zum Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen.
- Bereitstellung von notwendigen Informationen und/oder Kontaktmöglichkeiten zu Subunternehmen des Outsourcing-Dienstleisters, um auch hier Auditierungen zu ermöglichen.
- Dokumentation des (Wartungs-)Zustands von IT-Systemen und Anwendungen (Performance, Verfügbarkeit, Qualitätsniveau, Kapazität).
- Zusammenarbeit bezüglich der Datensicherung (siehe CON.3 *Datensicherungskonzept*).
- Des Weiteren sollte der Outsourcing-Dienstleister an regelmäßigen Abstimmungsrunden zu folgenden Punkten teilnehmen:
    - Informationsaustausch (z. B. Personalnachrichten, organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können).
    - Informationen über Sicherheitsrisiken und den Umgang damit.
    - Problemidentifikation und -analyse.
    - Gegenseitiges Feedback und das Aufspüren von Verbesserungspotenzialen (zur Motivation der Mitarbeiter können besonders positive Beispiele einer gelungenen Kooperation dargestellt werden).
    - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) des Outsourcing-Kunden sollten frühzeitig besprochen werden, um deren rechtzeitige Umsetzung zu gewährleisten.
- Planung, Durchführung und Auswertung von Übungen und Tests zu folgenden Themen:

- Reaktion auf Systemausfälle (Teilausfall, Totalausfall).
- Wiedereinspielen von Datensicherungen.
- Beherrschung von Sicherheitsvorfällen.

OPS.3.1.M11 Zutritts-, Zugangs- und Zugriffskontrolle (S)

Bei einem Outsourcing-Dienstleister werden typischerweise mehrere Outsourcing-Kunden gleichzeitig betreut, die eigenes Personal, aber auch Auditoren und andere Prüfer vorbeischicken. Dabei muss sichergestellt sein, dass Kunden nicht auf IT-Systeme, Netze oder Daten anderer Kunden Zugriff erhalten.

Um die Geschäftsprozesse, Informationen und IT-Systeme des Outsourcing-Dienstleisters ebenso wie die verschiedenen Outsourcing-Kunden angemessen zu schützen, sind Zutritts-, Zugangs- und Zugriffsberechtigungen zu regeln und ein geeigneter organisatorischer Rahmen zu schaffen (siehe auch ORP.4 *Identitäts- und Berechtigungsmanagement*).

Auf den verschiedenen Ebenen müssen angemessene und praktikable Berechtigungen vergeben werden (z. B. für den Zutritt zu Räumen, Zugang zu IT-Systemen, Zugriff auf Anwendungen). Es sollten immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Es muss ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.

Wenn Personen Aufgaben neu übernehmen oder abgeben, müssen Berechtigungen zeitnah angelegt, geändert oder gelöscht sowie ihre Benutzerkennungen aktiviert bzw. deaktiviert werden. Der Zutritt zu Räumen, der Zugriff auf Informationen und der Zugang zu IT-Systemen sollte so abgesichert sein, dass Personen nur auf die Informationen zugreifen können, die sie benötigen. Grundsätzlich sollte der Zugriff auf alle IT-Systeme und Dienste durch Identifikation und Authentisierung der zugreifenden Benutzer oder IT-Systeme abgesichert sein.

Es sollte Vorgaben an Art und Ausgestaltung der jeweiligen Authentisierung geben, z. B. zur Art der Authentisierung über Besitz, Wissen oder biometrische Eigenschaften sowie Mindestanforderungen an Passwörter. Voreingestellte Standardpasswörter müssen direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme von Hard- oder Software geändert werden. Die Mitarbeiter müssen für die korrekte Nutzung von Authentisierungsmechanismen geschult werden.

Die Vergabe von Berechtigungen sollte sich an den Funktionen der Berechtigten orientieren. Rollen und somit auch Berechtigungen sollten geeignet getrennt werden. Vergabe, Änderung sowie Entzug von Berechtigungen und Authentisierungsmitteln müssen dokumentiert werden.

