Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.3.2 Anbieten von Outsourcing

## 1. Beschreibung

### 1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietende von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen "IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff "Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Anbietenden von Outsourcing sicherzustellen. Der Baustein soll dazu beitragen, dass die Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing eine grundlegende Informationssicherheit gewährleistet. Mit Outsourcing ist dabei das klassische "IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen aus der Dienstleistung der Anbietenden von Outsourcing nicht die Nutzenden von Outsourcing gefährden. Dementsprechend sind diese Risiken zu mindern und vorzubeugen.

## 1.3. Abgrenzung und Modellierung

Der Baustein OPS.3.2 *Anbieten von Outsourcing* ist aus Sicht der Anbietenden auf jede oder jeden Nutzenden, der Dienstleistungen vom Anbietenden bezieht, einmal anzuwenden.

Dabei bezieht sich der Baustein auf die Perspektive der Anbietenden von Outsourcing im Outsourcing-Verhältnis. Die Anforderungen des Bausteins stellen sicher, dass fundamentale Sicherheitsstandards gegenüber den Nutzenden von Outsourcing eingehalten werden und dazu beitragen, dass die Anforderungen der Nutzenden von Outsourcing an die Informationssicherheit über den gesamten Outsourcing-Prozess eingehalten werden können.

Der Fall einer Weiterverlagerung wird in dem Baustein OPS.3.2 *Anbieten von Outsourcing* nur bedingt betrachtet, da dies ein weiteres Outsourcing-Verhältnis darstellt und somit die Anbietenden von Outsourcing den Baustein OPS.2.3 *Nutzung von Outsourcing* für diese Sub-Dienstleistenden modellieren müssen.

Vom klassischen „IT-Outsourcing“ (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.3.2 *Anbieten von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

# 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.3.2 *Anbieten von Outsourcing* von besonderer Bedeutung.

## 2.1. Unzureichendes Informationssicherheitsmanagement bei Anbietenden von Outsourcing

Ein mangelhaftes Informationssicherheitsmanagement kann dazu führen, dass die Schutzziele der Informationssicherheit durch die Anbietenden von Outsourcing nur unzureichend eingehalten werden. Durch einen Outsourcing-Vertrag sind die Anbietenden von Outsourcing dafür zuständig, das erforderliche Niveau an Informationssicherheit für den Outsourcing-Prozess einzuhalten. Sollten die Anbietenden von Outsourcing ihrer Zuständigkeit nicht nachkommen, so kann dies zu einer Gefahr für alle am Outsourcing-Prozess beteiligten Institutionen führen.

## 2.2. Unzureichendes Notfallmanagement der Anbietenden von Outsourcing

Wenn Störungen oder Notfälle bei Anbietenden von Outsourcing eintreten, kann dies zu einer Betriebsstörung führen, die auch die ausgelagerten Prozesse der Nutzenden von Outsourcing betreffen können und sich auf deren ordentlichen Geschäftsbetrieb auswirken. Insbesondere die Notfallvorsorge ist im Vorfeld von Not- und Krisensituation von entscheidender Bedeutung. Im Falle einer mangelhaften Notfallvorsorge kann für die Institution keine effektive Notfallbewältigung sichergestellt werden. Somit sind für die einzelnen Institutionen Störungen, Not- und Krisensituationen unter Umständen unkontrollierbar. Es kommt zu einem Kaskadeneffekt, der neben den Anbietenden von Outsourcing auch alle vor- und nachgelagerten Dienstleistenden sowie Kunden beeinträchtigt.

## 2.3. Unzulängliche vertragliche Regelungen mit Nutzenden von Outsourcing

Unzulänglichkeiten in der Vertragsgestaltung können dazu führen, dass die Informationssicherheit von ausgelagerten Prozessen der Nutzenden von Outsourcing unzureichend abgesichert ist. Vertragliche Regelungen definieren den gesamten Outsourcing-Prozess und stellen die rechtliche Grundlage für Ansprüche der Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing dar. Somit übertragen sich die Unzulänglichkeiten aus der Vertragsgestaltung auf den gesamten Outsourcing-Lebenszyklus. Dies ist verbunden mit einer Vielzahl an möglichen Gefährdungsszenarien mit finanziellen und gesellschaftlichen Auswirkungen für die Nutzenden sowie Anbietenden von Outsourcing.

