SOPHOS
Partner Program

Managed Service Provider

Verträge zwischen Anbieter und Kunden
rechtssicher gestalten

Inhalt

Vorwort

Unternehmen sind unabhängig ihrer Größe jeden Tag neuen Bedrohungen ausgesetzt. Diese sind vielfältig und nehmen naturgemäß mit dem technischen Fortschritt stetig zu. Diesen Herausforderungen müssen sich Unternehmen stellen. Sie müssen rechtzeitig reagieren um sich und Dritte, insbesondere ihre Kunden vor Schäden zu schützen. Bei der Absicherung der unternehmensinternen IT-Infrastruktur stellen sich zwei zentrale Fragen: Zum einen muss geklärt werden, ob das Unternehmen bereits über hinreichend effektive Schutzmaßnahmen verfügt und – sollte dies noch nicht der Fall sein – wie diese konkret umgesetzt werden können.

Hinsichtlich der Frage des „Ob" empfehle ich mein Whitepaper zum Thema „Datenschutz und IT-Sicherheit in Recht und Praxis" vom Februar 2017. Diese Darstellung setzt sich mit den Haftungsrisiken im Falle der unzureichenden Absicherung der unternehmensinternen IT-Infrastruktur auseinander und stellt entsprechende Lösungsansätze vor, um das Haftungsrisiko auf ein Minimum zu reduzieren.

Bei der Frage des „Wie" handelt es sich ebenfalls um eine rechtliche, aber zu weiten Teilen auch ökonomisch geprägte Frage. Der Unternehmer muss sich im Vorfeld klar sein, wie er die erforderlichen Schutzmaßnahmen umsetzt, um die im Whitepaper vom Februar 2017 dargestellten Haftungsfallen zu umgehen. Die Antwort liegt in einem umfassenden Sicherheitskonzept. In Abhängigkeit von Größe des Unternehmens und Sensibilität der Daten werden hierfür eine bestimmte Menge an personellen und finanziellen Ressourcen benötigt. Es liegt auf der Hand, dass insbesondere Unternehmen, die mit personenbezogenen Daten in Berührung kommen, wie Kreditinstitute oder Betriebe im Gesundheitswesen, besondere Sicherheitsvorkehrungen treffen müssen, um den Einblick vor unbefugten Dritten zu schützen.

Die Bereitstellung personeller und finanzieller Ressourcen stellt vor allem mittelständische Unternehmen vor einer kaum zu bewältigen Herausforderung, da Ressourcen hierfür nur begrenzt verfügbar sind und für das erforderliche Sicherheitskonzept häufig mehr Ressourcen benötigt werden, als zur Verfügung stehen.

Der Spagat zwischen Kosteneinsparung und ausreichender Sicherheit führt zur Überlegung, das IT-Sicherheitsmanagement an Fremdunternehmen auszulagern (sog. Outsourcing). In der Tat ist die Auslagerung des IT-Sicherheitsmanagements für den Unternehmer nicht zu Unrecht attraktiv. Eines der wesentlichen Hauptargumente für die Auslagerung der IT-Sicherheit ist sicherlich die Kosteneinsparung, da auf eine bereits vorhandene Infrastruktur und Expertise zurückgegriffen werden kann. Deren Kosten werden auf sämtliche Nutzer, namentlich alle Kunden des Fremddienstleisters verteilt.

Ein weiteres Argument für das IT-Security-Outsourcing ist die Tatsache, dass Fremddienstleister, deren Kerngeschäft in der IT-Sicherheit liegt, auf diesem Gebiet so spezialisiert, dass er seinem Kunden Lösungen anbieten kann, die der Kunde mangels hinreichendem Know-how und Ressourcen im vergleichbaren Rahmen nicht entwickeln kann.

Schließlich bietet das Outsourcing Modell auch maximale Skalierbarkeit. Das bedeutet, dass das Unternehmen den Umfang der Sicherheitslösung sowohl in quantitativer als auch qualitativer Hinsicht jederzeit an die individuellen Bedürfnisse anpassen kann, wenn etwa das Unternehmen wächst und mehr Geräte abgesichert werden müssen. Diese Skalierbarkeit vermeidet es, ein bestehendes IT-Sicherheitsmanagement zugunsten einer völlig neuen und meist kostenintensiven Lösung über Bord werfen zu müssen.

Somit profitieren vor allem Unternehmen, die bei der Frage des „Ob“ zu dem Ergebnis gekommen sind, dass die gegenwärtigen Schutzmaßnahmen nicht dem geforderten Niveau entsprechen und das Niveau angesichts knapper Ressourcen nicht bereitgestellt werden kann.

Im Zuge der erhöhten Nachfrage nach Outsourcing Lösungen haben sich auch für Fremddienstleister, insbesondere Systemhäuser neue Geschäftsfelder erschlossen. Das Model des sog. Managed Service Providers (MSP) oder konkreter: Managed Security Service Providers (MSSP) bietet wiederkehrende und planbare Einnahmen. Zudem wird die Bindung an den Kunden gefördert.

MSP bietet somit für den Kunden (Unternehmer) und dem Fremddienstleister (MSP) eine Vielzahl von Vorteilen. Da MSP-Verträge jedoch keine einmaligen Lieferverträge (sondern sog. Dauerschuldverhältnisse) sind und der Vertragsgegenstand angefangen von der Installation bis zum Support ein breites Leistungsspektrum abdeckt, sind viele Anbieter mit der Vertragsgestaltung überfordert.

Dieser Beitrag widmet sich der Fragestellung zur Gestaltung von Verträgen zwischen MSP und Kunden speziell für IT-Sicherheitslösungen. Die einzelnen vertraglichen Regelungen hängen aufgrund des breiten Leistungsspektrums stark vom Einzelfall ab. Naturgemäß kann und soll diese Darstellung keine Rechtsberatung ersetzen. Aufgrund der Komplexität ist auch dringend von der ungeprüften Verwendung von Formularen abzuraten. Dieser Beitrag richtet sich vor allem an den juristischen Laien. Die nachfolgende Darstellung soll die typischen Fallstricke erläutern und die rechtlichen Möglichkeiten der Vertragsgestaltung veranschaulichen, ohne den gebotenen Rahmen zu sprengen.

Magdeburg, im Mai 2017

Rechtsanwalt Sebastian Müller

Inhaber der Rechtsanwaltskanzlei Sebastian Müller und Inhaber der Akademie für Recht, Wirtschaft und Psychologie und Lehrbeauftragter an der Hochschule für Wirtschaft und Recht Berlin

I. Der Begriff des Managed (Security) Services Providers

Der Begriff des Managed Security Service Providers ist juristisch nicht definiert. Vielmehr handelt es sich um einen Begriff aus der Betriebswirtschaft und bedeutet so viel wie das Verwalten und Überwachen von IT-Anlagen im Kontext der Sicherheit.

Managed Security Services umfassen also primär Dienstleistungen zur Absicherung der unternehmensinternen IT-Infrastruktur. Das Leistungsspektrum reicht dabei von einfachen standardisierten Sicherheitslösungen, wie Anti-Malware, Firewalls und der üblichen Netzwerksicherheit bis hin zu komplexen und hochindividualisierten Diensten, um Unternehmensumgebungen mit besonderen Bedürfnissen gerecht zu werden.

Eine wesentliche Besonderheit ist die Tatsache, dass es sich hierbei nicht um eine einmalige Leistung, sondern um ein Dauerschuldverhältnis handelt. Einmalige Lieferverträge haben meist den Verkauf der Sicherheitslösung und gegebenenfalls die Einrichtung für die erstmalige Inbetriebnahme des Produkts zum Gegenstand. Damit wäre der Vertrag erfüllt.

Dauerschuldverhältnisse sind Lieferverträge, die über einen längerfristigen, häufig auch unbestimmten Zeitraum erfolgen. Der Leistungsgegenstand von Dauerschuldverhältnissen ist umfangreicher als bei einmaligen Leistungen. Vertragsgegenstand ist neben der Ersteinrichtung auch

- das Bereitstellen des Produktes für eine (un)bestimmte Lizenzlaufzeit,
- dessen Einrichtung im Unternehmen,
- Support sowie
- Pflege und Wartung.

Vereinfacht gesagt erwirbt der Kunde vom Systemhaus eine Rund-um-Komplettlösung für sämtliche Belange der IT-Sicherheit. Er lagert also das IT-Sicherheitsmanagement an das Fremdunternehmen aus.