OPS.3.1.M12 Änderungsmanagement (S)

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden IT Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle. In Bezug auf Informationssicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Bei Ausfällen oder Minderleistungen durch den Outsourcing-Dienstleister können empfindliche Vertragsstrafen fällig werden. Zudem leidet der Wertschöpfungsprozess des Outsourcing-Kunden und somit auch die Beziehung zwischen den Outsourcing-Partnern, was einen nachhaltigen Reputationsverlust für den Outsourcing-Dienstleister bedeuten könnte.

Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, so sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen führen.

Daher sollten Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten vorhanden sein (siehe Baustein OPS.1.1.3 *Patch- und Änderungsmanagement*). Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten nach einem standardisierten Prozess ablaufen. Dieser Prozess muss sicherstellen, dass Änderungen

- geplant,

- priorisiert,
- bewertet,
- implementiert,
- geprüft/getestet,
- freigegeben,
- dokumentiert,

und nach ihrer Umsetzung einem Review unterzogen werden. Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Hardware, Erweiterung oder Modifikation des Netzes, neue Applikationen und Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, usw.),
- Räumliche Änderungen, z. B. nach einem Umzug,
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme Benutzergruppen),
- Änderung des Benutzerverhaltens (Nachfrage zu bestimmten Zeiten oder Terminen, nachgefragte Mengen oder Kapazitäten, usw.)

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfungen und Tests der geplanten Aktionen sichergestellt werden, dass das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht ausgeschlossen werden können, muss die Planung auch eine Rückfalllösung vorsehen und Kriterien vorgeben, wann diese zum Tragen kommen soll. Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Dies gilt sowohl in der Betriebs- als auch in einer Testumgebung. Beim Änderungsmanagement ist das Berechtigungskonzept zur Durchführung von Änderungen ein wichtiger Punkt:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.
- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

Hinweis: Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen Änderungen in der Umsetzung einzelner Sicherheitsmaßnahmen, die Erstellung eines neuen Sicherheitskonzepts oder sogar die Überarbeitung der organisationsweiten Leitlinie zur Informationssicherheit erforderlich machen können. Bei größeren Änderungen sollte daher das Informationssicherheitsmanagement des Outsourcing-Dienstleisters und des Outsourcing-Kunden involviert werden.

OPS.3.1.M13 Sichere Migration bei Outsourcing-Vorhaben (S)

Die Migrationsphase beginnt nach dem Vertragsabschluss. Im Zuge der Migration werden folgende vertragliche Regelungen umgesetzt:

- Vereinbarungen hinsichtlich Services und Lösungen gemäß der vertraglichen Regelungen und den allgemeinen Geschäftsbedingungen,
- Service-Vereinbarungen, Anforderungsspezifikationen, Servicekatalog und Beschreibungen, Service-Level,
- detailliertes Outsourcing-Modell und aktualisierter Business Case,
- Migrationsplan.

Nach Beauftragung durch den Outsourcing-Kunden sollte ein Sicherheitsmanagement-Team speziell für die Migrationsphase von Seiten des Outsourcing-Kunden eingerichtet werden. Dieses sollte durch qualifizierte Mitarbeiter des Outsourcing-Dienstleisters ergänzt werden. Die Größe des (gemeinsamen) Sicherheitsmanagement-Teams sollte von Art und Größe des Outsourcing-Vorhabens abhängig gemacht werden, als Minimum kann es aus je einem Sicherheitsexperten des Kunden und des Dienstleisters bestehen.

Um den Erfolg der Migrationsphase zu fördern, sollte der Outsourcing-Kunde, insbesondere dessen Sicherheitsmanagement-Team, während der gesamten Migrationsphase durch den Outsourcing-Dienstleister aktiv in das Projektgeschehen mit einbezogen werden. Demnach sollte insbesondere sichergestellt werden, dass dieser rechtzeitig über aktuelle Fortschritte, Entwicklungen und eventuelle Komplikationen informiert wird.

Hierzu sollte ein Komitee mit fachlich qualifizierten Ansprechpartnern beider Seiten für das Migrationsmanagement etabliert sowie die Häufigkeit von Arbeitstreffen festgelegt werden. Die jeweiligen Verantwortlichkeiten sind im Vorfeld zu definieren und schriftlich zu fixieren sowie mögliche Stellen, die das Komitee unterstützen.