## 2.4. Schwachstellen bei der Anbindung Nutzender von Outsourcing

Die technische Anbindung der Nutzenden von Outsourcing an die Netze der Anbietenden von Outsourcing kann an den Schnittstellen zu technischen sowie organisatorischen Schwachstellen führen. Die technischen Schwachstellen in der Anbindung können zu Störungen, Datenverlust sowie zum Ausgangspunkt von IT-gestützte Angriffe führen. Dagegen können organisatorische Schwachstellen in Form von unbesetzten Schnittstellen zu Kommunikationsproblemen zwischen den Anbietenden und Nutzenden von Outsourcing führen. Diese können eine Gefahr für die Effizienz von Risikobewältigungsmaßnahmen in Not- und Krisensituationen darstellen.

## 2.5. Abhängigkeit von Sub-Dienstleistenden

Werden Tätigkeiten von Anbietenden von Outsourcing an Sub-Dienstleistende weiter verlagert, besteht das Risiko, dass die Sub-Dienstleistenden ihre Positionen ausnutzen, um Forderungen durchzusetzen sowie Vorgaben der Vereinbarung zu missachten. Es entsteht eine Abhängigkeit von Dritten, um die Kundenleistung zu erbringen. Sollten die Anbietenden von Outsourcing nicht in der Lage sein, eine Störung oder Ausfall der Sub-Dienstleistenden zu kompensieren, besteht eine zwingende Abhängigkeit. Dies bringt die Sub-Dienstleistenden gegenüber den Anbietenden von Outsourcing in eine vorteilhafte Position. Die Sub-Dienstleistenden können davon absehen, die vertraglich geregelte Qualität sowie das festgelegte Niveau der Informationssicherheit einzuhalten. Dies beeinträchtigt das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing und bedeutet für die Anbietenden von Outsourcing rechtliche und finanzielle Auswirkungen sowie einen Reputationsverlust.

## 2.6. Ungeeignete Konfiguration und Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Eine entweder ungeeignete oder unzureichende Konfiguration eines zentralen Verzeichnisdienstes kann dazu führen, dass Nutzende Rechte erhalten, die sie potenziell dazu befähigen auf sensible oder personenbezogene Daten der Anbietenden von Outsourcing oder anderer Kunden des Anbietenden von Outsourcing zuzugreifen. Unter Umständen erfordern Outsourcing-Vorhaben, dass Nutzende von Outsourcing auf den Informationsverbund der Anbietenden von Outsourcing zugreifen müssen. Dies ist mit entsprechenden Rechten für Zutritt-, Zugang- und Zugriff verbunden, die ein Risiko für die IT-Systeme, Informationen sowie Gebäude darstellen. Eine Folge ist, dass die Integrität und Vertraulichkeit dieser Daten gefährdet sind. Letztlich kann dies dazu führen, dass Vertragsstrafen von den Nutzenden von Outsourcing gegenüber den Anbietenden von Outsourcing geltend gemacht werden sowie ein Reputationsverlust für die Anbietenden von Outsourcing sowie ihre Kunden eintreten kann.

## 2.7. Unzureichende Mandantenfähigkeit bei Anbietenden von Outsourcing

Anbietende von Outsourcing haben in der Regel unterschiedliche Kunden, die auf die gleichen Ressourcen wie IT-Systeme, Netze oder Personal zurückgreifen. Sind IT-Systeme und Daten der Nutzenden von Outsourcing unzureichend voneinander getrennt und abgesichert, besteht die Gefahr, dass Nutzende auf die Bereiche anderer Nutzender zugreifen und unberechtigt auf Daten zugreifen können. Dies stellt einen unmittelbaren Verstoß gegen die Vertraulichkeit der jeweiligen Daten der Nutzenden dar. Insbesondere ist dies problematisch bei Nutzenden von Outsourcing, die im Wettbewerb miteinander stehen. Die Auswirkungen wären Reputationsverlust für die Anbietenden von Outsourcing sowie rechtliche Folgen durch die geschädigten Nutzenden von Outsourcing.

## 2.8. Kontroll- und Steuerungsverlust bei der Weiterverlagerung an Sub-Dienstleistende

Ausgelagerte Prozesse werden von Anbietenden von Outsourcing unter Umständen im Rahmen einer Weiterverlagerung vollständig oder partiell an Sub-Dienstleistende weitergegeben. Eine unzureichende Kontrolle der Sub-Dienstleistenden führt dazu, dass vereinbarte Aspekte der Informationssicherheit von Sub-Dienstleistenden unzureichend eingehalten werden. Dies hat im weiteren Verlauf Konsequenzen für das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing sowie unmittelbare finanzielle Auswirkungen und Reputationsverluste für die Anbietenden von Outsourcing zur Folge.