II. Dürfen Unternehmen die IT-Sicherheit an Fremddienst-leister auslagern?

Viele Unternehmen sind im Hinblick der zuvor beschriebenen Vorteile, insbesondere wegen der Kostenvorteile durchaus geneigt, die IT-Sicherheit an ein an das Systemhaus (MSP) des Vertrauens auszulagern.

1. Zulässigkeit der Auslagerung

Allerdings begegnen Fremddienstleister häufig noch Bedenken seitens des Unternehmens. Viele Unternehmen haben Zweifel, ob sie das IT-Sicherheitsmanagement auslagern dürfen, ohne sich dadurch Haftungsrisiken unterwerfen zu müssen.

Die gute Nachricht: Grundsätzlich dürfen Unternehmen die IT-Sicherheit an den MSP auslagern. Hierbei müssen jedoch einige Dinge beachtet werden. Zunächst muss differenziert werden, ob der MSP faktischen Zugriff auf die Daten von Dritten, insbesondere Kunden des Unternehmers hat. Sofern dies zutrifft, sollte sich das Unternehmen in jedem Fall von seinen Kunden und sonstigen betroffenen Dritten, eine Einwilligung bzgl. der Datenweitergabe einholen (näheres zur Datensicherheit im Abschnitt IV.)

2. Haftungsrisiken für das Unternehmen bei Auslagerung

Es lässt sich jedoch nicht leugnen, dass die Auslagerung des IT-Managements an den MSP durchaus Haftungsrisiken für den Unternehmer bereithält. Sofern die Kunden oder Mitarbeiter des Unternehmens aufgrund eines Datenverlustes oder Datenmissbrauchs Schäden erleiden, muss sich der Unternehmer das Verschulden des MSP grundsätzlich zurechnen lassen. Denn der MSP ist sog. Erfüllungsgehilfe gemäß § 278 BGB. Der MSP wird mit Wissen und Wollen des Unternehmers bei der Erfüllung einer dem Unternehmer obliegenden Verbindlichkeit tätig. Vereinfacht gesagt tut der MSP das, was eigentlich der Unternehmer hätte tun müssen, insbesondere die Daten vor Verlust und unbefugten Dritten zu schützen. Da sich der Unternehmer einer anderen Person (nämlich dem MSP) bedient, muss er im Schadensfall das Verschulden des MSP gegen sich gelten lassen. Deshalb ist es für den Unternehmer von überragender Bedeutung, dass der MSP

zuverlässig und sorgfältig arbeitet. Der Kunde kann, wenn er von einem Dritten in Anspruch genommen wird, die gezahlte Schadenssumme von dem MSP zurückfordern (sog. Regressanspruch). Die Haftung des MSP gegenüber dem Kunden kann jedoch vertraglich beschränkt werden (näheres zur Haftungsbeschränkung im Abschnitt III. 2. a. (3)).

Die Haftung für das Verschulden des MSP muss aus Sicht des Unternehmens jedoch nicht dazu führen, vom MSP-Modell Abstand zu nehmen. Denn wie eingangs erwähnt, verfügen Fremddienstleister regelmäßig über eine höhere Fachkompetenz, was die Absicherung von IT-Systemen anbelangt. Es spricht vieles dafür, die Sicherheit an einen hoch spezialisierten Fremddienstleister anzuvertrauen, als die IT-Sicherheit im Zweifelsfall halbherzig selbst in die Hand zu nehmen, weil die notwendigen Ressourcen nicht zur Verfügung stehen. Dies ist insbesondere dann der Fall, wenn die eigenen Mitarbeiter nicht ausreichend qualifiziert sind.

Letzteres birgt nämlich das Risiko wegen unzureichender Schutzmaßnahmen im Schadensfall wegen eigenem Verschulden des Unternehmers in Anspruch genommen zu werden. Der Unternehmer haftet im Ergebnis trotzdem, wenn er sich um die Sicherheit zwar selbst, aber nur unzureichend gekümmert hat. Solange jedoch der MSP über die erforderliche Expertise verfügt, kann sich der Unternehmer auf sein Kerngeschäft und die Wettbewerbsfähigkeit fokussieren und die IT-Sicherheit externen Spezialisten des Fremddienstleisters überlassen.

III. Vertragliche Regelungen

Nachdem sich das Unternehmen für die Auslagerung der IT-Sicherheit entschieden und sich daraufhin an das Systemhaus seines Vertrauens gewandt hat, stellt sich für den MSP die Frage, auf welcher vertraglichen Grundlage die Umsetzung des Kundenwunsches erfolgen soll. Der MSP muss also vorab klären, welche Qualität und welchen Leistungsumfang er seinem Kunden versprechen und erfüllen will.

Gemäß § 243 Abs. 1 BGB schuldet der MSP seinem Kunden grundsätzlich nur die Qualität nach mittlerer Art und Güte, also die „Durchschnittsqualität" die auch von anderen Anbietern erwartet werden kann.

Beispiel: Wenn im Kundenunternehmen ein Betriebsrat gewählt wurde und dieser gemäß § 40 Abs. 2 BetrVG Anspruch auf Zurverfügungstellung eines Computers gegenüber dem Arbeitgeber hat, muss der Arbeitgeber lediglich einen Computer nach „mittlerer Art und Güte" also einen durchschnittlichen Computer mit Maus, Tastatur und Drucker zur Verfügung stellen, der sich für *gewöhnliche Büroarbeiten eignet. Er muss also keinen High-End PC, insbesondere kein Gerät mit extravaganter Grafikkarte und exorbitantem Arbeitsspeicher* überlassen, *da diese Komponenten für gewöhnliche Büroarbeiten nicht erforderlich sind.*

Der oben genannte Sachverhalt ist aus Verständnisgründen bewusst einfach gestrickt. Dem MSP wird die Ermittlung eines solchen Referenzwertes – aufgrund des individuellen Leistungsspektrums und der besonderen Kundenwünsche – kaum gelingen. Es kann somit nicht ohne Weiteres der „Durchschnitt" einer Leistung für die Auslagerung der IT-Sicherheit bestimmt werden, da für jedes Unternehmen ein maßgeschneidertes Leistungspaket, kombiniert aus diversen Waren- und Servicedienstleistungen zusammengeschnürt wird. Ein direkter Vergleich unterschiedlicher Leistungspakete ist nicht möglich. Die Bestimmung dieses Referenzwertes ist jedoch für MSP und dem Kunden gleichermaßen von zentraler Bedeutung. Denn nur so kann der Kunde beurteilen, ob der MSP seine Leistung ordnungsgemäß erbracht hat und der MSP die Vergütung verlangen kann.

Dieses Problem lässt sich durch Vereinbarung sogenannter Service-Level-Agreements (SLA's) und Leistungsscheine lösen.

1. Transparenz dank Service-Level-Agreements (SLA) und Leistungsscheine

Um Klarheit für den Kunden und den MSP zu schaffen, empfiehlt es sich den Leistungsumfang und die Qualität schon bei Vertragsschluss möglichst detailliert festzulegen. Die Festlegung detaillierter Leistungen schafft Transparenz und hilft Missverständnisse, die das Kundenverhältnis nachhaltig schädigen, zu vermeiden.

Der MSP sollte in jedem Fall folgende wesentlichen Kernelemente festlegen:

a. Preis,

b. konkrete Leistungen,

c. Service-Level,

d. Mitwirkungspflichten und

e. Verantwortlichkeiten.

Naturgemäß wird der MSP versuchen, die für ihn vorteilhaftesten Regelungen in Form von modularen Einzel- oder Rahmenverträgen zu vereinbaren. Hier stellt sich die Frage, was noch zulässig und was nicht mehr erlaubt ist. Der Grundsatz der Vertragsfreiheit

gestattet den Parteien, den Inhalt von Verträgen frei zu bestimmen, solange nicht gegen geltendes Recht verstoßen wird. Bei Verträgen zwischen Unternehmern also B2B Geschäften sind die Regelungsbefugnisse sehr weitreichend und im Vergleich zum B2C Geschäft nur durch wenige Vorschriften, etwa Sittenwidrigkeit (§ 138 BGB) oder Verstöße gegen gesetzliche Verbote (§ 134 BGB) beschränkt.