Unter "fachlich qualifizierten Ansprechpartnern" werden in diesem Kontext jene Personen verstanden, die über das erforderliche Fachwissen und die benötigten Kompetenzen für die Outsourcing-Dienstleistung verfügen und für die speziellen Aufgaben und Herausforderungen im Rahmen eines Projekts zum Outsourcing geschult sind (Organisation, Kommunikation, Konfliktmanagement).

Alle Mitglieder des Komitees sollten im kommunikativen Umgang mit Mitarbeitern und weiteren Outsourcing-Partnern erfahren sein. Die zum Teil beträchtlichen organisationsinternen Änderungen, an die sich alle beteiligten Mitarbeiter des Outsourcing-Kunden gewöhnen müssen, können zu Widerständen führen, die sich nicht nur nachteilig auf die unmittelbare Zusammenarbeit auswirken, sondern auch den Erfolg des Outsourcing-Vorhabens beeinflussen. Um das Outsourcing-Vorhaben nicht zu gefährden und Widerständen vorzubeugen und/oder sie abzubauen, ist eine sensible Kommunikation aller Maßnahmen notwendig.

Der Outsourcing-Kunde hat das berechtigte Interesse, während der Migrationsphase deren Durchführung zu überwachen. Hierzu sollten die notwendigen Strukturen und Ressourcen geschaffen und bereitgestellt werden, wie z. B. definierte Kommunikationskanäle und –Verfahren sowie Eskalationsvorlagen und eine regelmäßige Berichterstattung. So kann die Migration transparent durchgeführt werden, was die Erreichung von Zielen durch beide Seiten messbar macht und zu einer nachhaltigen vertrauensvollen Outsourcing-Beziehung führt.

Außerdem sollte in dieser Phase gegebenenfalls eine Schulung der Mitarbeiter des Outsourcing-Kunden geplant werden. Diese arbeiten künftig an neu entstandenen Schnittstellen. Der Outsourcing-Dienstleister sollte hierbei unterstützen. Die Durchführung von Schulungen und deren Nachhaltigkeit liegen im Interesse des Outsourcing-Dienstleisters, da dieser aufgrund ungenügender Zuarbeit seinen Service meist nicht in dem vereinbarten Umfang bzw. mit dem geforderten Qualitätsniveau erbringen kann. Dies wiederum kann sich negativ auf die Outsourcing-Beziehung und somit auf die Reputation des Outsourcing-Dienstleisters auswirken.

Im Zuge der Migration kommt dem Testbetrieb eine hohe Bedeutung zu. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die oftmals unsicher sind. Dies gilt es zu vermeiden. So ist beispielsweise sicherzustellen, dass Produktivdaten nicht ohne besonderen Schutz als Testdaten verwendet werden dürfen. Dies muss durch das Sicherheitskonzept entsprechend ausgeschlossen werden.

Folgende Aspekte sollten von Seiten des Outsourcing-Dienstleisters im Zuge der Migrationsphase berücksichtigt werden:

- Für die Migrationsphase muss eine Sicherheitskonzept erstellt werden.
- Der Outsourcing-Dienstleister hat klare Verantwortlichkeiten und Hierarchien für die Migrationsphase festzulegen. Klare Führungsstrukturen sind eine Voraussetzung. Zudem sollten Ansprechpartner und Verantwortlichkeiten auch auf hohen Ebenen definiert werden.

Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.

- Die erforderlichen Tests müssen geplant und durchgeführt, Abnahmeprozeduren erarbeitet und die Produktionseinführung geplant werden.
- Der Outsourcing-Dienstleister muss geeignete interne Mitarbeiter für die Test-, Einführungsphase und den späteren Betrieb auszuwählen. Es ist zu prüfen, inwieweit dem Outsourcing-Kunden vertraglich ein Mitspracherecht bei der Personalauswahl eingeräumt werden sollte.
- Der Outsourcing-Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Outsourcing-Kunden genau kennenlernen und gegebenenfalls aktiv eine Einweisung fordern.
- Der störungsfreie Betrieb ist durch eine genaue Ressourcenplanung und Tests im Vorfeld sicherzustellen. Die produktiven IT-Systeme dürfen dabei nicht vernachlässigt werden. Zudem müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Outsourcing-Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Dokumentation neuer IT-Systeme oder Teilsysteme muss dabei ebenfalls sichergestellt sein.
- Während der Migration muss ständig überprüft werden, ob die SLAs oder die vorgesehenen Sicherheitsmaßnahmen angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen, eingestellt hat, sollten verstärkt Mitarbeiter zu Bereitschaftsdiensten verpflichtet werden.