## 2.9. Unzulängliche Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses

Unzulängliche Regelungen für das Ende eines Outsourcing-Verhältnisses können dazu führen, dass Hardware sowie Daten abschließend nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben oder übermittelt werden. Hinzu kommt, dass vorhandene Kundendaten nicht nach Speicherfrist der einschlägigen Gesetze und Vorschriften ordnungsgemäß gelöscht werden. Ein Outsourcing-Verhältnis kann durch eine ordentliche Kündigung sowie durch außerordentliche Gründe beendet werden. Exemplarisch hierfür ist eine Insolvenz von Anbietenden von Outsourcing. Die Anbietenden von Outsourcing schützen unter Umständen nach der Vertragsauflösung die vorhandenen Daten der Nutzenden von Outsourcing nicht angemessen gemäß des Schutzbedarfs des jeweiligen Eigentümers. Die Daten können in die Hand Dritter gelangen und bei Veröffentlichung zu Reputationsverlust führen.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| **Zuständigkeiten** | **Rollen** |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Institution, Datenschutzbeauftragte, Notfallbeauftragte |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig

zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

## 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

### OPS.3.2.A1 Einhaltung der Schutzziele der Informationssicherheit durch ein Informationssicherheitsmanagement (B)

Der Schutzbedarf für Vertraulichkeit, Integrität und Verfügbarkeit von Nutzenden von Outsourcing MUSS im Outsourcing-Prozess berücksichtigen werden. Dabei MUSS sichergestellt werden, dass das von den Nutzenden von Outsourcing geforderte Minimum an Informationssicherheit eingehalten wird. Zudem MÜSSEN die geltenden regulatorischen und gesetzlichen Aspekte berücksichtigt werden.

### OPS.3.2.A2 Grundanforderungen an Verträge mit Nutzenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese SOLLTEN einheitlich in Verträgen umgesetzt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit und Sicherheitsanforderungen der Nutzenden von Outsourcing beinhalten. Zudem MÜSSEN sie beinhalten, wie mit Weiterverlagerungen durch die Anbietenden umgegangen wird. Die Grundanforderungen MÜSSEN beinhalten, dass die Nutzenden das Recht haben Prüfungen, Revisionen und Auditierungen durchzuführen, um sicherzustellen, dass die vertraglich geregelten Anforderungen an die Informationssicherheit eingehalten werden. Mit den Nutzenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten, Vereinbarungen zum Informationsaustausch und Service-Level-Agreements vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

### OPS.3.2.A3 Weitergabe der vertraglich geregelten Bestimmungen mit Nutzenden von Outsourcing an Sub-Dienstleistende (B)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, MÜSSEN die vertraglichen Bestimmungen mit den Nutzenden von Outsourcing an die Sub-Dienstleistenden weitergegeben werden. Dies MUSS in den Verträgen mit den Sub-Dienstleistenden entsprechend festlegt und durchgesetzt werden. Auf Nachfrage von Nutzenden von Outsourcing MÜSSEN diese Verträge vorgelegt werden.

### OPS.3.2.A4 Erstellung eines Mandantentrennungskonzepts (B)

Es MUSS ein Mandantentrennungskonzept erstellt und umgesetzt werden. Das Mandantentrennungskonzept MUSS sicherstellen, dass Daten und Verarbeitungskontexte verschiedener Nutzender von Outsourcing ausreichend sicher getrennt werden. Dabei MUSS zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden. Es MUSS dargelegt werden, mit welchen Mechanismen die Anbietenden von Outsourcing die Mandanten trennen. Die benötigten Mechanismen zur Mandantentrennung MÜSSEN durch die Anbietenden von Outsourcing ausreichend umgesetzt werden. Das Mandantentrennungskonzept MUSS durch die Anbietenden von Outsourcing erstellt und den Nutzenden von Outsourcing zur Verfügung gestellt werden. Darüber hinaus MUSS es für den Schutzbedarf der Daten der Nutzenden von Outsourcing eine angemessene Sicherheit bieten.

### OPS.3.2.A5 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung (B)

Die Anbietenden von Outsourcing MÜSSEN für ihre Dienstleistungen ein Sicherheitskonzept erstellen. Für individuelle Outsourcing-Vorhaben MÜSSEN zusätzlich spezifische Sicherheitskonzepte erstellt werden, die auf den Sicherheitsanforderungen der Nutzenden von Outsourcing basieren. Das Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben SOLLTE jedem und jeder Nutzenden von Outsourcing vorgelegt werden. Das Sicherheitskonzept der Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Anbietende und Nutzende von Outsourcing MÜSSEN gemeinsam Sicherheitsziele erarbeiten und diese dokumentieren. Es MUSS außerdem eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erstellt werden. Darüber hinaus MÜSSEN die Anbietenden von Outsourcing regelmäßig überprüfen, ob das Sicherheitskonzept umgesetzt wurde.