Der MSP wird diese Vereinbarungen üblicherweise für eine Vielzahl von Kunden bereithalten, um die Vertragsbedingungen nicht jedes Mal von Grund auf neu mit dem Kunden aushandeln zu müssen. Dies wäre in Zeiten von Massengeschäften und der großen Anzahl von Kunden aus Kosten- und Zeitgründen auch kaum möglich. Juristisch gesehen handelt es sich hierbei um sog. Allgemeine Geschäftsbedingungen nach § 305 Abs. 1 Satz 1 BGB.

Bei der Verwendung Allgemeiner Geschäftsbedingungen ist Folgendes zu beachten:
Der Gesetzgeber geht zurecht davon aus, dass der Vertragspartner, der sich mit den Bedingungen einverstanden erklärt (i. d. R. also der Kunde) gegenüber dem Verwender (MSP) faktisch einen geringeren Einfluss in der Vertragsverhandlung ausüben kann. Er befindet sich also in einer „schwächeren" Position. Dieses Machtungleichgewicht zwischen dem MSP und dem Kunden soll ausgeglichen werden, indem der MSP bestimmte Vereinbarungen, die den Kunden unangemessen beachteiligen würden, zumindest in Formularverträgen nicht vereinbaren darf. Tut er dies doch, ist diese Klausel unwirksam (nicht jedoch der gesamte Vertrag!). Eine Auflistung verbotener Klauseln befindet sich in den §§ 308, 309 BGB. Auf verbotene Klauseln, die in der Praxis (aufgrund Unwissenheit) dennoch häufig verwendet werden, wird nachfolgend an geeigneter Stelle hingewiesen.

a. Preisvereinbarung

Die Preiskalkulation wird naturgemäß durch betriebswirtschaftliche Faktoren beeinflusst. Die Vereinbarung der Leistungsvergütung hingegen, ist eine Frage der rechtlichen Ausgestaltung. In jedem Fall muss dem Kunden klar sein, wann und für welche Leistungen eine Vergütung, in welcher Höhe anfällt.

Eine intransparente Preisgestaltung durch unklare Formulierung stört nicht nur die Kundenbeziehung, sondern gefährdet auch den Anspruch auf Vergütung.

An dieser Stelle wird vor bewusster Preisverschleierung und dem Verstecken von Kosten ausdrücklich gewarnt, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen. Denn unklar formulierte Vertragsklauseln muss der MSP im Zweifel gegen sich gelten lassen, mit der Folge, dass er die vereinbarte Vergütung nicht geltend machen kann.

Beispiel: Ein Kunde kauft bei der „Mal-Ware GmbH" einen Computer. Der Vertrag wird auch als „Kaufvertrag" bezeichnet. In den Allgemeinen Geschäftsbedingungen wurde allerdings auch ein kostenpflichtiger Wartungsvertrag untergeschoben. Mit einer solchen Klausel muss bei einem einfachen Kaufvertrag nicht gerechnet werden, sodass diese unwirksam ist. Der Händler hat somit für etwaig erfolgte Wartungsarbeiten am Computer keinen Anspruch auf Vergütung.

b. Vereinbarung der konkreten Leistung

Wie bereits eingangs erwähnt, muss die Leistung klar definiert werden. Nur so kann der Kunde prüfen, ob er zur Zahlung der Vergütung verpflichtet ist. Andernfalls besteht die Gefahr, dass der Kunde Einwände geltend machen wird, wenn er nicht sicher ist, ob die Leistung des MSP vereinbarungsgemäß oder nur unzureichend erbracht wurde.

Beispiel: Der Kunde lagert seine gesamte IT-Sicherheit auf den MSP aus. Er vertraut darauf, dass auch die Daten vor dem Verlust gesichert werden. Nachdem die Daten aufgrund eines Fehlers vom Mitarbeiter des Kunden versehentlich gelöscht wurden und sich der Kunde zwecks Wiederherstellung an den MSP wendet, verweist dieser auf den Leistungsvertrag, wonach die Anfertigung von Datensicherungskopien nicht zum Leistungsumfang gehören. Zwar enthalte die Vereinbarung eine Klausel mit der Bezeichnung „Schutz vor Datenverlust". Allerdings sei damit lediglich die Sicherung der Daten vor „Datendiebstahl" gemeint.

Diese Unsicherheit liegt regelmäßig auch nicht im Interesse des MSP. Im Gegenteil: Der MSP möchte verständlicherweise nach Erbringung der Leistung zügig abrechnen. Deshalb sollte er im Vorfeld sämtliche Faktoren, die zur Zahlungsverzögerung führen können, aus dem Weg schaffen. Je schneller der Kunde die Fälligkeit der Leistung überprüfen kann, desto schneller kommt der MSP an sein Geld. Damit dies dem Kunden ermöglicht wird, muss er den Ist- mit dem Sollzustand vergleichen können. Nur so kann er sich davon überzeugen, dass die Leistung frei von Defiziten ist.

Sinnvollerweise wird der Sollzustand in sog. Leistungsscheinen dokumentiert. Leistungsscheine gehören zum Hauptvertrag und definieren zusätzliche Leistungen. Empfehlenswert ist auch die Vereinbarung zugehöriger Zahlungsmodalitäten sowie sonstiger leistungsspezifischer Randbedingungen. Der Kunde soll im Zeitpunkt des Vertragsschlusses keinen Zweifel daran haben, was zum Leistungsumfang gehört und was nicht. Die Leistungsbeschreibung, sollte daher sämtliche Leistungen so detailliert, wie nur möglich beschreiben.

Bei umfangreichen Auslagerungsprojekten kann die Verwendung mehrerer Leistungsscheine sinnvoll sein. Dabei ist allerdings genauestens darauf zu achten, dass diese nicht im Widerspruch zueinander stehen.

c. Qualitätsstandards durch Service-Level-Agreements (SLA)

Neben der Festlegung des Leistungsumfangs muss noch dessen Qualität und Quantität bestimmt werden. Üblicherweise erfolgt die Festlegung im Rahmen sog. Service-Level-Agreements (SLA). Im Unterschied zur oben erläuterten Leistungsbeschreibung ist für ein SLA charakteristisch, dass der MSP jede (zuvor vereinbarte) relevante Leistung unaufgefordert in unterschiedlichen Gütestufen (Levels) anbietet, aus denen der Kunde unter ökonomischen Aspekten auswählen kann.

In jedem Fall sollten die maximalen Ausfallzeiten und die Verfügbarkeit klar definiert werden. Die hohe Systemverfügbarkeit und geringe Ausfallzeiten stellen für den Kunden eine der wohl wichtigsten Kriterien für die Qualitätsmessung dar. Von daher empfiehlt es sich, die minimale Verfügbarkeit bzw. maximaler Ausfallzeit entweder durch festgelegte Zeiten oder prozentuale Angaben innerhalb einer vordefinierten Zeitspanne zu bestimmen.

Neben den Ausfall- und Verfügbarkeitszeiten sollte der MSP klarstellen, in welcher Gütestufe er Support leisten wird. Der Kundensupport wird in der IT regelmäßig in sog. Support-Levels, angefangen vom First- bis zum Third-Level Support untergliedert. Der Kunde muss beim Vertragsschluss genau wissen, für welche Support-Level der MSP und der Hersteller zuständig sind. Das was für den MSP selbstverständlich erscheint, ist dem Kunden oft nicht klar.

Beispiel: Der Kunde lagert sein vollständiges IT-Sicherheitsmanagement an den MSP aus. Es kommt zu Kompatibilitätsproblemen aufgrund eines komplexen Programmes, das der Sicherheitssoftware unbekannt ist, weil dieses ausschließlich für die Bedürfnisse des Kunden entwickelt wurde. Nachdem sich der Kunde an den MSP wendet, wird die Ursache des Problems schnell bekannt. Das Problem ist behebbar, benötigt jedoch Expertise, die dem Third-Level Support einzuordnen ist. Der Kunde wendet sich erwartungsvoll an den MSP. Der MSP verweist jedoch auf das SLA, wonach er lediglich für den First-Level Support zuständig sei. Für den Second- und Third-Level Support sei der Hersteller zuständig.