Nach Abschluss der Migration muss sichergestellt werden, dass das Sicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- Interne und externe Ansprechpartner und Zuständigkeiten sollten mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert werden.
- Die Systemkonfigurationen sind zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.
- Alle Ausnahmeregelungen müssen am Ende der Migrationsphase aufgehoben werden.

Als letzte Aufgabe muss die Outsourcing-Dienstleistung nach der Migrationsphase in den sicheren Regelbetrieb (siehe OPS.3.1.M10 *Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb*) überführt werden.

OPS.3.1.M14 Notfallvorsorge beim Outsourcing (S)

Für ausgelagerte Aufgaben und Prozesse des Outsourcing-Kunden gelten die gleichen Anforderungen an die Notfallvorsorge wie im Falle einer Eigenerbringung. Das bedeutet, dass der Outsourcing-Dienstleister seine Maßnahmen zur Notfallvorsorge im Rahmen der entsprechenden Auslagerung an die Anforderungen des Outsourcing-Kunden anpassen muss, insbesondere mit Blick auf Wiederanlauf- und Wiederherstellungszeiten.

Eine wirksame gemeinsame Notfallvorsorge stärkt nachhaltig das Vertrauen in der Outsourcing-Beziehung und kann die eigene Notfallvorsorge des Outsourcing-Dienstleisters verbessern. Es können

Synergien entstehen, da der Outsourcing-Kunde möglicherweise Notfallarbeitsplätze für Mitarbeiter des Outsourcing-Dienstleisters im eigenen Haus zur Verfügung stellt.

Grundsätzlich sollten die Notfallkonzepte beider Parteien aufeinander abgestimmt sein. Da dieser Zustand nicht statisch ist, sollte diese Abstimmung regelmäßig und anlassbezogen wiederholt werden. Schnittstellen (z. B. Netzverbindung, Router, Telekommunikationsprovider) zwischen den Vertragsparteien und Dritten müssen identifiziert und im Rahmen der Notfallvorsorge berücksichtigt werden. In OPS.3.1.M2 Vertragsgestaltung mit den Outsourcing-Kunden wird beschrieben, welche Aspekte bereits im Service Level Agreement geregelt werden sollten.

Im Notfallvorsorgekonzept müssen folgende Aspekte genau spezifiziert und im Detail beschrieben werden:

- Zuständigkeiten, Ansprechpartner und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung (siehe Baustein CON.3 *Datensicherungskonzept*) sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Es sind detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen zu erstellen.
- Es muss ein Konzept für regelmäßig durchzuführende Notfallübungen erarbeitet und mit dem Outsourcing-Kunden abgestimmt werden.

Tritt ein Notfall im Haus des Outsourcing-Kunden ein, ist die Qualität der Arbeitsanweisungen für den Notfall von entscheidender Bedeutung für die Wirksamkeit der Notfallmaßnahmen. Der Outsourcing-Kunde sollte aus diesem Grund daran interessiert sein, die zu ergreifenden Notfallmaßnahmen mit dem Outsourcing-Dienstleister abzustimmen. Es ist jedoch auch im Interesse des Outsourcing-Dienstleisters, eine kompetente und schnelle Reaktion auf Notfälle des Outsourcing-Kunden zu garantieren, da der Fortbestand des Kunden und die eigene Reputation gefährdet sein können.

Dem Outsourcing-Dienstleister muss bewusst sein, dass der Outsourcing-Kunde im Zuge einer Auslagerung gegebenenfalls wesentliches Know-how für den ausgelagerten Bereich verliert und eine adäquate Notfallreaktion dadurch oft nur mit der Unterstützung des Outsourcing-Dienstleisters möglich ist.