### OPS.3.2.A6 Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses (B)

Es MÜSSEN Regelungen getroffen werden, wie verfahren wird, wenn Outsourcing-Verhältnisse geplant oder ungeplant beendet werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden von den Anbietenden von Outsourcing zurückgegeben werden. Anschließend MÜSSEN die verbleibenden Datenbestände der Nutzenden von Outsourcing nach Ablauf der gesetzlichen Vorgaben zur Datenaufbewahrung sicher gelöscht werden. Dies MUSS durch die Anbietenden von Outsourcing dokumentiert werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Nutzenden von Outsourcing aufgehoben wurden, nachdem das Outsourcing-Verhältnis beendet wurde.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

### OPS.3.2.A7 Bereitstellung der ausgelagerten Dienstleistung durch multiple Sub-Dienstleistende (S)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, SOLLTEN die Anbietenden von Outsourcing mehrere qualifizierte Sub-Dienstleistende zur Verfügung haben, falls Sub-Dienstleistende ausfallen oder kündigen. Dies SOLLTE gemeinsam mit den Nutzenden von Outsourcing dokumentiert werden.

### OPS.3.2.A8 Erstellung einer Richtlinie für die Outsourcing-Dienstleistungen (S)

Es SOLLTE eine Richtlinie für das Anbieten von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE das Test- und Freigabeverfahren regeln. Dabei SOLLTE die Weiterverlagerung an Sub-Dienstleistende berücksichtigt werden. Die Richtlinie SOLLTE Maßnahmen berücksichtigen, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

### OPS.3.2.A9 Überprüfung der Vereinbarung mit Nutzenden von Outsourcing (S)

Vereinbarungen mit Nutzenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Nutzenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Bei veränderter Gefährdungs- oder Gesetzeslage SOLLTEN die festgelegten Sicherheitsanforderungen nachgebessert werden. Alle Änderungen SOLLTEN durch die Anbietenden von Outsourcing dokumentiert werden.

## OPS.3.2.A10 Etablierung eines sicheren Kommunikationskanals und Festlegung der Kommunikationspartner (S)

Die Anbietenden von Outsourcing SOLLTEN einen sicheren Kommunikationskanal zu den Nutzenden von Outsourcing einrichten. Es SOLLTE dokumentiert sein, welche Informationen über diesen Kommunikationskanal an den Outsourcing-Partner übermittelt werden. Dabei SOLLTE sichergestellt werden, dass an den jeweiligen Enden des Kommunikationskanals entsprechend Zuständige benannt sind. Dabei SOLLTE regelmäßig und anlassbezogen überprüft werden, ob diese Personen noch in ihrer Funktion als dedizierte Kommunikationspartner beschäftigt sind. Zwischen den Outsourcing-Partnern SOLLTE geregelt sein, nach welchen Kriterien welcher Kommunikationspartner welche Informationen erhalten darf.

## OPS.3.2.A11 Etablierung eines Notfallkonzepts (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. In diesem Notfallkonzept SOLLTEN Nutzende von Outsourcing sowie Sub-Dienstleistende berücksichtigt werden.

## OPS.3.2.A12 Durchführung einer risikoorientierten Betrachtung von Prozessen, Anwendungen und IT-Systemen (S)

Werden Prozesse, Anwendungen oder IT-Systeme neu aufgebaut und Kunden bereitgestellt, SOLLTEN diese regelmäßig und anlassbezogen risikoorientiert betrachtet und dokumentiert werden. Aus den sich daraus ergebenen Ergebnissen SOLLTEN geeignete Maßnahmen festgelegt werden. Darüber hinaus SOLLTEN die Resultate dazu verwendet werden, um das Informationssicherheitsmanagement weiter zu verbessern.

## OPS.3.2.A13 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Anbietenden an das Datennetz der Nutzenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Bevor beide Netze verbunden werden, SOLLTEN sie auf bekannte Sicherheitslücken analysiert werden. Es SOLLTE geprüft werden, ob die Vereinbarungen für die Netzanbindung eingehalten werden und das geforderte Sicherheitsniveau nachweislich erreicht wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

## OPS.3.2.A14 Überwachung der Prozesse, Anwendungen und IT-Systeme (S)

Die für Kunden eingesetzten Prozesse, Anwendungen und IT-Systeme SOLLTEN kontinuierlich überwacht werden.

