Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: OPS.2.1 Outsourcing für Kunden

1. Einleitung

Immer mehr Institutionen entscheiden sich heutzutage, bestimmte Prozesse und Aktivitäten nicht mehr vollständig selbst zu erbringen, sondern diese an einen Dritten – 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 unter anderem erhebliche Kosten gespart, externe Ressourcen flexibel genutzt oder interne Ressourcen entlastet werden, um sich stärker auf die eigenen Kernkompetenzen zu konzentrieren. Diese Chancen gehen jedoch stets mit zum Teil erheblichen Risiken einher (hohe Abhängigkeit von externen Dienstleistern, Verlust von Kontroll- und Steuerungsmöglichkeiten, Risiken für die Informationssicherheit), die das Outsourcing-Vorhaben nicht nur scheitern lassen, sondern im schlechtesten Fall auch die Existenz der auslagernden Institution gefährden können. Ein Beispiel hierfür wäre die unautorisierte Veröffentlichung streng vertraulicher Geschäftsstrategien der auslagernden Institution durch Mitarbeiter des Dienstleisters von Outsourcing-Dienstleistungen. Umso wichtiger ist es, allen mit dem Outsourcing-Vorhaben einhergehenden Risiken ausreichend zu begegnen. Um dieses Ziel zu erreichen, werden nachfolgend Maßnahmen beschrieben, die der Outsourcing-Kunde im Rahmen jeder Phase eines Outsourcing-Vorhabens beachten bzw. umsetzen sollte.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins OPS.2.1 *Outsourcing für Kunden* aufgeführt.

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

2.1. Maßnahmen zum Baustein OPS.2.1 Outsourcing für Kunden

OPS.2.1.M1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben (B)

Im Rahmen eines Outsourcing-Vorhabens müssen Sicherheitsanforderungen festgelegt werden, die im Einklang mit der Outsourcing-Strategie stehen. Diese sollten als Grundlage für die Auswahl eines Outsourcing-Dienstleisters und die anschließende Vertragsgestaltung dienen (OPS.2.1.M3 *Auswahl eines geeigneten Outsourcing-Dienstleisters*, OPS.2.1.M4 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* und OPS.2.1.M11 *Planung und Aufrechterhaltung der Informationssicherheit*). Beide Outsourcing-Parteien müssen sich vertraglich dazu verpflichten, den IT-Grundschutz oder ein vergleichbares Schutzniveau einzuhalten. Um das erforderliche Sicherheitsniveau zu erreichen, sollten von Outsourcing-Kunden und Outsourcing-Dienstleister gemeinsam Sicherheitsziele und darauf aufbauend Sicherheitsanforderungen entwickelt werden, die der Individualität des jeweiligen Outsourcing-Vorhabens Rechnung tragen.

In diese Betrachtungen müssen alle Schnittstellen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister mit den jeweiligen Sicherheitsanforderungen mit einbezogen werden. Hierbei sollten alle Aspekte des Identitäts- und Berechtigungsmanagements berücksichtigt werden. Hierfür können z. B. alle beteiligten Benutzer bestimmten Gruppen (Administrator, Kontrolleur, Mitarbeiter etc.) zugeordnet werden, wobei jede Gruppe bestimmte Rechte erhält, die sie im Rahmen ihrer Tätigkeit zwingend benötigt. Eine weitere Möglichkeit ist die Definition bestimmter Rollen, d. h. die Zusammenfassung bestimmter Rechte. Benutzer, die im Rahmen ihrer Tätigkeit in dem Outsourcing-Vorhaben eine oder mehrere bestimmte Rollen ausfüllen, erhalten dann die erforderlichen Rechten.

In jedem Fall muss bei der Rechtevergabe das *Least-Privilege-Prinzip* beachtet werden. So erhalten alle Benutzer nur die unbedingt notwendigen Rechte. Die Gefahr vorsätzlich oder fahrlässig verursachter Sicherheitsvorfälle kann so reduziert werden (siehe hierzu auch OPS.2.1.M6 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*).

Um Zugriffsrechte adäquat vergeben zu können, ist es notwendig, alle Daten und Informationen zu klassifizieren. Die Klassifizierung muss entsprechend der strategischen Bedeutung vorgenommen werden.

Es ist zu bedenken, dass das Festlegen von Sicherheitsanforderungen ein iterativer Prozess ist:

- Zunächst werden die gewünschten Sicherheitsanforderungen durch den Kunden spezifiziert.
- Danach wird in der Angebotsphase abgeglichen, wie und ob die gewünschten Sicherheitsanforderungen durch die anbietenden Dienstleister geleistet werden können.
- Ist ein Dienstleister ausgewählt, so muss mit diesem die weitere Verfeinerung der Sicherheitsanforderungen (z. B. basierend auf den eingesetzten Betriebssystemen oder Sicherheitsmechanismen) erarbeitet werden. In der Endphase dieses Abstimmungsprozesses müssen dann auch die Sicherheitsanforderungen für die konkrete Umsetzung definiert werden.

Generell ergeben sich für Outsourcing-Szenarien folgende Mindestsicherheitsanforderungen:

- Die Umsetzung des IT-Grundschutzes oder eines vergleichbaren Schutzniveaus ist eine Minimalforderung an beide Outsourcing-Parteien. Zusätzlich müssen sowohl Outsourcing-Dienstleister als auch der Outsourcing-Kunde selbst ein Sicherheitskonzept besitzen und dieses umgesetzt haben.
- Es ist wichtig, die relevanten Informationsverbunde genau abzugrenzen (z. B. nach Fachaufgabe, Geschäftsprozess, IT-Systemen), so dass alle Schnittstellen identifiziert werden

können. An die Schnittstellen können dann entsprechende technische Sicherheitsanforderungen gestellt werden.

- Es muss eine Ist-Strukturanalyse von IT-Systemen und Anwendungen erfolgen.
- Es muss eine Schutzbedarfsfeststellung (z. B. von Anwendungen, IT-Systemen, Kommunikationsverbindungen, Räumen) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit erfolgen.

Natürlich sind auch relevante Gesetze und Vorschriften zu beachten. Dies kann besonders in Fällen, in denen Kunden oder Dienstleister länderübergreifend oder weltweit operieren, aufwendig sein.

Im Rahmen der Sicherheitsanforderungen ist festzulegen, welche Rechte (z. B. Zutrittsrechte, Zugriffsrechte auf Daten und IT-Systeme) dem Outsourcing-Dienstleister vom Kunden eingeräumt werden.

Die Sicherheitsanforderungen an Infrastruktur, Organisation, Personal und Technik müssen beschrieben werden. Es genügt hier oftmals die Verpflichtung auf ein Sicherheitsniveau, das IT-Grundschutz entspricht. Sollten darüber hinausgehende Anforderungen bestehen, müssen diese detailliert beschrieben werden. Dies hängt entscheidend von der Sicherheitsstrategie und bereits vorhandenen IT-Systemen und Anwendungen ab. Beispielsweise könnten folgende Punkte in Abhängigkeit vom Outsourcing-Vorhaben detailliert werden:

Organisatorische Regelungen und Prozesse

- Anforderungen an sicherheitskritische organisatorische Prozesse (z. B. Zeitrestriktionen für den Alarmierungsplan) können spezifiziert werden.
- Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein ISB mit speziellen Kenntnissen (z. B. Host-Kenntnissen) beim Outsourcing-Dienstleister benannt werden muss.

Hard- und Software

- Der Einsatz zertifizierter Produkte (z. B. gemäß Common Criteria oder ITSEC) beim Outsourcing-Dienstleister kann gefordert werden.
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen können gestellt werden. Beispielsweise kann in diesem Zusammenhang der Grad und die Methode der Lastverteilung (z. B. für Web-Server mit Kundenzugriff bei sehr vielen Kunden) vorgegeben werden.
- Vorgaben an die Mandantenfähigkeit sowie die diesbezügliche Trennung von Hard- und Software können formuliert werden. Beispielsweise kann festgelegt werden, dass keine IT-Systeme des Kunden in Räumen untergebracht werden dürfen, in denen bereits IT-Systeme anderer Mandanten des Dienstleisters stehen.

Kommunikation

- Spezielle Verfahren zur Absicherung der Kommunikation zwischen Dienstleister und Auftraggeber wie Einsatz von Verschlüsselungs- und Signaturverfahren können fest vorgegeben werden.

Kontrollen und QS

- Allgemeine Anforderungen bezüglich Kontrolle und Messung von Informationssicherheit, Qualität oder auch Abläufen und organisatorischen Regelungen können festgelegt werden, z. B. Zeitintervalle, Zuständigkeiten.
- Gewünschte Verfahren oder Mechanismen für die Kontrolle und Überwachung, wie unangekündigte Kontrollen vor Ort, Audits (unter Umständen durch unabhängige Dritte) können spezifiziert werden.
- Anforderungen an die Protokollierung und Auswertung von Protokollierungsdaten können festgelegt werden.

Generell bilden die festgelegten Sicherheitsanforderungen eine der Grundlagen für die Wahl eines geeigneten Outsourcing-Dienstleisters. Spezielle Sicherheitsanforderungen müssen jedoch eventuell an das von Dienstleistern umsetzbare Sicherheitsniveau angepasst werden.

Bei Ausschreibungen oder bei der Auswahl eines Outsourcing-Dienstleisters sollte immer eine Leistungsbeschreibung oder ein Pflichtenheft erstellt werden mit den folgenden Inhalten:

- Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung) sowie
- Beschreibungen zum geforderten Qualitätsniveau, das nicht zwangsläufig dem Niveau des Auftraggebers entsprechen muss,
- Anforderungen an die Informationssicherheit und
- Kriterien zur Messung von Servicequalität und Informationssicherheit.

