SOURCING | INTERNATIONAL
Digital Transformation Advisors

LEITFADEN

Cloud Computing

Auswahl und Einführung von Cloud Services – Prozesse und Organisation

04

INHALT

Impressum

Sourcing International

Palais Savoy, Johannesgasse 15
1010 Wien, Osterreich

E-Mail: office@sourcing-international.org
Web: www.sourcing-international.org

1 Vorwort

Liebe Leserinnen und Leser!

Die erste Ausgabe dieses Leitfadens wurde im April 2012 veröffentlicht, und mein Vorwort begann mit dem Satz: „Es gibt wenige IT-Themen, die so kontrovers diskutiert werden wie Cloud Computing." Vier Jahre später hat sich einiges geändert – manches blieb unverändert.

Noch immer sind wir weit von einem routinierten und standardisierten Umgang mit den Cloud-Herausforderungen entfernt – aber kontrovers ist die Diskussion nicht mehr. Die Diskussion ist auf die vielfältigen Herausforderungen fokussiert, aber dass Cloud ein Teil der digitalen industriellen Revolution ist, ein Milliardengeschäft, eine ***conditio sine qua non*** in den meisten Unternehmen, die IT nutzen – das bezweifelt niemand mehr.

Die im Vorwort 2012 genannten „Verlockungen und Herausforderungen" sind jedoch dieselben geblieben: Auf der einen Seite locken Einsparungen durch Konsolidierung, Standardisierung und Automatisierung der IT, die eine flexible Nutzung von IT-Services über Self-Service-Portale prognostiziert. Auf der anderen Seite stellen die Sicherheit, gesetzliche Vorgaben, problematische Servicelevel Agreements, Fragen der Schnittstellen und die komplexe Umsetzung die Herausforderungen dar.

Der Druck, sich mit der Modernisierung und Ökonomisierung von Unternehmens-IT zu beschäftigen, ist größer geworden und drängt Unternehmen dazu, sich mit dem Bezug von IT-Services aus der Cloud zu beschäftigen. Der hybride IT-Ansatz (interne IT, Outsourcing und Cloud Sourcing in Kombination) wird wohl weiterhin der meistgewählte Ansatz bleiben.

EuroCloud hat bereits viele Leitlinien und Guidelines veröffentlicht. Einige technische, viele rechtliche und eben auch solche zu Organisation und Prozessen. Nicht umsonst wird der Qualitätsrahmen StarAudit mittlerweile bereits in vielen Ländern der Welt für den Vergleich von Cloud Services, für Gap-Analysen, Ausschreibungen oder klare Qualitätszusagen benutzt. EuroCloud ist mittlerweile ein Standardplayer im Cloud-Qualitätsmanagement und in der Cloud-Zertifizierung geworden. Siehe dazu staraudit.org.

Mein allergrößter Respekt und Dank gilt an dieser Stelle der hervorragenden Leistung der Co-Autoren Huber, Laux, Lindlbauer, Kramer, Schönfeldinger und Weiss, die als erfahrene Unternehmensberater, routinierte Outsourcing-Spezialisten und akkreditierte StarAudit Professionals mit diesem Dokument wohl einen der hervorragendsten Leitfäden der EuroCloud-Serie verfasst haben.

Wien, Juni 2016

Dr. Tobias Höllwarth
Vorstand EuroCloud Austria

2 Einleitung

Wurden Cloud Services in den letzten Jahren noch als Trend oder als gewinnträchtiges Angebot globaler Serviceanbieter gesehen, so werden sie mittlerweile von den Institutionen der öffentlichen Hand und der europäischen Kommission (als ein Aspekt der Digital Single Market Initiative) als probates Mittel zur Erreichung von Effizienzzielen, zur Produktivitätssteigerung und zur Eliminierung von Nutzungsbarrieren gefördert.