Möglich ist zudem, dass IT-Systeme des Outsourcing-Kunden von Mitarbeitern des Outsourcing-Dienstleisters betrieben werden, ohne dass diese über Detailkenntnisse bezüglich der Anwendungen besitzen, welche auf den IT-Systemen betrieben werden. Tritt ein Fehler in einer Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung durchführen, ohne umfangreiche Kenntnisse über das Gesamtsystem zu besitzen. Der Outsourcing-Dienstleister sollte daher dafür sorgen, dass das Notfallvorsorgekonzept genaue Anweisungen enthält, wie er im Rahmen der Notfallbewältigung vorzugehen hat. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot einer Maschine).

Ein Fehlverhalten einer Anwendung kann technische (z. B. voller Datenträger, Netzprobleme) oder anwendungsspezifische Ursachen haben (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung). Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können, eine Kooperation mit dem Outsourcing-Kunden ist meist aber dennoch notwendig, um unerwünschte Nebeneffekte auf Applikationsebene zu verhindern. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, über welche nur einer der Vertragspartner verfügt. Darum müssen kooperative Vorgehensweisen, Kommunikations- und Eskalationspläne im Vorhinein geplant werden.

Des Weiteren sollten der Outsourcing-Dienstleister und der Outsourcing-Kunde regelmäßig gemeinsame Übungen durchführen, die die Wirksamkeit der Notfallvorsorge der übertragenen Aufgaben und Prozesse prüft bzw. nachweist. Der Outsourcing-Dienstleister sollte die in diesem

Zusammenhang benötigten Ressourcen zur Planung, Durchführung und Nachbereitung der Übungen bei seiner Kalkulation berücksichtigen.

OPS.3.1.M15 Geordnete Beendigung eines Outsourcing-Verhältnisses (S)

Die Empfehlungen dieser Maßnahme lassen sich in der Regel nur umsetzen, wenn bereits im Vertrag mit dem Outsourcing-Kunden alle relevanten Themen zum Vertragsende geregelt wurden (siehe OPS.3.1.M2 *Vertragsgestaltung mit den Outsourcing-Kunden*). So ist die ordnungsgemäße Rückintegration der ausgelagerten Prozesse bzw. die Übertragung dieser auf einen anderen Outsourcing-Dienstleister nur möglich, wenn ausreichend Zeit innerhalb der festgelegten Kündigungsfristen bleibt.

Zudem müssen ausreichend Vorkehrungen getroffen werden, dass durch das Vertragsende des Outsourcing-Vertrags die Geschäftstätigkeit des Outsourcing-Kunden nicht beeinträchtigt wird.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Outsourcing-Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software ist für den Fall der Beendigung des Vertragsverhältnisses zu regeln.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe sollten ausreichend dokumentiert sein, um dem Outsourcing-Kunden die Reintegration der ausgelagerten Prozesse und Aktivitäten zu erleichtern.
- Alle notwendigen Informationen und Daten müssen vom Outsourcing-Dienstleister an den Outsourcing-Kunden übertragen bzw. übergeben werden.
- Alle Datenbestände des Outsourcing-Kunden beim Outsourcing-Dienstleisters müssen sicher gelöscht werden.
- Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, sind zu überprüfen. Der Outsourcing-Dienstleister sollte alle Berechtigungen löschen, die für den Outsourcing-Kunden oder Dritte eingerichtet wurden.

OPS.3.1.M16 Sicherheitsüberprüfung von Mitarbeitern (H)

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder fremdem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen bei der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Der Outsourcing-Dienstleister sollte sich daher im Vorfeld der Leistungserbringung mit den Outsourcing-Kunden in Hinsicht auf die Anforderungen an das einzusetzende Personal abstimmen. Diese Anforderungen sollten bei jedem Personalwechsel oder -neuzugang berücksichtigt werden.

Bei der Vertragsgestaltung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden sollte festgehalten werden, welche Seite im Bedarfsfall welche Überprüfungen durchzuführen hat und in welcher Tiefe diese zu erfolgen haben.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

Für den Umsetzungshinweis OPS.3.1 *Outsourcing für Dienstleister* sind keine Quellenverweise vorhanden.