In Einzelfällen kann es notwendig sein, die Detailanforderungen bezüglich Informationssicherheit nur gegen eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement) an Dienstleister herauszugeben, da sich daraus Hinweise auf existierende oder geplante Sicherheitsmechanismen ableiten lassen.

OPS.2.1.M2 Rechtzeitige Beteiligung der Personalvertretung (S)

Die rechtzeitige und umfassende Information der Personalvertretung empfiehlt sich grundsätzlich bei allen Projekten, die die betrieblichen Interessen der Beschäftigten berühren. Hierzu gehören im Allgemeinen auch Outsourcing-Vorhaben. Eine frühzeitige Einbindung der Personalvertretung des Outsourcing-Kunden sollte möglichst schon in der Angebots- und Planungsphase des Outsourcing stattfinden. Dies kann zum Gelingen des Projekts beitragen. Die frühzeitige Einbeziehung kann Zeitverzögerungen bei der Umsetzung von Maßnahmen verhindern und die Akzeptanz für das Outsourcing-Vorhaben erhöhen. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden. Zudem ist die Expertise jener Mitarbeiter, die später im Rahmen der konkreten Prozesse rund um das Outsourcing-Vorhaben arbeiten, ein nicht zu unterschätzender Erfolgsfaktor bei der Umsetzung.

Rechtliche Grundlage der Beteiligung der Personalvertretung sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern sowie einzelne Vorschriften des Bürgerlichen Gesetzbuchs (BGB).

Mit Outsourcing-Vorhaben gehen oft Maßnahmen einher, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeitern ermöglichen. Dies bedarf z. B. der Mitbestimmung der Personalvertretung.

Die Übertragung von Aufgaben oder Prozessen einer Institution an einen Dritten führt in der Regel auch zu Veränderungen in der Personalstruktur, was ebenfalls die Einbindung der Personalvertretung notwendig macht. Dies kann auch bedeuten, dass Mitarbeiter nach der Umsetzung eines Outsourcing-Vorhabens vom Outsourcing-Kunden zum Dienstleister wechseln müssen. Für den Kunden, also den ursprünglichen Arbeitgeber, besteht in diesem Fall eine Informationspflicht. Die Arbeitnehmer sind vor dem Betriebsübergang schriftlich zu unterrichten. Die Mitarbeiter müssen nicht individuell unterrichtet werden, es ist jedoch empfehlenswert, auf die speziellen Auswirkungen für spezifische Arbeitnehmergruppen individuell einzugehen. Inhalte der Unterrichtung werden in § 613a Abs. 5 BGB festgeschrieben.

Auch die Folgen für die Betriebsverfassungsorgane selbst müssen im Rahmen eines Outsourcing-Vorhabens geprüft werden. Hierzu ist es empfehlenswert, eine professionelle Rechtsberatung hinzuzuziehen.

OPS.2.1.M3 Auswahl eines geeigneten Outsourcing-Dienstleisters (S)

Da die Auswahl des Outsourcing-Dienstleisters eine weitreichende und risikobehaftete Entscheidung ist, sollten für jedes Outsourcing-Vorhaben klare Auswahl-Kriterien festgelegt werden. Es sollte ein Anforderungsprofil mit den Sicherheitsanforderungen an das Outsourcing-Vorhaben erstellt werden. Außerdem sollten Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal

vorliegen. Im Folgenden sind beispielhafte Bewertungskriterien beschrieben, die bei der Entscheidung für einen Outsourcing-Dienstleister berücksichtigt werden sollten.

Transparenz

Der Outsourcing-Dienstleister sollte die für seine Leistungserbringung grundlegenden Prozesse, so transparent darstellen können, dass zweifelsfrei von einer Vertragserfüllung durch ihn ausgegangen werden kann. Dem Outsourcing-Kunden sollten zudem die Sicherheitsvorkehrungen, die der Outsourcing-Dienstleister für das spezielle Outsourcing-Vorhaben getroffen hat, soweit nötig bekannt sein. Dies soll insbesondere ein reibungsloses Zusammenspiel der Sicherheitsmechanismen zwischen den Outsourcing-Partnern ermöglichen.

Prüfung der Sicherheitsanforderungen

Der Outsourcing-Kunde muss sich mit den Sicherheitsanforderungen auf Seiten des Outsourcing-Dienstleisters insofern befassen, dass der Outsourcing-Dienstleister mindestens das gewünschte Sicherheitsniveau des Outsourcing-Kunden abdeckt. Fordert der Outsourcing-Kunde beispielsweise einen hohen Schutzbedarf, muss der Outsourcing-Dienstleister mindestens die Anforderungen für einen hohen Schutzbedarf erfüllen.

Reputation

Die Reputation eines Dienstleisters am Markt lässt sich quantitativ nur schwer erfassen. Erfahrungsberichte anderer Kunden, Medienberichte und auch die aktive öffentliche Präsenz des Dienstleisters können hier qualitativ betrachtet werden.

Referenzen

Der Dienstleister sollte Referenzen für ähnliche Outsourcing-Vorhaben aufweisen können. Dabei ist auf Interessenkonflikte durch Geschäftsbeziehungen zu Konkurrenten des Kunden zu achten.

Die angegebenen Referenzen sollten zumindest stichprobenartig hinterfragt werden. So können bestehende oder ehemalige Kunden des potenziellen Dienstleisters zu ihren Projekterfahrungen mit dem Dienstleister befragt werden.

Je nach Bedarf sollte der Dienstleister einschlägige Sicherheitsstandards umsetzen, z. B. ISO 27001 auf Basis von BSI IT-Grundschutz. Bei bestehenden Zertifizierungen muss der Outsourcing-Kunde darauf achten, dass der im Zertifikat enthaltene Geltungsbereich und Schutzbedarf den vom Outsourcing-Kunden benötigten Einsatzbereich umfasst. Hierzu ist eine Prüfung des zertifizierten Geltungsbereichs erforderlich.

Business Fit/Unternehmenskultur

Bei ausländischen Dienstleistern müssen besondere Aspekte bedacht werden. Dazu gehören beispielsweise: fremde Gesetzgebung, andere Haftungsregelungen, Spionagerisiken, andere Sicherheitskultur, im Partnerunternehmen oder durch die landesspezifische Gesetzgebung zugelassene und verwendbare Sicherheitsmechanismen.

Zudem sollte die Organisationsform des Dienstleisters betrachtet werden, da diese z. B. die Haftungsgrenzen beeinflussen kann. Weiterhin sollte die Eigentümerstruktur recherchiert werden, um mögliche Einflussfaktoren im Vorfeld abzuklären.

Abschließend sollte überprüft werden, inwieweit die beschriebenen Aspekte mit der Situation bzw. den Vorstellungen des Kunden vereinbar sind.

Anforderungen an Mitarbeiter

Auch an die Mitarbeiter eines Outsourcing-Dienstleisters sind Anforderungen zu stellen.

Der Outsourcing-Kunde sollte überprüfen, inwieweit die Mitarbeiter des Outsourcing-Dienstleisters über die notwendigen Qualifikationen verfügen. Zudem sollte die Anzahl der verfügbaren qualifizierten Mitarbeiter, die für den Outsourcing-Kunden zur Verfügung stehen, bewertet werden. Dabei sollten auch Vertretungsregelungen und Arbeitszeiten hinterfragt werden.

Bei der Wahl ausländischer Partner muss eine gemeinsame Sprache für die Kommunikation zwischen den eigenen Mitarbeitern und denen des Dienstleisters festgelegt werden. Hierbei sollte auch hinterfragt werden, ob die vorhandenen Sprachkenntnisse für die Klärung von Detailproblemen ausreichen. Hier sind zudem Aspekte wie unterschiedliche Zeitzonen oder rechtliche Besonderheiten zu beachten.

Abhängig von dem notwendigen Sicherheitsniveau für das Outsourcing-Vorhaben sollte, falls erforderlich, geprüft werden, ob eine Sicherheitsüberprüfung der Mitarbeiter vorliegt bzw. eine solche komplikationslos durchgeführt werden kann.

OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister (S)

Outsourcing-Verträge sind nicht, wie Kauf-, Werk- oder Dienstverträge, im Bürgerlichen Gesetzbuch (BGB) geregelt. Es ist demzufolge darauf zu achten, alle Aspekte eines Outsourcing-Projekts bei der Vertragsgestaltung schriftlich zu vereinbaren. Das Vertragswerk sollte dabei die erforderlichen Rechte und Pflichten der Outsourcing-Partner festschreiben. Die Art, der Umfang und der Detaillierungsgrad der vertraglichen Regelungen sollten dabei individuell an das Outsourcing-Vorhaben angepasst werden. Vertragliche Regelungen im Vorfeld sind insbesondere deshalb wichtig, weil viele Risiken für den Outsourcing-Kunden dadurch vorab reduziert bzw. vermieden werden können. Die folgenden Aspekte sind daher aus Sicht des Outsourcing-Kunden im Zuge jeder Vertragsgestaltung zu beachten.

Klare Spezifizierung und Abgrenzung der Leistung

Eine ungenaue Definition der Leistungserbringung führt oftmals zu nachträglichen und unvorhersehbaren Mehrkosten für den Outsourcing-Kunden, da dieser beispielsweise eine vermeintliche "Mehrleistung" des Outsourcing-Dienstleisters in Anspruch nehmen muss. Ansprüche des Dienstleisters auf eine Abgeltung bei zusätzlich erbrachten Leistungen können besser bewertet werden, wenn die zu erbringende Leistung klar definiert wurde. Es ist daher empfehlenswert, auch "selbstverständliche" Leistungen zu spezifizieren. Entsprechende Diskussionen beziehungsweise Meinungsverschiedenheiten, die das Geschäftsverhältnis zwischen den Vertragsparteien nachhaltig schädigen könnten, werden dadurch im Vorfeld bestmöglich vermieden. Zudem kann dem Risiko des Verlusts der Kontroll- und Steuerungsmöglichkeiten entgegengewirkt werden, wenn die auslagernde Institution mittels einer klaren Leistungsabgrenzung Abweichungen leichter erkennen bzw. nachweisen kann. In diesem Zusammenhang schafft der Outsourcing-Kunde zudem eine vertragsrechtliche Grundlage für mögliche Sanktionen oder Schadensersatzforderungen bei Schlecht- oder Nichterfüllung der Leistung.