## OPS.3.2.A15 Berichterstattung gegenüber den Nutzenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN den Nutzenden von Outsourcing in festgelegten Abständen Berichte über den ausgelagerten Prozess bereitstellen. Es SOLLTE ein Bericht an die Nutzenden von Outsourcing versendet werden, wenn Änderungen am Prozess durch die Anbietenden von Outsourcing oder Sub-Dienstleistenden stattfanden. Dazu SOLLTEN standardisierte Protokolle zur Berichterstattung etabliert werden.

## OPS.3.2.A16 Transparenz über die Outsourcing-Kette der ausgelagerten Kundenprozesse (S)

Die Anbietenden von Outsourcing SOLLTEN ein Auslagerungsregister für die in Kundenprozessen eingesetzten Sub-Dienstleistenden führen. Dieses SOLLTE Informationen zu den Sub-Dienstleistenden, Leistungskennzahlen, Kritikalität der Prozesse, abgeschlossenen Verträgen und Vereinbarung sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN nachgehalten werden. Das Auslagerungsregister SOLLTE auch die Weiterverlagerungen durch die Sub-Dienstleistenden behandeln. Die Anbietenden von Outsourcing SOLLTEN das Auslagerungsregister regelmäßig und anlassbezogen überprüfen.

### OPS.3.2.A17 Zutritts-, Zugangs- und Zugriffskontrolle (S)

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN sowohl für das Personal der Anbietenden von Outsourcing als auch für das Personal der Nutzenden von Outsourcing geregelt sein. Ebenfalls SOLLTEN Zutritts-, Zugangs- und Zugriffsberechtigungen für Auditoren und andere Prüfer festgelegt werden. Dabei SOLLTEN nur so viele Rechte vergeben werden, wie für die Tätigkeit notwendig ist.

### OPS.3.2.A18 Regelungen für den Einsatz von Sub-Dienstleistenden (S)

Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit der Anbietenden von Outsourcing unterrichtet werden. Soweit es gefordert ist, SOLLTEN das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden nach Vorgaben der Nutzenden von Outsourcing überprüft werden, z. B. durch ein Führungszeugnis. Das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN schriftlich dazu verpflichtet werden, einschlägige Gesetze und Vorschriften, Vertraulichkeitsvereinbarungen sowie interne Regelungen einzuhalten. Es SOLLTEN Vertretungsregelungen in allen Bereichen existieren.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

### OPS.3.2.A19 Sicherheitsüberprüfung von Beschäftigten (H)

Die Vertrauenswürdigkeit des Personals der Anbietenden von Outsourcing SOLLTE durch geeignete Nachweise überprüft werden. Es SOLLTEN mit den Nutzenden von Outsourcing vertragliche Kriterien vereinbart werden.

### OPS.3.2.A20 Verschlüsselte Datenübertragung und -speicherung (H)

Für die Übertragung von Daten von und zu den Nutzenden von Outsourcing sowie die Speicherung SOLLTE mit den Nutzenden von Outsourcing eine sicheres Verschlüsselungsverfahren festgelegt werden. Dabei SOLLTE sich die eingesetzte Verschlüsselungsmethode am Schutzbedarf der Daten orientieren. Die Verschlüsselungsmethode SOLLTE regelmäßig und anlassbezogen auf ihre Funktionsfähigkeit hin überprüft werden.

### OPS.3.2.A21 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Nutzenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 „Steuerung der Dienstleistungserbringung von Lieferanten“ Vorgaben für die Steuerung von Dienstleistenden. In der DIN ISO 37500:2015-08 werden im „Leitfaden Outsourcing“ weiterführende Informationen zum Umgang mit Dienstleistenden aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Der „Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen“ des Bundesverbandes Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) führt Informationen zur Thematik „Compliance“ in IT-Outsourcing-Projekten auf und liefert Hilfestellungen zur Umsetzung der rechtlichen Rahmenbedingungen in einem Outsourcing-Verhältnis.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53 Anforderungen an Dienstleistende. In einer weiteren Publikation NISTIR 8276 beschreibt NIST die Best-Practices im Risikomanagement einer „Cyber Supply Chain“.

Der BSI-Standard 200-4 Notfallmanagement enthält wichtige Informationen sowie Vorlagen zur Erstellung und Etablierung eines funktionsfähigen Notfallkonzepts.