Dieses Beispiel taucht in der Praxis relativ häufig auf und zeigt, dass der Kunde lediglich den MSP als Ansprechpartner wahrnimmt. Er vertraut darauf, dass er das „Rund-um-Sorglos Paket" nach dem Prinzip „alles aus einer Hand" erworben hat. Allerdings können bestimmte Probleme nur vom Hersteller gelöst werden. Dieser Aspekt sollte mit dem Kunden offen und transparent kommuniziert werden. Andernfalls gefährdet der MSP nicht nur die Kundenbeziehung, sondern muss sich gegebenenfalls Zurückbehaltungsrechte der Vergütung auseinandersetzen. Diese Auseinandersetzung ist ärgerlich, da die Einwände des Kunden – unabhängig davon, ob sie zutreffen oder nicht – in jedem Fall die Zahlung verzögern und deren Entkräftung unnötig mit Arbeit verbunden ist.

d. Mitwirkungspflichten

Bestimmte Leistungen des MSP setzen eine sog. Mitwirkungspflicht des Kunden voraus. Der MSP kann oftmals seine Leistungen nur erbringen, wenn der Kunde bestimmte Handlungen vornimmt oder Handlungen des MSP duldet.

Beispiel: Der Kunde hat sein IT-Sicherheitsmanagement bereits vor Jahren an den MSP ausgelagert. Das System läuft zuverlässig. Der Kunde ist mit der vom MSP installierten Sicherheitslösung hochzufrieden. Allerdings wird die im Kundenbetrieb eingesetzte IT-Sicherheitssoftware – wie vom Hersteller beabsichtigt und rechtzeitig angekündigt – in absehbarer Zeit das Produktlebensende erreichen. Das Produkt wird nach Ablauf dieser Frist vom Hersteller nicht mehr unterstützt, sodass ein weiterhin zuverlässiger Schutz nicht mehr gewährleistet werden kann. Der MSP möchte mit dem Kunden einen Termin zwecks Installation der neueren Produktversion vereinbaren. Er teilt dem Kunden auch mit, er müsse im Hinblick unvorhergesehener Probleme eine umfangreiche Datensicherung vornehmen. Der Kunde sieht jedoch keinen Anlass, auf eine höhere Produktversion umzustellen. Er lehnt die Terminvereinbarung mit der Begründung ab, dass er und seine Mitarbeiter mit dem Produkt zufrieden seien und sich alle an die „alte" Produktversion gewöhnt haben. Im Übrigen sei eine

umfassende Datensicherung viel zu aufwendig. Jedenfalls will er dem MSP den Zutritt zu den Räumlichkeiten zwecks Produktaktualisierung nicht gewähren.

Wie das Fallbeispiel veranschaulicht, ist bereits im Vorfeld zu klären, was der Kunde seinerseits tun oder dulden muss, damit der MSP seine Leistung überhaupt erbringen kann. Es empfiehlt sich daher, die Mitwirkungspflicht als Bedingung für die Leistungspflicht des MSP zu vereinbaren. Der soeben dargestellte Konflikt ließe sich einfach verhindern, indem die Leistungspflicht unter der Bedingung gestellt wird, dass der Kunde im Fall notwendiger Produktaktualisierungen, seine Daten sichert und den Zugriff zu den Räumlichkeiten gewährt.

Die Mitwirkungspflicht kann je nach Leistungsparameter, bereits in einer Meldepflicht bestimmter Ereignisse (z. B. Missbrauch von Zugangsdaten) bestehen, die erst dann eine Leistungspflicht des MSP begründen (z. B. Sperrung des betroffenen Kontos). Die Beispiele für das Festlegen von Mitwirkungspflichten des Kunden sind so zahlreich, dass die vollständige Aufzählung sämtlicher Fallkonstellationen den Rahmen dieser Darstellung sprengen würde. Der MSP muss sich im Vorfeld darüber Gedanken im Klaren sein, welche Handlung oder Duldung seitens des Kunden erforderlich ist, um die Leistung erbringen zu können.

Bei der Ausgestaltung von Mitwirkungspflichten müssen jedoch auch die Kundeninteressen berücksichtigt werden. Dies gilt insbesondere bei der Verwendung Allgemeiner Geschäftsbedingungen. Die Mitwirkungspflichten dürfen nicht so ausgestaltet sein, dass der Kunde ad hoc sämtliche unternehmensinterne Geschäftsprozesse stehen und liegen lassen muss. Es empfiehlt sich daher die Mitwirkungspflichten so zu gestalten, dass dem Kunden auch die Möglichkeit besteht, die notwendigen Vorkehrungen zu treffen um den Geschäftsbetrieb und die Mitwirkungspflicht in Einklang zu bringen. Möglich ist etwa eine vorherige Ankündigung der geplanten Maßnahme mit einer ausreichenden Karenzzeit. Keinesfalls sollten umfangreiche Maßnahmen, die den Geschäftsbetrieb beeinträchtigen können zur Unzeit erfolgen. Ratsam ist auch die Differenzierung der Mitwirkungspflichten zwischen routinemäßigen bis hin zu kritischen Ereignissen (Ampelsystem). Bei besonders kritischen Ereignissen (z. B. akuter Malwarebefall) wird der Kunde Einschränkungen im Geschäftsbetrieb eher hinnehmen müssen, als lediglich bei routinemäßigen Wartungsarbeiten.

Die Vereinbarung der Leistungspflicht unter der Bedingung, dass der Kunde seiner Mitwirkungspflicht nachkommt, hat zugleich den Vorteil, dass der MSP von seiner Leistungspflicht befreit wird, falls der Kunde seiner Mitwirkungspflicht nicht nachkommt. Die Klarstellung der Mitwirkungspflicht hat auch den Vorteil der Haftungserleichterung. Denn es wäre widersinnig den MSP für einen Schadenseintritt aufgrund nicht erbrachter Leistung in Anspruch zu nehmen, obwohl der Kunde selbst dafür verantwortlich ist.

e. Verantwortlichkeiten

Neben den einzelnen Mitwirkungspflichten ist an die Zuweisung der Verantwortlichkeiten zu denken. Die Auslagerung der IT-Sicherheitsmaßnahmen an den MSP entbindet dem Kunden nicht vor jeglicher Verantwortung. Anders als Mitwirkungspflichten, die vorrangig den Zweck haben, die Leistung des MSP überhaupt erst zu ermöglichen, handelt es sich bei der zugewiesenen Verantwortung um eine Pflicht, die originär schon immer dem Kunden oblag und auch nach Auslagerung der IT-Sicherheit beim Kunden verbleibt.

Wie das nächste (zugegeben drastische, wenn auch praxisnahe) Fallbeispiel zeigt, ist das beste Sicherheitskonzept wertlos, wenn der Schlüsselinhaber des verschlossenen Safes seine Schlüssel offen und für jedermann zugänglich aufbewahrt.

Beispiel: Der Kunde, der auch diesmal sein IT-Sicherheits-management ausgelagert hat, verfügt nunmehr dank dem Sicherheitskonzept des MSP über umfangreiche Schutzmechanismen. Neben dem Schutz vor digitalen Bedrohungen, wie Malware und Hackern sind auch relevante Daten, insbesondere auf den Notebooks der Außendienstmitarbeiter verschlüsselt. Ein Mitarbeiter aus dem Außendienst fährt mit dem Zug. Während der Fahrt bearbeitet er Kundenaufträge. Auf dem Notebook befinden sich sensible unternehmensinterne Daten. Die Festplatte ist verschlüsselt. Da sich der Mitarbeiter jedoch Passwörter sehr schlecht merken kann, befindet sich das Passwort zur Festplattenentschlüsselung auf einem Zettel, der auf der Innenseite des Notebooks angebracht ist. Dieses Passwort nutzt er zudem gleichzeitig für andere Dienste, die im Zusammenhang mit seinem Arbeitsverhältnis stehen. Als er versunken in seiner Arbeit mitbekommt, dass er sein Reiseziel erreicht hat, vergisst er im Eifer des Gefechts das Notebook. Dieses wird von einem Fahrgast gefunden, der daraufhin die Daten ausliest.

Es leuchtet ein, dass jedes Sicherheitskonzept spätestens beim vor dem Bildschirm sitzenden Anwender seine Grenzen findet. Der MSP kann auf das Benutzerverhalten überhaupt keinen Einfluss ausüben. Auch wenn dies logisch erscheint, sollte die Zuweisung der Verantwortungen für das Aufrechterhalten des Sicherheitskonzepts vertraglich geregelt werden. Mit der Zuweisung der Verantwortung erfüllt der MSP häufig, aber nicht zwingend die Aufklärungspflicht gegenüber seinem Kunden. Der Kunde sollte mit dem Sicherheitskonzept vertraut gemacht werden. Ihm muss klar sein, was die einzelnen Schutzkomponenten bewirken und welche Folgen die unsachgemäße Verwendung und das unsachgemäße Verwahren von Zugangsdaten haben können.