Datenschutz und Datensicherheit

Weiterhin sollten Regelungen zur Einhaltung datenschutzrechtlicher Bestimmungen festgelegt werden. Dazu zählen u. a. Sicherheitsvorkehrungen, die der Outsourcing-Dienstleister im Zuge der Datenverarbeitung zu beachten hat. Dadurch soll gewährleistet werden, dass die Outsourcing-Partner die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) bzw. die EU-Datenschutz-Grundverordnung (EU-DSGVO) und andere Regelungen wie Sozialgesetzbuch (SGB) einhalten und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen schützten. Der Vertrag sollte die notwendigen Sicherheitsmaßnahmen festlegen, die von dem Outsourcing-Dienstleister ergriffen werden müssen, um einen unbefugten Zugriff auf die Daten des Outsourcing-Kunden zu verhindern. Zudem sollte festgelegt werden, in welcher Weise die Vertraulichkeit der Daten durch interkulturelle, technische, personelle und organisatorische Maßnahmen geschützt werden soll. Falls erforderlich sind zusätzliche Vereinbarungen zur Wahrung der Geschäftsgeheimnisse des Kunden vertraglich zu regeln.

Infrastruktur

- 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

- 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 Sicherheitsmaßnamen 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).
- Zugriffsmöglichkeiten des Outsourcing-Dienstleisters auf IT-Ressourcen des Outsourcing-Kunden: Wer greift wie 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

- 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.

Regelungen im Rahmen der Notfallvorsorge

Im Rahmen der Notfallvorsorge sollten zumindest die folgenden Aspekte geregelt werden, um eine kontinuierliche Fortführung des Geschäftsbetriebs zu gewährleisten:

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit.
- Erforderliche Maßnahmen beim Eintreten eines Störfalls.
- Reaktionszeiten und Eskalationsstufen.
- Mitwirkungspflicht des Outsourcing-Dienstleisters bei der Behebung von Notfällen.
- Art der Einbindung und zeitliche Abfolge von Notfallübungen beim Outsourcing-Dienstleister.
- 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 im Fall 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 wird. Besonders wenn Outsourcing-

Dienstleister und Outsourcing-Kunden unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Kunde von derartigen Vorkommnissen gänzlich überrascht werden.

Weiterverlagerungen

Es muss geregelt werden, wie Dritte, Subunternehmer und Unterauftragnehmern durch den Outsourcing-Dienstleister eingebunden werden. Allgemein empfiehlt es sich, dies nicht grundsätzlich auszuschließen, sondern sinnvolle Bedingungen festzulegen. Grundsätzlich sollte jede Weiterverlagerung nur zulässig sein, wenn alle Anforderungen erfüllt werden, die im Rahmen der bestehenden Outsourcing-Beziehungen an den Dienstleister gestellt werden. Der Outsourcing-Kunde sollte sich eine Zustimmung zur Weiterverlagerung vorbehalten.

Mandanten

Im Rahmen der Mandantentrennung muss der Outsourcing-Dienstleister sicherstellen, dass Störungen oder Notfälle bei anderen Mandanten nicht die Abläufe und IT-Systeme des Outsourcing-Kunden beeinträchtigen. Zudem dürfen die Daten des Outsourcing-Kunden unter keinen Umständen anderen Mandanten zugänglich werden.

Der Outsourcing-Dienstleister sollte daher vertraglich verpflichtet werden, ein Mandantenkonzept zu erstellen, in dem beschrieben ist, auf welche Weise die IT-Systeme und Anwendungen mandantenfähig betrieben werden. Falls notwendig, muss eine physische Trennung, d. h. dedizierte Hardware, vereinbart werden. Weiterhin kann festgelegt werden, dass die vom Outsourcing-Dienstleister eingesetzten Mitarbeiter nicht für andere Outsourcing-Kunden eingesetzt werden dürfen.

Änderungsmanagement und Testverfahren

Es müssen vertragliche Regelungen festgelegt werden, die es dem Outsourcing-Kunden jederzeit ermöglichen, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn sich beispielsweise gesetzliche Vorgaben ändern. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert wird.

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 diese damit nicht mehr in seinem Sinne weiterentwickeln kann. Der Evolutionspfad von IT-Systemen sollte daher ebenfalls vertraglich geregelt werden.

Eine kontinuierliche Verbesserung der Dienstleistungsqualität und des Sicherheitsniveaus sollte möglichst präzise in den Service/Security Level Agreements (SLAs) festgeschrieben werden. Dies gilt sowohl für den jeweiligen Zeitrahmen zur Behebung von Fehlern als auch für die Nachverfolgung der Sicherheitsanforderungen.

Des Weiteren sollten Testverfahren für neue Hard- und Software festgelegt werden. Dabei sind folgende Punkte einzubeziehen:

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

- Genehmigungsverfahren für die Durchführung von Tests.
- Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit und Kapazität).

Kontroll-und Prüfungsrechte

Die Qualität der Leistungserbringung muss regelmäßig kontrolliert werden. Dem Outsourcing-Kunden müssen die dazu notwendigen Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte zu den von ihm genutzten Räumlichkeiten vertraglich zugesichert werden. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies ebenfalls im Vertrag geregelt werden.

Allen Institutionen, die bei dem Outsourcing-Kunden Prüfungen durchführen müssen (z. B. Aufsichtsbehörden), müssen auch bei dem Outsourcing-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) wahrnehmen können.

Um die Prüfungs- und Kontrollmöglichkeiten zu gewährleisten, sollte der Outsourcing-Vertrag eine entsprechende Erklärung des Outsourcing-Dienstleisters enthalten, dass dieser eine, falls erforderlich auch unangekündigte, Prüfung des durch den Outsourcing-Kunden ausgelagerten Bereichs duldet.

Informationspflichten und Kommunikation

Der Dienstleister sollte vertraglich dazu verpflichtet werden, über alle Entwicklungen zu berichten, die einen Einfluss auf die Leistungserbringung haben könnten. Dadurch soll es dem Outsourcing-Kunden ermöglicht werden, rechtzeitig zu reagieren. Zudem sollte gewährleistet sein, dass der Outsourcing-Dienstleister regelmäßig über aktuelle (Sicherheits-) Vorkommnisse bzw. Probleme hinsichtlich interner Arbeitsabläufe berichtet. In dieser Hinsicht sind z. B. Ergebnisse von Revisionen relevant.

Um einen angemessenen Informationsfluss zu gewährleisten, sollten z. B. die Art der Information, die zu nutzenden Kommunikationswege und die jeweiligen Ansprechpartner (Rollen), an die bestimmte Informationen weitergeleitet werden sollen, vertraglich festgelegt werden.

Es sollten Regelungen für das Ende der Outsourcing-Beziehung spezifiziert werden. So sollten in jedem Fall Kündigungsfristen vereinbart und ausreichend dimensioniert werden. In Hinsicht auf die Dimensionierung der Kündigungsfristen ist darauf zu achten, dass dem Outsourcing-Kunden genügend Zeit bleibt, um die ausgelagerten Aktivitäten und Prozesse wieder zu integrieren oder auf einen anderen Outsourcing-Dienstleister zu übertragen.

Zudem kann der Outsourcing-Dienstleister falls erforderlich darauf verpflichtet werden, im Zuge einer Rückintegration oder einer Übertragung der Leistungserbringung auf einen anderen Outsourcing-Dienstleister auch nach dem Ende der Outsourcing-Beziehung unterstützend zur Verfügung zu stehen.

Des Weiteren ist der Outsourcing-Dienstleister vertraglich darauf zu verpflichten, nach Beendigung der Outsourcing-Beziehung alle Hard- und Software inklusive der darauf gespeicherten Daten, die sich ursprünglich im Besitz des Outsourcing-Kunden befanden, zurückzugeben oder zu vernichten.

OPS.2.1.M5 Festlegung einer Strategie zum Outsourcing (S)

Outsourcing-Vorhaben sind oftmals mit vielen Vorteilen verbunden. Diesen Vorteilen stehen jedoch einige Risiken gegenüber, die dazu führen können, dass die erwünschten Ziele nicht erreicht werden können. Zudem erfolgt die Bindung an einen Outsourcing-Dienstleister normalerweise für längere Zeit. Eine strategische Planung des Outsourcing-Vorhabens ist daher von großer Bedeutung.

Hierbei sollten wirtschaftliche, technische, rechtliche und organisatorische Aspekte bedacht werden. Zudem spielen sicherheitsrelevante Aspekte eine wichtige Rolle. Die Informationssicherheit sollte bereits bei Beginn der Planungen mit betrachtet werden, da ihr eine zentrale Bedeutung in Outsourcing-Vorhaben zukommt.

Festlegung der Outsourcing-Ziele

In jeder Outsourcing-Strategie sollten die Ziele des Vorhabens genau definiert werden. Dabei sollte stets die Konformität mit der Leitlinie für Informationssicherheit gewahrt werden. So dürfen die

Outsourcing-Ziele den übergeordneten Zielen der Institution sowie den daraus abgeleiteten Sicherheitszielen nicht widersprechen. Folgende Gesichtspunkte sollten betrachtet werden:

- Leitlinie für Informationssicherheit (Flexibilität, Abhängigkeiten, zukünftige Planungen),
- Machbarkeitsstudie mit Zusammenstellung der Rahmenbedingungen und
- betriebswirtschaftliche Aspekte mit Kosten-Nutzen-Abschätzung.

Nach ersten strategischen Überlegungen muss zunächst geklärt werden, welche Geschäftsprozesse, Aufgaben oder Anwendungen generell für ein Outsourcing in Frage kommen.

Dabei darf die Bedeutung der rechtlichen Rahmenbedingungen nicht unterschätzt werden. Gesetze könnten beispielsweise das Auslagern bestimmter Kernaufgaben einer Institution generell verbieten oder zumindest weitreichende Auflagen enthalten und die Beteiligung von Aufsichtsbehörden vorschreiben. In der Regel bleibt der Auftraggeber weiterhin gegenüber seinen Kunden oder staatlichen Stellen voll verantwortlich für Dienstleistungen oder Produkte, unabhängig davon, ob einzelne Aufgabenbereiche ausgelagert wurden.

Die Informationssicherheit wird leider häufig zu Beginn der Planung vernachlässigt, obwohl ihr eine zentrale Bedeutung zukommt. Dies gilt sowohl für technische als auch organisatorische Sicherheitsaspekte, denen im Outsourcing-Szenario eine entscheidende Rolle zukommt. Generell ist nämlich zu bedenken:

- Die Entscheidung zum Outsourcing ist in der Regel nicht einfach zu revidieren. Die Bindung an den Dienstleister erfolgt unter Umständen sehr langfristig.
- Ein Dienstleister hat häufig Zugriff auf Daten und Ressourcen des Kunden. Der Outsourcing-Kunde verliert dadurch die alleinige und vollständige Kontrolle über Daten und Ressourcen. Je nach Outsourcing-Vorhaben betrifft dies dann auch Daten mit erhöhtem Schutzbedarf.
- Für die technische Umsetzung des Outsourcing-Vorhabens ist es notwendig, dass zwischen Kunden und Dienstleister Daten übertragen werden. Dadurch ergibt sich automatisch ein erhöhtes Gefahrenpotential.
- In der Regel ist es erforderlich, dass Mitarbeiter oder Subunternehmer des Outsourcing-Dienstleisters (und damit Betriebsfremde) zeitweise in den Räumlichkeiten des Kunden arbeiten müssen. Auch dadurch ergibt sich ein erhöhtes Gefahrenpotential.
- Im Rahmen eines Outsourcing-Vorhabens müssen neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt werden. Die Folgen der notwendigen Umstellungen müssen geklärt und abgeschätzt werden.
- Für jeden Outsourcing-Dienstleister besteht ein nicht zu unterschätzender Interessenkonflikt: Einerseits muss er die Dienstleistung möglichst kostengünstig erbringen, um seinen Gewinn zu maximieren, andererseits erwartet der Outsourcing-Kunde hohe Dienstleistungsqualität, Flexibilität und kundenfreundliches Verhalten. Dieser Punkt ist erfahrungsgemäß der am häufigsten unterschätzte. Während IT-Manager in der Regel sehr kritisch und kostenbewusst sind und Versprechungen von Herstellern und Beratern mit großer Skepsis begegnen, ist beim Outsourcing leider oft das Gegenteil zu beobachten. Allzu leicht verfällt hier der Kunde den Werbeaussagen der Dienstleister in der frohen Erwartung, seine IT-Kosten signifikant senken zu können. Die Praxis lehrt jedoch, dass höchstens die Dienstleistungen in der Zukunft erbracht werden, die von Anfang an vertraglich fixiert worden sind. Stellt sich heraus, dass die Dienstleistungsqualität unzureichend ist, weil der Kunde Leistungen erwartet, die er – im Gegensatz zum Outsourcing-Dienstleister – als selbstverständlich erachtet, sind Nachbesserungen in der Regel ohne hohe zusätzliche Kosten nicht zu erwarten. Jeder IT-Manager, der über Outsourcing nachdenkt, sollte sich im Vorfeld die Mühe machen, nachzurechnen, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit Kunde und Dienstleister beide von dem Vertragsverhältnis profitieren. Bei dieser Rechnung stellt sich vielleicht heraus, dass eine seriöse Leistungserbringung zu den versprochenen niedrigen Kosten höchst unwahrscheinlich ist.

Um die Outsourcing-Strategie festzulegen, muss daher immer eine individuelle Sicherheitsanalyse durchgeführt werden. Nur so kann letztendlich festgestellt werden, wie bestehende Geschäftsprozesse oder Informationsverbünde abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Die Sicherheitsanalyse sollte nach der in der IT-Grundschutz-Vorgehensweise beschriebenen Methodik durchgeführt werden:

- Es sollte zunächst eine Strukturanalyse durchgeführt werden, um den aktuellen Ist-Zustand zu ermitteln.
- Danach erfolgt eine Schutzbedarfsfeststellung.
- Darauf aufbauend müssen geeignete Sicherheitsmaßnahmen ausgewählt und auf die jeweiligen Rahmenbedingungen des Outsourcing-Vorhabens angepasst werden. Dabei sind auch der Handlungsbedarf, die Prioritäten sowie die Kosten für die umzusetzenden Maßnahmen zu identifizieren. Die Ergebnisse können dann insbesondere in die Betrachtung der Wirtschaftlichkeit des Outsourcing-Vorhabens mit einbezogen werden.

Wenn der Schutzbedarf wichtiger IT-Systeme oder Anwendungen hoch ist oder die Modellierung des Informationsverbunds nach IT-Grundschutz nicht möglich ist, muss eine Sicherheitsanalyse (z. B. Risikoanalyse) durchgeführt werden. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll.

Schlussendlich wird dennoch ein gewisses Restrisiko durch den Outsourcing-Kunden zu tragen sein. Die Ergebnisse der Sicherheitsanalyse gehen unmittelbar in die Kosten-Nutzen-Abschätzung ein.

Das Management darf bei der Entwicklung einer erfolgversprechenden, langfristigen Outsourcing-Strategie den Blick nicht nur auf die Einsparung von Kosten richten. Die Auswirkungen eines Outsourcing-Vorhabens auf die Aufgabenerfüllung, das Geschäftsmodell und das Dienstleistungs- oder Produktportfolio müssen ebenfalls berücksichtigt werden. Sollen Standardabläufe oder Kerngeschäftsprozesse ausgelagert werden? Wichtig ist in diesem Zusammenhang, dass die Fähigkeit, Anforderungen an die Informationssicherheit selbst zu bestimmen und zu kontrollieren, in ausreichendem Maße erhalten wird. Insbesondere an die Weiterentwicklung und Pflege selbstentwickelter IT-Systeme und Anwendungen sollte gedacht werden.

Folgende Chancen, die grundsätzlich mit einem Outsourcing-Projekt verbunden sind, können als Ziele für den Outsourcing-Kunden formuliert werden:

- Kostenvorteile: Die Reduzierung der Kosten bei der Leistungserbringung und die damit verbundene Steigerung der Produktivität stellen nach wie vor das Hauptmotiv aus Sicht von Outsourcing-Kunden dar. Kostenersparnisse können dabei z. B. durch Personaleinsparungen erzielt werden. Sowohl Löhne und Gehälter als auch Kosten für Qualifizierung und Weiterbildung entfallen auf den Outsourcing-Dienstleister. Fixe Personalkosten können so zu variablen Dienstleistungskosten umgewandelt werden, die je nach Bedarf zeitnah angepasst werden können. Auch Bedarfe an Ressourcen, wie z. B. die IT-Infrastruktur, können schnell angepasst werden, ohne dadurch das Investitionsrisiko zu erhöhen.
- Konzentration auf Kernkompetenzen: Die Auslagerung bestimmter Prozesse kann zu einer Entlastung des Managements, des IT-Betriebs oder anderen Fachbereichen führen, so dass sich diese auf ihre Kernkompetenzen konzentrieren können. Auf diese Weise werden Personalkapazitäten frei, die anderweitig eingesetzt werden können.
- Verbesserung des Sicherheitsniveaus: Im Idealfall kann durch das Outsourcing-Vorhaben ein besseres Sicherheitsniveau erreicht werden. Der Outsourcing-Dienstleister ist auf seinem Leistungsgebiet in der Regel durch einen hohen Spezialisierungsgrad gekennzeichnet. Gerade in der Informationssicherheit ist einschlägiges Know-how erforderlich, um regelmäßig die aktuellen Sicherheitshinweise, Security-Bulletins, Updatemeldungen und Bug-Reports auszuwerten, ihre Relevanz zu erkennen und bei Bedarf rasch die richtigen Schritte einzuleiten. Outsourcing-Dienstleister können zudem das Einspielen von Sicherheitspatches oder

sicherheitsrelevanten Systemkonfigurationen zeitlich auf die Produktion des Outsourcing-Kunden anpassen, so dass der Betrieb durch diese Vorgänge nicht gestört wird.