Auch hier trägt die klare Zuweisung der Verantwortung maßgeblich zur Senkung des Haftungsrisikos bei. Für den Schadensfall aufgrund eines Handelns, das in den Verantwortungsbereich des Kunden fällt, kann der MSP grundsätzlich nicht in Anspruch genommen werden. Es fehlt am sog. Verschulden.

Bei dem Kunden stellt sich die Frage, wie seinem Verantwortungsbereich Herr werden kann. Diese Frage muss am Ende durch den Kunden selbst beantwortet werden. Denn nur der Kunde kann den notwendigen direkten Einfluss auf die Organisation und das Verhalten seiner Mitarbeiter nehmen. Diese Tatsache kann dem MSP jedoch neue Geschäftsfelder eröffnen. Denkbar wäre das Anbieten optionaler Leistungen, etwa Schulungen der Mitarbeiter des Kunden, um den Kunden bei der Erfüllung seiner Pflichten zu unterstützen. Eine solche Schulung kann in einer Leistungsvereinbarung aufgenommen werden, die der MSP separat abrechnet.

2. Leistungsstörungen

Unabhängig wie gut die Leistungsbeschreibung und die SLA formuliert sind, kommt es dennoch vor, dass der Kunde mit der Leistung nicht zufrieden ist, weil tatsächlich etwas bei der Leistungserbringung schiefgegangen ist. Der Kunde wird bei einer mangelbehafteten Leistung regelmäßig Einwendungen geltend machen.

Welche Einwendungen geltend gemacht werden können, hängt dabei vom Vertragstyp ab. Wie bereits eingangs erwähnt, handelt es sich bei MSP-Verträgen typischerweise um sog. Mischverträge. Das bedeutet, dass Teile davon beispielsweise dem Dienst-, Kauf-, Miet- oder Werkvertrag zuzuordnen sind. Diese Zuordnung ist in der Praxis schwierig, dennoch unumgänglich. Denn je nach Vertragstyp kommen unterschiedliche Einwendungen mit jeweils unterschiedlichen Voraussetzungen in Betracht. Dieser Zustand ist von keinem der beiden Parteien gewünscht, weil er zur Rechtsunsicherheit auf beiden Seiten führt. Der Kunde wird sich nicht sicher sein, ob er seinen Einwand geltend machen kann. Dem MSP hingegen fehlt die Gewissheit, ob der Kunde nicht doch im Recht ist. Problematisch ist auch die Geltendmachung von Schadensersatzansprüchen, da nach den allgemeinen Regeln der Beweislast grundsätzlich der Geschädigte das Verschulden des Schädigers und den Schaden darlegen und beweisen muss.

Dieses Dilemma lässt am einfachsten lösen, indem die gesetzlichen Gewährleistungsrechte, soweit dies zulässig ist, vertraglich ausgeschlossen und durch eigene Sanktionsinstrumente ersetzt werden.

a. Sanktionsmöglichkeiten bei Vertragsverletzungen

Sanktionsvereinbarung erscheinen für den MSP auf den ersten Blick nachteilig. Allerdings ist zu bedenken, dass die Rechtssicherheit auch dem MSP zugutekommt. Schließlich ist auch er an einer raschen Klärung interessiert. Im Übrigen wird dem Kunden der Eindruck von Seriosität vermittelt. Das schafft Vertrauen. Angesichts des hart umkämpften Wettbewerbsumfeldes wird sich kaum ein Kunde auf einen Vertrag einlassen, bei dem nahezu sämtliche seiner Rechte ausgeschlossen werden.

Sinnvoll ist die Vereinbarung einer Vergütungsminderung, Vertragsstrafe, eines pauschalisierten Schadensersatzanspruches und des Rechts auf außerordentliche Kündigung. Diese Regelungen werden im Hauptvertrag oder direkt im SLA festgelegt.

(1) Minderung der Vergütung
Eine sehr unkomplizierte Regelung der Fälle bei denen das Service-Level nicht erreicht wird, stellt die Minderung dar. Die Minderung ist tendenziell kundenfreundlich, weil sie aufgrund der Transparenz einfach zu handhaben ist. Die Handhabung der Minderung hängt jedoch maßgeblich von der Ausgestaltung des SLA's ab. Häufig erfolgt die Minderung gestaffelt, sodass ab einem bestimmten nicht erreichten Service-Level eine Pauschale von der Vergütung einbehalten wird.

Für den Fall, dass der MSP eine garantierte Mindestvergütung einbehalten will, empfiehlt sich die Vereinbarung einer prozentualen Begrenzung oder eines Höchstbetrages.

Bei der Vereinbarung einer Minderung als Sanktionsmöglichkeit sollte der MSP jedoch bedenken, dass etwaige Schadensersatzansprüche mit der Minderung nicht abgegolten und gegebenenfalls neben der Minderung geltend gemacht werden.

> Die Vereinbarung einer pauschalen Minderung im Rahmen Allgemeiner Geschäftsbedingungen ist sehr fehleranfällig, wenn sie im Zusammenhang mit einer Leistung des MSP steht, die als Dienstleistung zu qualifizieren ist. In diesem Fall sollte eine derartige Vereinbarung keinesfalls ohne rechtskundige Unterstützung vereinbart werden. Verstößt die Regelung gegen die §§ 305 ff. BGB, muss die Unwirksamkeit der Klausel in Kauf genommen werden.

(2) Vertragsstrafe
Wenn der Kunde ein Schadensfall erleidet, dass auf den MSP zurückzuführen ist, muss dieser grundsätzlich nach den Grundsätzen der vertraglichen und unerlaubten Handlung Schadensersatz leisten. Diese Regel gilt im Zivilrecht allgemein und spiegelt die Ausgangslage im Gesetz wieder. Der Geschädigte muss jedoch den Eintritt eines Schadens beweisen. Dass dem Kunden dies nicht immer gelingt, zeigt das nachfolgende Fallbeispiel.

Beispiel: Bei einem Kunden, der sein IT-Sicherheitsmanagement an einen MSP ausgelagert hat, sollen Wartungsarbeiten stattfinden. Der Kunde betreibt ein Dolmetscher- und Übersetzungsbüro. Neue Aufträge werden überwiegend telefonisch – über eine computergesteuerte VoIP-Anlage – entgegengenommen. Der Kunde muss die Telefonate sofort entgegennehmen, da andernfalls die Aufträge an Mitbewerber vergeben werden. Aufgrund einer fahrlässigen Unachtsamkeit des MSP-Mitarbeiters fallen die Systeme aus. Betroffen sind auch die VoIP-Anlagen. Erst nach einigen Stunden funktionieren die Telefone wieder ordnungsgemäß. Im Nachhinein kann nicht festgestellt werden, ob überhaupt und wenn ja, wie viele neue Aufträge in dieser Zeit nicht entgegengenommen werden konnten.

Häufig weiß nicht einmal der Kunde selbst, ob ein Schaden aufgrund des SLA Verstoßes eingetreten ist. Viele Kunden sind sich dieses Risikos bei der IT-Auslagerung auch bewusst. Um das Vertrauen des Kunden zu gewinnen und den Vertragsabschluss attraktiver zu gestalten, kann die Vereinbarung einer Vertragsstrafe im Sinne der §§ 339 ff. BGB zuungunsten des MSP sinnvoll sein. In diesem Fall muss der Kunde lediglich den schuldhaften Verstoß gegen das SLA, nicht jedoch den Schadenseintritt beweisen.

Der MSP sollte jedoch bedenken, dass der Kunde im Falle eines Schadensfalles, den der Kunde auch beweisen kann, neben der Vertragsstrafe zusätzlich Schadensersatz leisten muss. Allerdings kann der Kunde im Schadensfall grundsätzlich nicht zweimal kassieren. Die Vertragsstrafe wird auf den Schadensersatzbetrag angerechnet, sofern vertraglich nicht etwas anderes vereinbart wurde.

(3) Pauschalierter Schadensersatz
Sofern der MSP eine Vertragsstrafe zu seinen Ungunsten nicht vereinbaren, aber dem Kunden dennoch entgegenkommen möchte, kommt als anbieterfreundlichere Alternative der sog. pauschalierte Schadenersatz in Betracht. Normalerweise muss der Kunde nicht nur den Schaden, sondern auch die Schadenshöhe auf den Cent genau beziffern.