- Kompetenzinseln: Interne IT-Abteilungen wachsen oft nicht im gleichen Maße wie die Organisation, für die sie zuständig sind. Ein Flickenteppich aus Workarounds und anderen provisorischen Sicherheitslösungen kann die Folge sein. Zusätzlich könnten nur wenige, wenn nicht nur ein einziger Mitarbeiter in der Lage sein, die komplette IT-Infrastruktur zu überblicken. Fallen diese Mitarbeiter aus oder verlassen sie die Organisation des Outsourcing-Kunden, ergeben sich gravierende Sicherheitsmängel, da die Kompetenz zur Pflege der IT-Infrastruktur nicht mehr vorhanden ist. Die Outsourcing-Dienstleister können hingegen in der Regel auf mehrere gleich qualifizierte Experten zurückgreifen, die sich gegenseitig vertreten können. Zusätzlich verfügen sie über eine homogene IT-Infrastruktur, die aufgrund ihres hohen Standardisierungsgrads insbesondere aus sicherheitstechnischer Sicht leichter zu pflegen ist und eine höhere Resilienz aufweist. Hierbei ist jedoch sicherzustellen, dass der Outsourcing-Kunde weiterhin den Überblick über seine Gesamtstruktur hat.
- Nutzung von externem Know-how und Verbesserung des Leistungsangebots: Ein weiteres Outsourcing-Motiv kann die Nutzung von externem Know-how sein, ohne dies selbst vorhalten oder entwickeln zu müssen. Hierdurch ergeben sich wiederum Kosteneinsparungspotenziale. Zudem kann die Qualität der Leistungserbringung durch die Nutzung des Spezialwissens des Outsourcing-Dienstleisters gesteigert werden. Eine effizientere Prozessgestaltung und risikoarme Diversifikation kann zudem durch die Verringerung der Fertigungstiefe realisiert werden. Outsourcing-Kunden können ihre Kompetenzen auf schlanke Wertschöpfungsprozesse konzentrieren, die durch spezialisierte Outsourcing-Dienstleister unterstützt werden. Auch in diesem Zusammenhang kann die Unterstützung eines Outsourcing-Dienstleisters möglicherweise dazu beitragen, das allgemeine Sicherheitsniveau zu verbessern. Outsourcing-Dienstleister werden aufgrund ihrer Spezialisierung häufig besser geeignet sein, dynamische Sicherheitslagen auszuwerten und unmittelbar notwendige Schritte einzuleiten. Insbesondere mit Blick auf neue IT-Lösungen und die damit einhergehende steigende Komplexität kann ein spezialisierter Dienstleister nützlich sein, der die Balance zwischen Sicherheit und einem erweiterten Leistungsangebot bzw. mehr Funktionalität halten kann.
- Risikoverlagerung: Neben der bereits erwähnten Übertragung von Investitionsrisiken ist ein weiterer Vorteil die Auslagerung weiterer Risiken, z. B. Fehlverhalten von Mitarbeitern, Softwarefehler oder das Eintreten von Katastrophen. Ausfälle dieser Art treffen allerdings nicht allein den Outsourcing-Dienstleister, sondern können immer auch auf den Outsourcing-Kunden zurückfallen. Selbst bei einer vertraglich vereinbarten kompletten Übertragung der Risiken auf den Outsourcing-Dienstleister bleibt fraglich, inwiefern dieser im Haftungsfall zahlungsfähig ist. Mögliche Imageschäden hingehen treffen meist den Outsourcing-Kunden allein.

Risiken und Herausforderungen

Den Outsourcing-Zielen stehen eine Reihe vielseitiger Outsourcing-Risiken gegenüber. Diese Risiken sollten in der Outsourcing-Strategie beschrieben und in Folge dessen im Rahmen jedes Outsourcing-Projekts berücksichtigt werden. Im Folgenden werden mögliche Risiken eines Outsourcing-Vorhabens beschrieben.

- Versteckte Kosten: Ein Outsourcing-Vorhaben ist nicht nur mit Kosteneinsparungen verbunden. Die damit einhergehenden Kosten sollten im Vorhinein genau analysiert und abgewogen werden. So sind z. B. Kosten für die Steuerung des Outsourcing-Vorhabens und das Vertragsmanagement einzukalkulieren. Während einer Outsourcing-Beziehung kommt es auf der Seite des Outsourcing-Kunden möglicherweise zu unerwarteten Kommunikations- und Koordinationskosten. Wurde zu Beginn des Outsourcing-Vorhabens ein zu geringer Leistungsumfang definiert, werden im Laufe der Vertragsbeziehung eventuelle Anpassungen notwendig. Solche Vertragsänderungen können teilweise erhebliche Zusatzkosten nach sich

ziehen. Zudem können einmalige Kosten entstehen. Hierzu zählen beispielsweise Abfindungen oder Kosten für Neueinstellungen, die im Zuge personeller Umstrukturierungen anfallen.

- Verlust von Know-how: Die Vorteile durch die Nutzung externen Know-hows bringen auch Risiken mit sich. So bewirkt die dauerhafte Nutzung des Fachwissens von Dritten in der Regel nach und nach den Verlust des eigenen Know-hows. Die Mitarbeiter des Outsourcing-Kunden geben ihr Fachwissen im Zuge eines Outsourcing-Projekts oftmals ab oder auf bzw. erhalten dieses nicht weiter aufrecht. Die Kompetenz für die ausgelagerten Funktionen liegt letztendlich nicht mehr in den Händen des Outsourcing-Kunden. Besonders kritisch ist eine solche Situation, wenn das Know-how der Mitarbeiter des Outsourcing-Dienstleisters nicht mehr angemessen ist und somit gravierende Sicherheitslücken entstehen, diese jedoch nicht entdeckt werden können, weil das benötigte Fachwissen beim Outsourcing-Kunden nicht mehr vorhanden ist. Der Verlust des eigenen Know-hows steigert demnach zwangsläufig die Abhängigkeit von dem Outsourcing-Dienstleister.
- Abhängigkeit vom Outsourcing-Dienstleister: Die Abhängigkeit des Outsourcing-Kunden vom Outsourcing-Dienstleister steigt insbesondere mit der Komplexität des ausgelagerten Prozesses und mit der Dauer der Outsourcing-Beziehung. Für den Outsourcing-Kunden besteht stets das Risiko einer Preisanhebung durch den Outsourcing-Dienstleister, nachdem das Outsourcing-Vorhaben weit fortgeschritten ist und eine Rückintegration nicht wirtschaftlich oder zu risikobehaftet wäre. Infolgedessen müssen die Kostenerhöhungen häufig akzeptiert werden, wodurch die Wirtschaftlichkeit des Outsourcing-Vorhabens im Nachhinein stark beeinflusst werden kann. Die dadurch notwendig gewordenen Kosteneinsparungen führen wiederum oftmals zu Einsparungen im Sicherheitsbereich und haben entsprechende Auswirkungen auf das Sicherheitsniveau.
- Ansehens- und Vertrauensverlust: Die aus Leistungsdefiziten des Outsourcing-Dienstleisters resultierenden Auswirkungen auf Outsourcing-Kunden können zu weitreichenden Konsequenzen führen. Entsprechende Folgen, wie z. B. ein Ansehens- oder Vertrauensverlust, treffen den Outsourcing-Kunden selbst, ganz gleich, ob die Schuld ursprünglich bei dem Outsourcing-Dienstleister liegt.
- Verlust von Kontroll- und Steuerungsmöglichkeiten: Der Outsourcing-Kunde besitzt gegenüber dem Outsourcing-Dienstleister in der Regel nur eingeschränkte Befugnisse in Bezug auf Anordnungen. Daraus resultieren eingeschränkte Steuerungsmöglichkeiten und ein erhöhter Abstimmungsbedarf im Vergleich mit einer Eigenerbringung. Auch die Kontrollmöglichkeiten des Outsourcing-Kunden sind eingeschränkt. Trotz vereinbarter Zugangsrechte wird der Outsourcing-Kunde nicht über alle Informationen hinsichtlich Organisation und Abläufe des Outsourcing-Dienstleisters verfügen.
- Einblicke Dritter in interne Betriebsabläufe und Daten: In Abhängigkeit von der Art des Outsourcing-Vorhabens kann der Outsourcing-Dienstleister Informationen über interne Betriebsabläufe und möglicherweise auch über Geschäftsverbindungen des Outsourcing-Kunden erhalten. So ist für letzteren eine alleinige Kontrolle über diese Informationen nicht mehr sichergestellt. Zudem ist es eventuell notwendig, dass die Mitarbeiter des Outsourcing-Dienstleisters zumindest vorübergehend in den Räumlichkeiten der Outsourcing-Kunden arbeiten, wodurch ihnen der Zugang zu Daten und Ressourcen erleichtert wird. Handelt es sich bei einer Offenlegung von Informationen um personenbezogene Daten, sind zusätzlich die einschlägigen Datenschutz-Gesetze zu beachten.
- Risiken für die Sicherheit der Daten: Die Sicherheit der Daten ist ein wesentlicher Aspekt im Rahmen einer Auslagerung. Besonders Risiken, die aus dem Verlust der Verfügbarkeit von IT-Systemen und Daten resultieren, z. B. bei einem Systemausfall einer IT-Auslagerung, sind zu betrachten. Generell wird bei Einbeziehung eines Outsourcing-Dienstleisters die Anzahl der Übertragungswege und somit auch das Gefahrenpotenzial erhöht. Typische Bedrohungen sind Hacker-Angriffe, Schadprogramme, Ausfälle aufgrund technischen Versagens bei der Soft- und Hardware und weitere Schadensszenarien, z. B. durch Strom- oder Klimaanlagenausfälle. Die

Risiken des Dienstleisters wirken sich direkt auf den Outsourcing-Kunden aus. Schon kleinere bzw. Teilausfälle führen zu inkonsistenter oder fehlerhafter Datenverarbeitung.

Beschreibung der Vorgehensweise im Rahmen des Outsourcing-Projekts

Nachdem die Outsourcing-Ziele sowie die zu berücksichtigenden Outsourcing-Risiken in der Outsourcing-Strategie dargelegt wurden, sollte eine strukturierte Vorgehensweise für das Management eines Outsourcing-Vorhabens skizziert werden. Ausführliche Vorgaben zur Durchführung können in nachgelagerten Dokumenten (z. B. einer Rahmenanweisung für das Outsourcing) beschrieben werden. Mittels der beschriebenen Vorgehensweise sollen die Outsourcing-Risiken behandelt und somit die Erreichung der gesetzten Ziele gewährleistet werden. Im Rahmen der beschriebenen Vorgehensweise sollten die folgenden Phasen des Outsourcing-Vorhabens berücksichtigt werden:

- Selektion möglicher Outsourcing-Bereiche: Welche Prozesse und/oder Aktivitäten dürfen aufgrund gesetzlicher Vorgaben oder aus strategischen Gründen (Kernkompetenzen) nicht ausgelagert werden? Zudem ist im Rahmen dieser Phase eine Kosten-Nutzen-Analyse durchzuführen, auf deren Grundlage die Wirtschaftlichkeit des geplanten Outsourcing-Vorhabens beurteilt werden kann.
- Erfassung und Beurteilung des Outsourcing-Sachverhalts: Welche individuellen Risiken bestehen für den betrachteten Sachverhalt, wie ist diesen zu begegnen bzw. welche Anforderungen sind aufgrund dessen an einen potenziellen Outsourcing-Dienstleister zu stellen?
- Auswahl eines passenden Outsourcing-Dienstleisters: Die Auswahl sollte aufgrund der zuvor ermittelten Risiken und der daraus abgeleiteten (Sicherheits-)Anforderungen getroffen werden.
- Vertragsgestaltung: Welche Aspekte sind vertraglich zu regeln?
- Überführung in den Regelbetrieb: Welche (Sicherheits-)Maßnahmen sind im Zuge der Übertragung der Leistungserbringung auf den Outsourcing-Dienstleister zu ergreifen?
- Regelbetrieb und Beendigung: Welche Steuerungs-, Überwachungs-, Kontroll- und Abstimmungsmaßnahmen sind im laufenden Betrieb zu ergreifen und welche Vorsorgemaßnahmen sind für eine erwartete bzw. unerwartete Beendigung des Outsourcing-Vorhabens zu treffen?

OPS.2.1.M6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (S)

Für jedes Outsourcing-Vorhaben muss ein Sicherheitskonzept existieren, das auf den Sicherheitsanforderungen des Outsourcing-Kunden basiert (OPS.2.1.M1 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*).

Das Gesamt-Sicherheitskonzept sollte nach Beauftragung eines Outsourcing-Dienstleisters erstellt werden. Outsourcing-Projekte sind dadurch gekennzeichnet, dass sich viele technische und organisatorische Details erst im Laufe der Planung und bei Migration der IT-Systeme ergeben. Das Sicherheitskonzept wird daher in den wenigsten Fällen von Beginn an vollständig und endgültig sein und muss während der Migrations- und der Betriebsphase von allen Beteiligten stetig weiterentwickelt und konkretisiert werden. Spezielle Anforderungen an das Sicherheitskonzept für die Migrationsphase (als Teil des Gesamt-Sicherheitskonzepts) sind in OPS.2.1.M13 *Sichere Migration bei Outsourcing-Vorhaben* beschrieben.

Generell unterscheiden sich Sicherheitskonzepte für Outsourcing-Vorhaben nur wenig von Sicherheitskonzepten für Informationsverbünde unter der eigenen Kontrolle. Zu berücksichtigen ist jedoch, dass bei einem Outsourcing-Vorhaben weitere Parteien involviert sein können. Dies können neben dem Outsourcing-Dienstleister beispielsweise Netzprovider und Unterauftragnehmer des Dienstleisters sein. Auch durch diese dürfen die vereinbarten Sicherheitsziele nicht beeinträchtigt werden. Die erforderlichen Sicherheitsanforderungen für deren Aufgabengebiete müssen entweder im

Sicherheitskonzept des Dienstleisters integriert oder in eigenständigen Sicherheitskonzepten beschrieben sein, die dem Outsourcing-Kunden vorzulegen sind.

Jede am Outsourcing-Vorhaben beteiligte Partei sollte ein eigenes Sicherheitskonzept erstellen und umsetzen, welches auch das spezielle Outsourcing-Vorhaben umfasst. Damit sind folgende Sicherheitskonzepte erforderlich:

- für den Einflussbereich des Outsourcing-Kunden,
- für den Einflussbereich des Outsourcing-Dienstleisters sowie
- für die Schnittstellen und die Kommunikation zwischen diesen Bereichen.

Der Outsourcing-Kunde sollte hierauf aufbauend ein Sicherheitskonzept für das Gesamtsystem erstellen, welches die Sicherheit im Zusammenspiel der Einzelsysteme betrachtet.

Die verschiedenen Teil-Konzepte müssen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister abgestimmt werden. Dabei ist der Outsourcing-Kunde am Sicherheitskonzept des Outsourcing-Dienstleisters nicht direkt beteiligt, sollte aber in einem Audit prüfen, ob es vorhanden und ausreichend ist. Für das Audit kann der Outsourcing-Kunde dabei auch auf externe Dritte zurückgreifen. Im Verlauf des Vorhabens sollten alle Teil-Konzepte kontinuierlich auf Aktualität und Korrektheit geprüft werden.

Das Gesamt-Sicherheitskonzept sollte alle relevanten Risiken berücksichtigen, die mit dem Outsourcing-Vorhaben einhergehen. Mögliche Risiken werden in OPS.2.1.M5 *Festlegung einer Strategie zum Outsourcing* beschrieben.

Die in OPS.2.1.M1 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben* und OPS.2.1.M4 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* genannten Sicherheitsanforderungen bilden die Basis für das Gesamt-Sicherheitskonzept. Aufbauend auf den dort beschriebenen grundlegenden Anforderungen muss im Sicherheitskonzept die detaillierte Ausgestaltung erfolgen, wobei beispielsweise die Maßnahmen konkretisiert und Ansprechpartner namentlich festgelegt werden.

Erfahrungsgemäß ist der Übergang (Migration) von Aufgaben und IT-Systemen vom Kunden zum Outsourcing-Dienstleister eine Projektphase, in der verstärkt mit Sicherheitsvorfällen zu rechnen ist. Aus diesem Grund müssen im Sicherheitskonzept Regelungen und Maßnahmen zur Migration behandelt werden, die in OPS.2.1.M13 *Sichere Migration bei Outsourcing-Vorhaben* genauer behandelt werden.

Im Folgenden sind einige Aspekte und Themen aufgelistet, die im Sicherheitskonzept im Detail beschrieben werden sollten. Da die Details eines Sicherheitskonzeptes direkt vom Outsourcing-Vorhaben abhängen, ist die Liste als Anregung zu verstehen und erhebt keinen Anspruch auf Vollständigkeit. Neben einem Überblick über die Gefährdungslage, die der Motivation der Sicherheitsmaßnahmen dient, und den infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

Organisation

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen bzw. Vernichten.
- Festlegung von Aktionen, für die das "Vier-Augen-Prinzip" anzuwenden ist.
- Vertretungsregelungen.

Hard- und Software

- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren.
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen.
- Einsatz von Prüfungssystemen für Datei-Integrität, um Veränderungen z. B. nach erfolgreichen Angriffen zu erkennen.

- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen.
- Einsatz kaskadierter Firewall-Systeme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters.
- sorgfältige Vergabe von Benutzer-Kennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters.

Kommunikation

- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Kunde, um vertrauliche Daten zu schützen.
- Authentisierungsmechanismen.
- Detailregelungen für weitere Netzanbindungen.
- Detailregelungen für den Datenaustausch.

Kontrollen und QS

- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Informationssicherheit, Dienstqualität, Abläufen und organisatorische Regelungen.

Notfallvorsorge

- Outsourcing-Kunden und -Dienstleister müssen aufeinander abgestimmte Notfallkonzepte haben, siehe auch OPS.2.1.M14 *Notfallvorsorge beim Outsourcing*.

OPS.2.1.M7 Festlegung der möglichen Kommunikationspartner (S)

Im Rahmen eines Outsourcing-Vorhabens werden vom Outsourcing-Kunden viele Informationen zu externen Kommunikationspartnern übertragen. Hierbei muss sichergestellt werden, dass die jeweiligen Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzen. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat beziehungsweise erhalten wird.

Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen, sowohl aufseiten des Outsourcing-Kunden als auch aufseiten des Outsourcing-Dienstleisters sowie für alle weiteren Beteiligten. Hierfür ist es erforderlich, dass alle Informationen entsprechend ihrer strategischen Bedeutung für die auslagernde Institution klassifiziert sind (OPS.2.1.M1 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*).

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 z. B. BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenübertragung oder Datenträgeraustausch zu erhalten. Diese Übersicht muss aktuell und korrekt sein.

Zu diesem Zweck sind den Verantwortlichkeiten bestimmte Rollen zuzuweisen, die diese Aufgaben übernehmen und die Einhaltung der getroffenen Regelungen regelmäßig aufseiten des Outsoucing-Kunden wie auch des Outsourcing-Dienstleisters überprüfen.

OPS.2.1.M8 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters (S)

Im Rahmen von Outsourcing-Projekten werden die Mitarbeiter des Outsourcing-Dienstleisters eventuell auch in Räumlichkeiten des Outsourcing-Kunden eingesetzt. Dies kann auf Dauer dazu

führen, dass die Mitarbeiter des Outsourcing-Kunden nicht immer genau wissen, ob es sich um eigene oder externe Mitarbeiter handelt.

Personal des Outsourcing-Dienstleisters, das über einen längeren Zeitraum innerhalb der Räumlichkeiten des Outsourcing-Kunden tätig ist und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommt, ist schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

Weiterhin sollte sichergestellt werden, dass die Mitarbeiter des Outsourcing-Dienstleisters – ähnlich wie eigene Mitarbeiter – in ihre Aufgaben eingewiesen werden. Soweit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist, sind sie über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie die institutionsweite Sicherheitsvorgaben zu unterrichten. Dies gilt in besonderem Maß, wenn sie in den Räumlichkeiten des Outsourcing-Kunden arbeiten.

Zudem sollte sichergestellt sein, dass auch für die Mitarbeiter des Outsourcing-Dienstleisters angemessene Vertretungsregelungen existieren. Auch die jeweiligen Vertreter müssen ordnungsgemäß eingewiesen und auf die Einhaltung der geltenden Gesetze, Vorschriften und internen Regelungen verpflichtet werden.