Beispiel: Bei einem Kunden, der sein IT-Sicherheits-management an einen MSP ausgelagert hat, sollen geringfügige Wartungsarbeiten stattfinden. Als der Kunde den Mitarbeiter des MSP fragt, ob eine vorherige Datensicherung notwendig ist, erwidert dieser lediglich, es handele sich lediglich um routinemäßige Wartungsarbeiten und dass eine Sicherung nicht notwendig sei. Aufgrund einer fahrlässigen Unachtsamkeit werden sämtliche Kundendaten, nebst Aufträgen gelöscht. Zahlreiche Aufträge können nicht mehr abgewickelt und müssen storniert werden. Seit dem Vorfall gehen die Aufträge nachweislich zurück.

In diesem Fall hat sich der MSP gegenüber seinem Kunden schadensersatzpflichtig gemacht. Das Beispiel zeigt, dass die Bezifferung des Schadensersatzanspruches bei Schadensvorfällen am System regelmäßig schwierig bis unmöglich ist. Bei einem vereinbarten pauschalierten Schadensersatzanspruch muss der Kunde lediglich den Schaden beweisen. Ein Nachweis der Schadenshöhe ist nicht erforderlich.

Der MSP hat den Vorteil, dass er nicht mehr zahlen muss, als pauschal vereinbart wurde. Die Haftungshöchstsummen können auf bestimmte, Ereignisse, Zeiträume, Wiederholungen bezogen und auch miteinander kombiniert werden. Von elementarer Bedeutung ist dabei die genaue Beschreibung des Schadensereignisses.

Ein pauschalierter Schadensersatz bietet somit einen interessengerechten Kompromiss für beide Parteien.

> Auch hier zeigen sich die Tücken bei der Verwendung Allgemeiner Geschäftsbedingungen. Diese betreffen allerdings den Fall, dass die AGB vom Kunden und nicht vom MSP gestellt werden. Eine Schadenspauschale ist unwirksam, wenn sie den nach dem gewöhnlichen Verlauf der Dinge den zu erwartenden Schaden übersteigt.
>
> Beispiel: Die Pauschale für den Ausfall der VoIP-Telefonanlagen beträgt je Stunde 10.000 EUR. Innerhalb einer Stunde ist jedoch lediglich ein Auftragsvolumen von 100 EUR zu erwarten.
>
> Der Kunde kann vom MSP nicht die Pauschale in Höhe von 10.000 EUR geltend machen. Im Übrigen muss es dem MSP gestattet bleiben, den Nachweis des Eintritts eines geringeren Schadens, als in der Pauschale vorgesehen, führen zu dürfen.

(4) Bonus-Malus-Regelungen

In einigen Fällen kann es für beide Parteien sinnvoll sein, die bereits erörterte pauschale Minderung mit einer Erhöhung zu kombinieren: Für den Fall, dass der MSP die im SLA vereinbarten Anforderungen unterschreitet, verbleibt es soweit bei einer (gestaffelten) Minderung. Sofern der MSP jedoch die Anforderungen aus dem SLA überschreitet, wird ein (ebenfalls gestaffelter) Zuschlag fällig.

Die Bonus-Malus-Regelung eignet sich besonders für die Fälle, bei denen der Kunde ein Interesse an auch dem SLA übersteigenden Leistungen hat und das SLA lediglich zur Sicherung eines Mindestqualitätsstandards dienen soll. Der MSP wird dadurch zur besonders hochwertigen Arbeit motiviert.

> Hinsichtlich der Vereinbarung einer pauschalierten Minderung durch den Kunden im Rahmen Allgemeiner Geschäftsbedingungen, die als Leistung einem Dienstvertrag einzuordnen sind, kann auf die Ausführungen zur Minderung der Vergütung verwiesen werden.

(5) Außerordentliche (fristlose) Kündigung

Es gibt auch Fälle, bei denen die Geschäftsbeziehung durch Vorkommnisse geprägt ist, die das Festhalten am Vertrag unzumutbar erscheinen lässt. In diesen Fällen bleibt der Vertragspartei nichts Anderes übrig, als den Vertrag zu beenden. Das wichtigste Instrument zur sofortigen Beendigung dieser Vertragsbeziehung stellt die Kündigung dar.

Die außerordentliche Kündigung (auch als fristlose Kündigung bekannt) ist in den §§ 626, 314 BGB geregelt. Sie ist das schärfste Schwert, um Konflikte in der Beziehung zwischen MSP und Kunde zu beenden. Sie kommt nur bei Extremfällen in Betracht, bei denen die Geschäftsbeziehung wegen eines schwerwiegenden Vorfalls oder mehrerer wiederholter schädigender Ereignisse irreparabel zerrüttet ist.

Als kündigungsbegründendes Ereignis kommt grundsätzlich jede Art schwerer Pflichtverletzung in Betracht, sodass sie – je nachdem wer die Pflichtverletzung begangen hat – von beiden Seiten ausgesprochen werden kann.

Beispiel: Das SLA eines MSP, der mit dem IT-Sicherheitsmanagement eines Kunden betraut ist, sieht das regelmäßige Anfertigen von Datensicherungskopien vor. Der Kunde betreibt ein Inkassounternehmen. Als der Mitarbeiter des MSP die turnusgemäße Datensicherung vornimmt, entdeckt er zufällig eine Datei, die eine einzutreibende Forderung seines Nachbarn betrifft. Im Geiste der guten Nachbarschaft löscht er diese Datei, damit der Nachbar nicht mehr vom Kunden belästigt wird.

Das Recht zur außerordentlichen Kündigung ist im Gesetz, namentlich in den §§ 626, 314 BGB geregelt. Es muss dementsprechend nicht zwingend im Vertrag vereinbart werden. Dennoch sollten die relevanten Fälle, die zur außerordentlichen Kündigung berechtigen sollen, im Vorfeld festgelegt werden. Der Grund hierfür liegt im Wortlaut des § 314 BGB. Dieser erlaubt nämlich die außerordentliche Kündigung nur, wenn ein „wichtiger Grund" vorliegt. Hierbei handelt es sich um einen sog. unbestimmten Rechtsbegriff. Das bedeutet, es bedarf stets der Prüfung, ob ein wichtiger Grund vorliegt. Hierbei sind sämtliche Umstände des Einzelfalles zu berücksichtigen. Das sorgt für Streitstoff, da es insoweit auf die Argumentation der Vertragsparteien ankommt und die Frage, ob ein wichtiger Grund vorliegt, im Zweifel gerichtlich entschieden werden muss.

Die Kündigung ist ein einseitiges Rechtsgeschäft bestehend aus einer empfangsbedürftigen Willenserklärung. Das bedeutet, dass eine bereits ausgesprochene Kündigung nicht mehr zurückgenommen werden kann. Deshalb sollte sich der Kündigungsberechtigte sorgfältig überlegen, ob er den Vertrag wirklich kündigen will, da er den Vertrag ohne Zustimmung des Gekündigten nicht wieder „auferstehen" lassen kann. In diesem Zusammenhang kann auch die Vereinbarung der Möglichkeit einer Teilkündigung, etwa einzelner SLA's sinnvoll sein.

b. Ausschluss von Gewährleistungsrechten

Sofern sich MSP und Kunde auf eine oder mehrere Sanktionsformen geeinigt haben, kann der weitgehende Ausschluss gesetzlicher Gewährleistungsrechte sinnvoll sein. Schließlich sollen die vertraglichen Sanktionsformen das gesetzliche Gewährleistungsrecht – soweit dies zulässig ist – ersetzen. Andernfalls riskiert der MSP, dass er aufgrund der vertraglichen Sanktionen und aus den gesetzlichen Gewährleistungsansprüchen in Anspruch genommen wird.

Aufgrund des Grundsatzes der Vertragsfreiheit können Gewährleistungsrechte modifiziert werden. Die Frage inwieweit diese ausgeschlossen werden können, hängt davon ab, ob der Gewährleistungsausschluss mit dem Vertragspartner individuell (sog. Individualabrede) oder durch Formularvertrag (Allgemeine Geschäftsbedingung) ausgehandelt wird.

(1) Ausschluss durch Individualabrede

Der Ausschluss der Gewährleistungsansprüche des Kunden ist nahezu vollständig möglich, wenn der MSP den Ausschluss (nicht notwendigerweise den gesamten Vertrag!) individuell aushandelt. In diesem Fall begegnen sich Kunde und MSP auf Augenhöhe. Aufgrund seiner faktischen Möglichkeit, Einfluss auf dem Vertrag nehmen zu können, ist er weniger schutzwürdig. Er ist quasi seines Glückes eigener Schmied. Auch finden im B2B Geschäft keine verbraucherschützenden Vorschriften Anwendung. Der Ausschluss der Gewährleistung wird lediglich durch die allgemeinen Verbote, wie Sitten-, Treuwidrigkeit, arglistige Täuschung, Drohung und den Verstoß gegen gesetzliche Verbote begrenzt. Auch kann die Haftung und Gewährleistung für Vorsatz (d. h. Schädigung mit Wissen und Wollen) nicht ausgeschlossen werden.

Inwieweit es sinnvoll ist die Gewährleistungsansprüche auszuschließen, ohne den Kunden vom Vertragsabschluss abzuschrecken, ist eine Frage der Kalkulation und muss aus betriebswirtschaftlichen Gesichtspunkten entschieden werden.

(2) Ausschluss durch AGB

Aufwändiger ist der Ausschluss durch Allgemeine Geschäftsbedingungen. Im Gegensatz zur Individualabrede hat der Kunde, der die AGB vom MSP vorgesetzt bekommt, deutlich geringeren Einfluss auf den Vertragsinhalt. Insoweit erachtet der Gesetzgeber den Kunden als besonders schutzwürdig unabhängig davon, dass es sich um ein B2B Geschäft handelt.

> Zu beachten ist die Anfälligkeit von Klauseln, welche die Einschränkung von Gewährleistungsrechten bezwecken. Der Verwender (i. d. R. der MSP) sollte die formularmäßige Einschränkung, bei denen der Kunde „nur noch unterschreiben muss" keinesfalls ohne rechtskundige Unterstützung vereinbaren.
> Wie schon zuvor erwähnt ist das AGB-Recht sehr komplex und erfordert die Kenntnis aktueller Rechtsprechung. Klauseln, die den Kunden bei der Ausübung von Gewährleistungsrechten unangemessen benachteiligen, sind unwirksam und haben zur Folge, dass anstelle der unwirksamen Klausel, die sehr weitrechenden gesetzlichen Gewährleistungsrechte Anwendung finden.

c. Haftungsfragen

Neben den Fragen des Gewährleistungsrechts ist die Haftung auf Schadensersatz des MSP gegenüber dem Kunden zu klären. Im deutschen Zivilrecht sind Schadensersatzansprüche grundsätzlich nach dem folgenden Prinzip aufgebaut:

Voraussetzung	Fallbeispiel
1. Rechtsgutverletzung des Geschädigten	Der Kunde schließt mit dem MSP einen Vertrag mit einem Auftragsvolumen i.H.v. 50.000 EUR ab. Im Kundenbetrieb wird während der üblichen Wartungsarbeiten das System beschädigt und kann erst wieder nach einer Woche in Betrieb genommen werden.
2. Pflichtverletzung des Schädigers	Die Beschädigung des Systems stellt eine Verletzung leistungsbezogener Pflichten aus dem MSP-Vertrag dar. Die Wartungsarbeiten dienen gerade dazu, die Funktionsfähigkeit des Systems aufrechtzuerhalten.
3. Verschulden des Schädigers (es gibt jedoch wenige Haftungsvorschriften, bei denen das Verschulden nicht vorausgesetzt wird, etwa dem Produkthaftungs-gesetz)	Die Beschädigung des Systems erfolgte aufgrund einer leichten Unachtsamkeit und somit fahrlässig.
4. Eintritt eines Schadens.	Dem Kunden ist aufgrund des Systemausfalls ein Schaden von 2.500.000 EUR entstanden.

Wie das vereinfachte Beispiel veranschaulicht, unterwirft sich der MSP unkalkulierbaren Haftungsrisiken. Der gesetzliche Haftungsmaßstab aus § 276 Abs. 1 BGB sieht die Haftung des Schädigers für Vorsatz und Fahrlässigkeit vor. Fahrlässig handelt nach § 276 Abs. 2 BGB derjenige, der die erforderliche Sorgfalt außer Acht lässt. Dies gilt selbst für leichte Fahrlässigkeit aufgrund Augenblicksversagens. Diesbezüglich kennt das Zivilrecht also keine Gnade.

Angesichts des im Vergleich zur Schadenshöhe geringen Auftragsvolumens empfiehlt es sich, die Haftung zu modifizieren. Dies ist gesetzlich auch zulässig. Eine mögliche Form der Haftungsbegrenzung ist das zuvor erörterte Instrument der Pauschalierung des Schadenersatzanspruches auf eine Höchstsumme.

Einzelvertraglich kann auch die vollständige Haftung wegen Fahrlässigkeit ausgeschlossen werden. Von dieser Möglichkeit sollte jedoch nur dosiert Gebrauch gemacht werden, da sich der Kunde bei einer nahezu vollumfänglichen Haftungsbefreiung wohl kaum auf ein Outsourcing-Projekt einlassen wird.

> Bei dem Haftungsausschluss im Rahmen Allgemeiner Geschäftsbedingungen, also Formularverträgen muss beachtet werden, dass die Haftung nur wegen leichter und mittlerer Fahrlässigkeit ausgeschlossen werden kann. Der Haftungsausschluss bei grober Fahrlässigkeit und Vorsatz ist unzulässig. Grobe Fahrlässigkeit liegt vor, wenn die Sorgfalt außer Acht gelassen wurde, die jedem (also auch einer nicht IT bewanderten Person) hätte einleuchten müssen.

Unabhängig der Beschränkung des Schadensersatzes auf bestimmte Verschuldensformen, kann und sollte der MSP sog. Folgeschäden ausschließen. Andernfalls droht eine uferlose Ausweitung der Haftung.

Sofern zum Leistungsspektrum des MSP nicht die Datensicherung gehört und diese durch den Kunden in Eigenregie selbst vorgenommen wird, empfiehlt sich ferner die Haftungsbeschränkung auf die letzte Dateisicherungskopie, um auch hier der uferlosen Ausweitung der Haftung entgegenzutreten.

IV. Datenschutz

Regelmäßig kommt der MSP bei der Erfüllung seiner Leistungspflicht mit Daten des Kunden in Berührung, die oftmals sensiblen Charakter haben. Von daher muss die Vertragsbeziehung zwischen den Parteien datenschutzkonform ausgestaltet werden. Neben Geschäftsgeheimnissen müssen auch sog. personenbezogene Daten hinreichend geschützt werden. Personenbezogene Daten sind nach § 3 BDSG Daten, die einer Person zugeordnet werden können und etwas über diese Person aussagen. Betroffen sind vor allem Daten über die Mitarbeiter im Kundenbetrieb und sonstige Kundendaten. Die Anforderungen an den Schutz personenbezogener Daten werden primär durch das Bundesdatenschutzgesetz (BDSG) normiert. Keine personenbezogenen Daten liegen vor, wenn die Daten soweit anonymisiert werden, dass diese keine Rückschlüsse auf die betroffene Person ermöglicht. In diesem Fall findet das BDSG keine Anwendung.

1. Allgemeines zum Datenschutz

Im Vertrag zwischen MSP und dem Kunden sollte in jedem Fall eine Vereinbarung aufgenommen werden, die den MSP verpflichtet seine Mitarbeiter zur Verschwiegenheit zu verpflichten. Diese Pflicht trifft dem MSP im Hinblick auf § 5 BDSG ohnehin. Um dieser Anforderung gerecht zu werden, sollte der MSP seine Mitarbeiter belehren, dass es ihnen untersagt ist geschützte personenbezogene Daten zu einem anderen Zweck als deren Aufgabenerfüllung im Rahmen des Arbeitsverhältnisses zu erheben, verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Es empfiehlt sich die Mitarbeiter auch im Vorfeld über mögliche Sanktionen, insbesondere der Kündigung und einer möglichen Strafbarkeit nach § 44 BDSG zu belehren.

Das Verbot, personenbezogene Daten zu einem anderen Zweck, als der Aufgabenerfüllung zu erheben, verarbeiten oder sonst zu nutzen, gilt selbstverständlich auch für den MSP gegenüber dem Kunden selbst. Aus diesem Grund sind nach Beendigung des Auftrages sämtliche Daten zurückzugeben bzw. zu löschen, sobald sie nicht mehr für die Ausführung des Auftrages benötigt werden.