Außerdem muss geregelt sein, wie mit Personalveränderungen beim Outsourcing-Dienstleister umgegangen wird. Diese müssen dem Outsourcing-Kunden rechtzeitig mitgeteilt werden.

Bei Beendigung des Outsourcing-Verhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Den Mitarbeitern des Outsourcing-Dienstleisters sind zudem sämtliche Zugangsberechtigungen und Zugriffsrechte zu entziehen.

Sollten Mitarbeiter des Outsourcing-Dienstleisters lediglich kurzfristig oder einmalig vor Ort eingesetzt werden, sollten diese wie Besucher behandelt werden und sich dementsprechend beispielsweise nur in Begleitung von Mitarbeitern des Outsourcing-Kunden in dessen Räumlichkeiten aufhalten dürfen.

OPS.2.1.M9 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner (S)

Vor der Anbindung des Netzes des Outsourcing-Kunden an das Netz des Outsourcing-Dienstleisters sollte eine detaillierte Vereinbarung (Data Connection Agreement, DCA) geschlossen werden. In dieser muss genau definiert sein, wer Zugriff auf das Netz des Outsourcing-Kunden erhält und unter welchen Bedingungen dies geschehen soll. Analog muss geregelt sein, wer aus dem Netz des Outsourcing-Kunden mit welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf das Netz des Outsourcing-Dienstleisters erhalten soll. Eine solche 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 Protokolldaten 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).

Die Vereinbarung sollte durch jene Personen abgeschlossen werden, welche die Verantwortung für die Einhaltung der Vereinbarungen tragen. Dafür ist zunächst zu klären, wer die Verantwortung für die Netzanbindung tragen sollte, da hier üblicherweise unterschiedliche Bereiche einer Institution involviert sind. Sinnvollerweise sollte hierzu ein Team gebildet werden, zu dem zumindest der Informationssicherheitsbeauftragte, der Leiter des IT-Betriebs, die Fachverantwortlichen der betroffenen Bereiche und der Datenschutzbeauftragte gehören. Bei kritischen Entscheidungen sollten alle genannten Personen beteiligt werden, da sich deren Interessen erfahrungsgemäß stark voneinander unterscheiden können.

Bevor eine Netzanbindung aktiviert wird, sollten alle Sicherheitsmängel auf beiden Seiten ausgeräumt worden sein. Hier sollte auch ein Weg gefunden werden, wie sich der Outsourcing-Kunden von dem Sicherheitsniveau des Outsourcing-Dienstleisters oder sonstiger Dritter überzeugen kann, beispielsweise durch IT-Grundschutz-Checks oder Stichproben vor Ort. Auf keinen Fall darf die Beseitigung von Sicherheitslücken in den Echtbetrieb verschoben werden, da dies erfahrungsgemäß niedriger priorisiert wird als reine Probleme in Bezug auf die Verfügbarkeit.

Dem Outsourcing-Kunden sollten nur die Dienste zur Verfügung gestellt werden, die vertraglich vereinbart wurden und unbedingt erforderlich sind. Bei ausländischen Outsourcing-Dienstleistern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie, Datenschutz und Urheberrecht.

Falls durch die Netzanbindung Sicherheitsvorfälle auftreten, muss klar definiert sein, wer wann die Verbindung trennen darf, wer darüber zu informieren ist und welche Eskalationsschritte vorzusehen sind.

OPS.2.1.M10 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern (S)

Datenaustausch zwischen dem Outsourcing-Kunden und dem Outsourcing-Dienstleister kann über verschiedene Wege erfolgen, neben Netzanbindung (siehe OPS.2.1.M9 *Vereinbarung über die Anbindung an Netze der Outsourcing-Partner*) z. B. über Datenträgeraustausch oder per E-Mail. Neben den Sicherheitsmaßnahmen, die bereits beim sporadischen Datenaustausch zu beachten sind, sollten bei einem regelmäßigen Datenaustausch mit festen Kommunikationspartnern Vereinbarungen getroffen werden, um diesen möglichst reibungslos zu gestalten. Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

- Benennung von Ansprechpartnern sowohl für organisatorische als auch für technische Probleme und insbesondere für sicherheitsrelevante Ereignisse,
- die erforderlichen technischen Informationen, also Festlegungen darüber:
  - welche Anwendungen und Datenformate unterstützt werden,
  - welche Verfügbarkeit zu gewährleisten ist, also wie häufig beispielsweise E-Mails zu lesen und wie schnell sie zu beantworten sind,
- welche Sicherheitsmaßnahmen beim Datenaustausch gewährleistet werden müssen, also z. B.
  - dass die Daten vor und nach dem Austausch auf Schadsoftware zu überprüfen sind,
  - wie die Daten vor Transportschäden und unbefugtem Zugriff zu schützen sind (verschlossene Behältnisse, Checksummen, Verschlüsselung),
  - wie das Schlüsselmanagement geregelt ist,
  - dass die Daten auf der Senderseite frühestens nach Bestätigung des korrekten Empfangs gelöscht werden dürfen, falls eine Löschung erforderlich ist,
- eine Vertraulichkeitsvereinbarung,
- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen),
- eine 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 im Baustein CON.9 *Informationsaustausch*.

OPS.2.1.M11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (S)

Nachdem die Übertragung der Leistungserbringung auf den Outsourcing-Dienstleister erfolgt ist, muss die Informationssicherheit auch im laufenden Betrieb gewährleistet werden. Dabei unterscheiden sich die IT-bezogenen Einzelaufgaben generell nicht von denen, die zu planen und durchzuführen sind, wenn kein Outsourcing betrieben wird. Besonderheiten ergeben sich jedoch dadurch, dass die Aufgaben auf mehrere Parteien verteilt und daher zusätzliche Abstimmungs- und Kontrollmaßnahmen erforderlich sind. Im Rahmen dessen sind folgende Aspekte zu berücksichtigen:

- Dokumentationen und Richtlinien müssen regelmäßig aktualisiert werden.
- Die geltenden Sicherheitskonzepte aller Beteiligten müssen daraufhin geprüft werden, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten. Insbesondere sollte der Outsourcing-Dienstleister den Outsourcing-Kunden über wichtige Änderungen in seinem Einflussbereich informieren.
- Das Mandantenkonzept des Outsourcing-Dienstleisters sollte daraufhin überprüft werden, ob es den Sicherheitsanforderungen des Kunden genügt.
- Regelmäßige Kontrollen zu folgenden Aspekten sind durchzuführen:

  - Durchführung der vereinbarten Audits.
  - Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen.
  - Wartungszustand von IT-Systemen und Anwendungen.
  - Rechtezuweisung durch den Outsourcing-Dienstleister (Missbrauch von Rechten).
  - Einsatz von Mitarbeitern, die dem Outsourcing-Kunden nicht gemeldet wurden (z. B. bei Vertretungen).
  - Einhaltung der Anforderungen in Hinsicht auf Performance, Verfügbarkeit, Qualitätsniveau.
  - Einhaltung der Anforderungen im Rahmen der Datensicherung.
- Regelmäßige Abstimmungsrunden zu folgenden Punkten sind abzuhalten:
  - 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.
  - Identifikation und Analyse von Problemen.
  - gegenseitiges Feedback und Identifizierung von Verbesserungspotenzialen.
  - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) sollten frühzeitig besprochen werden.
- Es sollten regelmäßige Übungen und Tests zu folgenden Themen durchgeführt werden:
  - Reaktion auf Systemausfälle (Teilausfall, Totalausfall).
  - Wiedereinspielen von Datensicherungen.
  - Beherrschung von Sicherheitsvorfällen.

OPS.2.1.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. Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz einzelner Sicherheitsmaßnahmen und damit zu einer Gefährdung der Gesamtsicherheit führen.

Änderungen, die während eines Outsourcing-Vorhabens auf Seiten des Outsourcing-Dienstleisters vorgenommen werden, sind ebenso durch das Änderungsmanagement des Outsourcing-Kunden zu betrachten. Daher sollte mit dem Outsourcing-Dienstleister vertraglich geregelt werden, dass Sicherheitsaspekte bei der Planung und Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten berücksichtigt werden. Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten vom Outsourcing-Dienstleister geplant, getestet, genehmigt und dokumentiert werden. Vom Outsourcing-Dienstleister ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware usw.).

- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für den Outsourcing-Kunden.
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme Benutzergruppen).
- räumliche Änderungen, z. B. nach einem Umzug.

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfung und Test 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
- die Überarbeitung der institutionsweiten Leitlinie zur Informationssicherheit erforderlich machen können.
- Bei größeren Änderungen sollte vereinbart werden, dass das Informationssicherheitsmanagement des Outsourcing-Kunden vom Outsourcing-Dienstleister schon im Vorfeld involviert werden muss. Eine Rückfalllösung sollte gemeinsam erarbeitet werden.

OPS.2.1.M13 Sichere Migration bei Outsourcing-Vorhaben (S)

Nach Beauftragung des Outsourcing-Dienstleisters muss zunächst ein vorläufiges Sicherheitskonzept für die Migrationsphase entwickelt werden, in dem auch die Test- und Einführungsphase als Teilaspekt des Outsourcing-Vorhabens betrachtet wird (siehe OPS.2.1.M6 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*). Zum einen sind in dieser Phase zahlreiche Betriebsfremde involviert, zum anderen müssen Abläufe etabliert, Aufgaben übertragen und IT-Systeme neu eingerichtet bzw. angepasst werden. Ein sorgfältiger Testbetrieb ist deshalb überaus wichtig. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die selten sehr sicher sind. Es ist daher beispielsweise sicherzustellen, dass produktive Daten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das Sicherheitskonzept ausgeschlossen werden.

Vor der Erstellung eines Migrationskonzepts als Teil des Sicherheitskonzepts für ein Outsourcing-Vorhaben sollte ein Informationssicherheitsmanagement-Team speziell für die Migrationsphase beim Outsourcing-Kunden eingerichtet werden. Dieses muss während der Migrationsphase auf Sicherheitsbelange achten und durch geeignete Maßnahmen auch schon vor der Migration dafür sorgen, dass ein sicherer IT-Betrieb während der Migration gewährleistet ist. Die Größe des Informationssicherheitsmanagement-Teams hängt dabei von Art und Größe des Outsourcing-Vorhabens ab, als Minimum kann es aus einem Sicherheitsexperten von jedem Outsourcing-Partner bestehen.

Dem Informationssicherheitsmanagement-Team kommen dabei folgende Aufgaben zu, aus denen sich Regelungen und Vorgaben ableiten, die im Migrationskonzept zu erfassen sind:

- Es ist ein gemischtes Team aus Mitarbeitern des Outsourcing-Kunden und des Outsourcing-Dienstleisters zu bilden. Dieses kann auch durch externe Experten verstärkt werden, um spezielles Know-how verfügbar zu machen.
- Für die Migrationsphase muss ein Sicherheitskonzept erstellt werden.
- Die Verantwortlichkeiten und Hierarchien für die Migrationsphase sind festzulegen. Dabei ist es wichtig, dass klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige Ansprechpartner festgelegt werden. Zusätzlich ist darauf zu achten, dass auf beiden Seiten Verantwortlichkeiten auch auf hohen Ebenen festgelegt 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 Inbetriebnahme der Dienstleistung geplant werden.
- Es sind geeignete Mitarbeiter auf beiden Seiten der Outsourcing-Partner für die Test- und Einführungsphase und für den späteren Betrieb auszuwählen. Vertraglich kann sich ein Outsourcing-Kunde natürlich auch ein Mitspracherecht bei der Personalauswahl des Outsourcing-Dienstleisters einräumen lassen.
- Die Mitarbeiter des Outsourcing-Kunden sind zum Verhalten während und nach der Migrationsphase zu schulen. In der Regel sind die Mitarbeiter dabei mit neuen und unbekannten Ansprechpartnern konfrontiert. Dies birgt die Gefahr des Social Engineerings (z. B. Anruf eines vermeintlichen Mitarbeiters des Sicherheitsteams des Outsourcing-Dienstleisters).
- Der Outsourcing-Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Outsourcing-Kunden genau kennenlernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen. Die produktiven IT-Systeme dürfen dabei nicht vernachlässigt werden. Dazu ist im Vorfeld zu überprüfen, ob die vorgesehenen Mitarbeiter zur Verfügung stehen. Zusätzlich müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Outsourcing-Dienstleister übernehmen soll, sollten ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit sollte dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch das Outsourcing-Vorhaben. Die Dokumentation neuer IT-Systeme oder Teilsysteme sollte dabei ebenfalls sichergestellt sein.
- Während der Migration sollte ständig überprüft werden, ob die SLAs oder die vorgesehenen Security Level Agreements 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, sind verstärkt Mitarbeiter zu Bereitschaftsdiensten zu verpflichten.

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.
- Ansprechpartner und Zuständigkeiten werden mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert.

- Die Systemkonfigurationen sind zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.
- Als letzte Aufgabe muss das Outsourcing-Vorhaben nach der Migrationsphase in den sicheren Regelbetrieb überführt werden. Dabei ist vor allem darauf zu achten, dass alle während der Migrationsphase notwendigen Ausnahmeregelungen, z. B. erweiterte Zugriffsrechte, aufgehoben werden.

OPS.2.1.M14 Notfallvorsorge beim Outsourcing (S)

Für die Notfallvorsorge beim Outsourcing gelten grundsätzlich die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb von Geschäftsprozessen oder IT-Systemen. Besonderheiten ergeben sich aber dadurch, dass die Notfallvorsorge von unterschiedlichen Parteien und dadurch auch für unterschiedlich verteilte IT-Systeme gewährleistet werden muss.

Generell müssen Notfallvorsorgekonzepte für die IT-Systeme beim Outsourcing-Kunden und beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren. In OPS.2.1.M4 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* wird beschrieben, welche Aspekte bereits im Rahmen der Vertragsgestaltung geregelt werden sollten. Im Notfallvorsorgekonzept müssen diese Vorgaben im Detail beschrieben werden. Im Rahmen der Notfallvorsorge sollten zudem insbesondere die folgenden Aspekte berücksichtigt werden:

- Zuständigkeiten, Ansprechpartner und Abläufe sollten klar geregelt und vollständig dokumentiert werden.
- Es sollten detaillierte Arbeitsanweisungen für bestimmte Fehlersituationen erstellt werden.
- Es sollte ein Konzept für die Durchführung regelmäßiger Notfallübungen erarbeitet werden.

Die Informationssicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Outsourcing-Dienstleisters ab. Oftmals werden die IT-Systeme des Outsourcing-Kunden vom Personal des Outsourcing-Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die Anwendung liegt dennoch ausschließlich beim Outsourcing-Kunden. Tritt ein Fehler in der Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das Gesamtsystem zu besitzen. Durch das Notfallvorsorgekonzept müssen dem Outsourcing-Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden. Im Zuge dessen kann es auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot eines IT-Systems).

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. Liegen anwendungsspezifische Probleme vor, benötigt der Outsourcing-Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit Ansprechpartnern aufseiten des Outsourcing-Kunden, damit er richtig reagieren kann. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Patch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Kunden vorhanden sind.

Wichtig ist auch, dem Outsourcing-Dienstleister Informationen über den Schutzbedarf der betroffenen Daten und IT-Systeme zur Verfügung zu stellen, damit er angemessen handeln kann.

Der Outsourcing-Kunde sollte regelmäßig überprüfen, wie effizient und effektiv die Notfallmaßnahmen des Outsourcing-Dienstleisters umgesetzt sind und wie gut diese mit den eigenen Notfallmaßnahmen abgestimmt sind. Daher sollten regelmäßig gemeinsame Notfallübungen von Outsourcing-Kunden und Outsourcing-Dienstleister durchgeführt werden.

OPS.2.1.M15 Geordnete Beendigung eines Outsourcing-Verhältnisses (S)

Ein Outsourcing-Verhältnis endet entweder beabsichtigt und erwartet (z. B. nach dem Erreichen eines definierten Ziels nach dem Projektende oder aufgrund einer Übertragung der Leistungserbringung auf einen anderen Dienstleister) oder unbeabsichtigt und unerwartet (z. B. aufgrund einer Insolvenz des Outsourcing-Dienstleisters).

Um im Zuge einer beabsichtigten Beendigung ausreichend Zeit für die Rückintegration bzw. Übertragung der ausgelagerten Prozesse und Aktivitäten auf einen anderen Outsourcing-Dienstleister zu haben, sind ausreichende Kündigungsfristen zu vereinbaren (siehe OPS.2.1.M4 *Vertragsgestaltung mit dem Outsourcing-Dienstleister*). Die Einhaltung der vereinbarten Kündigungsfristen kann jedoch nicht immer gewährleistet werden. Aufgrund von Insolvenzen, technischen Störungen oder Naturkatastrophen kann die Leistungserbringung des Outsourcing-Dienstleisters kurzfristig ausfallen. Um diesem Risiko zu begegnen und in solchen Fällen die Kontinuität sowie die Qualität der Leistungserbringung aufrecht zu erhalten, sollte der Outsourcing-Kunde über angemessene Notfallkonzepte verfügen (siehe OPS.2.1.M14 *Notfallvorsorge beim Outsourcing*). Dies gilt insbesondere für Outsourcing-Vorhaben, die zeitkritische Prozesse und Aktivitäten betreffen.

Sollte im Anschluss an die Beendigung der Outsourcing-Beziehung eine Übertragung der Leistungserbringung auf einen anderen Outsourcing-Dienstleister erfolgen, ist diese als neues Outsourcing-Vorhaben anzusehen. Demnach sind dafür alle Anforderungen des Bausteins erneut umzusetzen. Beim Insourcing, also der Wiedereinlagerung der Leistungserbringung in die eigene Institution, gilt dies analog. Für Strategie, Sicherheitskonzept für Insourcing, Migration und Notfallvorsorge gelten die gleichen Anforderungen wie bei einem "klassischen" Outsourcing-Vorhaben.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- Die IT-Systeme, -Anwendungen und Arbeitsabläufe beim Outsourcing-Dienstleister müssen ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an den Kunden übertragen beziehungsweise übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden. Die Löschung der Datenbestände sollte sich der Outsourcing-Kunde schriftlich bestätigen lassen.
- Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, sind zu überprüfen. Der Outsourcing-Kunde sollte alle Berechtigungen löschen, die für den Outsourcing-Dienstleister oder Dritte eingerichtet wurden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen, müssen eingewiesen und geschult werden.
- Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der ehemalige Dienstleister noch für Rückfragen und Hilfestellungen zur Verfügung steht.
- Bei Beendigung des Outsourcing-Verhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Den Mitarbeitern des Outsourcing-Dienstleisters sind zudem sämtliche Zugangsberechtigungen und Zugriffsrechte zu entziehen.

OPS.2.1.M16 Sicherheitsüberprüfung von Mitarbeitern (H)

Der Outsourcing-Kunde sollte sich die Qualifikation, aber auch die Vertrauenswürdigkeit der Mitarbeiter des Outsourcing-Dienstleisters geeignet nachweisen lassen.

Die Möglichkeiten, die Vertrauenswürdigkeit von Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Zudem sind die Ergebnisse meist wenig aussagekräftig, z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme neuer oder externer Mitarbeiter in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten,
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist

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.

Wenn Personal auf Seiten des Outsourcing-Dienstleisters intern beim Kunden eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit Outsourcing-Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

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.2.1 *Outsourcing für Kunden* sind keine Quellenverweise vorhanden