Schließlich stellt sich – allerdings primär für den Kunden – die Frage, ob er personenbezogene Daten in die „fremden Hände" des MSP geben darf. Die Anforderungen an die Zulässigkeit der Überlassung personenbezogener Daten an den MSP hängt davon ab, ob lediglich eine Auftragsdatenverarbeitung oder eine Funktionsübertragung vorliegt.

2. Auftragsdatenverarbeitung

Weniger problematisch ist der Fall, dass der MSP im Auftrag des Kunden personenbezogene Daten verarbeitet. Eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG liegt vor, wenn der Kunde trotz Datenauslagerung „Herr der Daten" bleibt. Der MSP verarbeitet zwar die Daten, dennoch ist er nur der Gehilfe des Kunden. In einem solchen Fall fungiert der MSP lediglich als verlängerter Arm des Kunden. Es findet keine echte Datenübermittlung im Sinne des BDSG statt.

Beispiele hierfür sind

- Wartungsdienstleistungen des MSP, sofern die Möglichkeit besteht, dass der MSP Kenntnis von den personenbezogenen Daten erlangt,
- die Auslagerung der Daten in ein externes Rechenzentrum (also in die Cloud),
- die Vernichtung von Daten durch ein externes Unternehmen.

Der MSP kann also in der Regel davon ausgehen, dass in dem Outsourcing-Projekt immer eine Auftragsdatenverarbeitung vorliegt, da nie ausgeschlossen werden kann, dass er mit Kundendaten in Berührung kommt. Der Fall der Auftragsdatenverarbeitung ist datenschutzrechtlich im Vergleich zur Funktionsübertragung weitgehend unproblematisch, weil der Kunde für die Datenverarbeitung nach wie vor verantwortlich bleibt und der MSP lediglich nur Weisungen des Kunden befolgt. Da keine Datenübermittlung im Sinne des BDSG stattfindet, bedarf es keiner weitergehenden Legitimation durch die betroffene Person. Der Kunde muss lediglich den Auftragnehmer (also den MSP) sorgfältig auswählen und ihn schriftlich mit der Datenverarbeitung beauftragen. Nach dem 10 Punkte Katalog des § 11 Abs. 2 BDSG sind in dem Auftrag folgende Einzelheiten festzulegen:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die bestehenden Pflichten des MSP, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7. die Kontrollrechte des Kunden und die entsprechenden Duldungs- und Mitwirkungspflichten des MSP,
8. mitzuteilende Verstöße des MSP oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Kunde gegenüber dem MSP vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim MSP gespeicherter Daten nach Beendigung des Auftrags.

Die Vereinbarung einer Auftragsdatenverarbeitung ist zwingend notwendig, da eine Auftragsdatenverarbeitung ohne vorherigen Auftrag eine Ordnungswidrigkeit nach § 43 I Nr. 2 b) BDSG darstellt. Diese kann mit empfindlichen Bußgeldern geahndet werden. § 11 Abs. 2 BDSG enthält keine abschließende Aufzählung einzelner Festlegungen, sodass je nach Outsourcing-Projekt erforderlichenfalls weitere Inhalte zu vereinbaren sind.

3. Funktionsübertragung

Weitaus komplizierter ist der Fall, wenn eine Funktionsübertragung vorliegt. Denn im Gegensatz zur bloßen Auftragsdatenverarbeitung gibt der Kunde die Datenverarbeitung aus seiner Hand. Zwischen dem Kunden und dem MSP findet hier eine echte Datenübermittlung gemäß § 28 I 1 Nr. 2 BDSG statt. Im Zuge dieser Datenübermittlung fungiert der MSP nicht mehr bloß als verlängerter Arm, sondern übernimmt die „Herrschaft" über die Daten des Kunden.

Beispiele für die Funktionsübertragung finden sich auch außerhalb der reinen IT-Dienstleisterbranche, etwa

- Beauftragung eines externen Callcenterbetriebs mit der Befragung von Kunden zwecks Marktforschung,
- Beauftragung eines Rechtsanwalts, Steuerberaters oder Inkassodienstleisters,
- Verarbeitung von Patientendaten eines Krankenhauses durch eine spezielle Fachklinik.

Der MSP handelt im Gegensatz zur Auftragsverarbeitung frei von Weisungen und in Eigenverantwortung. Auch ist er für den Schutz, insbesondere die Sicherung der Daten verantwortlich. Der Kunde gewährt dem MSP Nutzungsrechte an den Daten, da der MSP ohne diese Nutzung das Ergebnis bzw. die Leistung (z. B. Steuererklärung, Auswertung von Patientendaten) nicht erbringen kann. Typischerweise tritt der MSP häufig im eigenen Namen gegenüber den betroffenen Personen auf.

Da nicht mehr der Kunde „Herr über die Daten" ist, bedarf es nach dem BDSG einer Rechtsgrundlage für die Datenübermittlung. Eine solche Rechtsgrundlage wird primär durch die Zustimmung der betroffenen Person geschaffen. Insgesamt gestaltet sich die Einholung der Zustimmung durch die betroffenen Personen in der Praxis als äußerst aufwendig und ist mit einer Vielzahl von Herausforderungen verbunden.

Die Funktionsübertragung kann auch durch ein berechtigtes Interesse des Kunden gerechtfertigt werden. Allerdings muss hier zwischen den berechtigten Interessen der Person und denen des Kunden sorgfältig abgewogen werden. Eine Funktionsübertragung, die sich nur auf die überwiegenden Interessen des Kunden stützt, birgt regelmäßig die Gefahr, dass aufgrund einer fehlerhaften Abwägung die Funktionsübertragung unzulässig ist.

Probleme entstehen auch dann, wenn der MSP vom Kunden die Erlaubnis erhält, die Daten an einen Subunternehmer des MSP zu übermitteln diese an Drittländer übertragen werden sollen, in denen datenschutzrechtliche Regelungen herrschen, die unter dem Niveau des BDSG liegen. Solche Datenübermittlungen sind sehr komplex und sollten nicht ohne rechtliche Beratung durchgeführt werden.

4. Zusammenfassung

Das MSP-Modell der IT-Sicherheit erfreut sich nicht zu Unrecht großer Beliebtheit. Der Kunde kann trotz knapper finanzieller und personeller Ressourcen auf die notwendige Expertise zurückgreifen um sich im Falle eines Schadenseintritts von der Haftung wegen unzureichender Absicherung der unternehmensinternen IT-Infrastruktur zu befreien. Dies setzt selbstverständlich voraus, dass es sich bei dem MSP um einen zuverlässigen Partner handelt, der über das notwendige Know-how verfügt. Ob eine teilweise oder vollständige Auslagerung sinnvoll ist, hängt dabei nach den betriebswirtschaftlichen Umständen des Einzelfalles ab.

Dem Anbieter eröffnet das MSP-Modell wiederkehrende und planbare Einnahmen und festigen die Beziehung zum Kunden.

Die Durchführung eines MSP-Projektes setzt selbstredend eine sorgfältige Planung voraus. In der Vertragsverhandlung sollten MSP und Kunde neben den Hauptleistungspflichten, auch festlegen, wie das Aktivitätsmonitoring des MSP zur Abnahmekontrolle der Leistung erfolgen soll. Der MSP sollte sich im

Vorfeld Gedanken machen über etwaige Sanktionen und Gewährleistungsansprüche für den Fall, dass die Leistung nicht wie vereinbart erbracht wird. Für besonderes Konfliktpotenzial sorgen Haftungsfragen, deren lückenhafte Regelung erst im Falle eines Schadensereignisses zu tragen kommen.

Der Grundsatz der Vertragsfreiheit erlaubt den Parteien im B2B-Geschäft, umfangreiche Regelungen und Abweichungen vom Gesetz vorzunehmen. Allerdings ist insbesondere bei Formularverträgen, also Allgemeinen Geschäftsbedingungen darauf zu achten, dass die Regelungsbefugnis im Vergleich zur einzelvertraglichen Vereinbarung stark eingeschränkt wird. Von daher ist dem MSP vor allem von der Verwendung vorgefertigter „Mustervereinbarungen", ohne vorherige Prüfung durch einen Rechtskundigen, dringend abzuraten.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2017-05 DE (NP)

SOPHOS