Cloud Services haben mittlerweile einen Reifegrad erreicht, der sie als tatsächliche Option oder zumindest als Erweiterung zum klassischen „on Premise"-Serviceangebot erscheinen lässt. Dabei ist neben der prinzipiellen Frage des Service Sourcings zur Realisierung der damit potenziell verbundenen Vorteile (Reduktion der Investitionskosten, bedarfsorientierte Ressourcenbereitstellung und dergleichen) auch die mögliche Fokussierung auf Kernservices bzw. auch die Nutzung als Inkubator für neue Geschäftsmodelle und Geschäftsideen von Interesse.

Prinzipiell kann aus Anwendersicht mittels Cloud Services das langjährige Versprechen der IT-Industrie wahr werden.

Die prinzipielle Unsicherheit in der Nutzung von Cloud Services hat sich durch die verbreitete Privatnutzung von „Apps" auf Bildschirmen aller Verwendungszwecke und Größen (Fitness-Armband, Smartphone, Table,...) soweit entspannt, dass damit einhergehend eine gewisse Sorglosigkeit im Umgang mit persönlichen Daten zu beobachten ist. Diese ist im Kontext jeglicher Organisationsformen durch unternehmensspezifische Informationssicherheitsrichtlinien zu adressieren.

Prinzipiell kann aus Anwendersicht mittels Cloud Services das langjährige Versprechen der IT-Industrie wahr werden: von überall, jederzeit Zugriff auf Daten und Informationen. Cloud Services versprechen eine einfache Nutzung, da der Anwender sich nicht um eine Installation oder um Software-Aktualisierungen kümmern muss, meist reicht ein Browser, um das Service zu nutzen.

Weiterhin ist gültig, dass Cloud Services das Verständnis der Nutzungserwartungen an die IT-Anwendungen in Unternehmen ändern, insbesondere das Paradigma, dass IT-Abteilungen in den Unternehmen Anwendungen entwickeln oder beschaffen, diese auf den IT-Arbeitsplätzen der Mitarbeiter installieren und auf internen Servern betreiben. Durch Cloud Services stehen nunmehr Anwendungen zur Verfügung, die nicht im Firmennetzwerk betrieben werden, sondern durch die Anwender über das Internet bezogen und genutzt

werden, immer unabhängiger von Vorgaben und Entscheidungen der jeweiligen IT. Dieses Faktum verändert bereits die Rolle und Verantwortungen der IT in Unternehmen.

Die technischen Voraussetzungen sind vorhanden, die Anzahl der angebotenen Cloud Services wächst beständig. Viele Unternehmen haben daher Cloud Services bereits auf ihre Aufgabenliste gesetzt und in ihre IT-Strategie aufgenommen. Wenn es nun um die Umsetzung einer Cloud-Strategie im Unternehmen geht, muss jedes Unternehmen für sich klären, in welchen Bereichen begleitende Maßnahmen zur gesicherten Nutzung notwendig sind.

Durch die Möglichkeit des Multiservice Sourcings erwachsen auch neue Aufgaben für die IT-Abteilungen, da konsequenterweise eine Anpassung der Strukturen bzw. Prozesse, der Infrastruktur und des Betriebsmodelles auf die neuen Rahmenbedingungen erfolgen muss.

Einer Beschaffung und dem Einsatz von Cloud Services muss die Analyse der unternehmerischen Anforderungen in funktionaler, aber auch insbesondere organisatorischer und betriebswirtschaftlicher Hinsicht vorangehen. Die Integration von Cloud Services hat Auswirkungen auf Prozesse im Unternehmen und auf die Aufgaben, mit denen Abteilungen und Personen betraut sind. Die Einsparungspotenziale von Cloud Services klingen oft vielversprechend, sie sind aber als alleiniges Entscheidungskriterium zu wenig. Es sind eine ganze Reihe von anderen Kosten- und Nutzenfaktoren, aber auch Risiken zu beachten.

Gleichzeitig erwachsen durch die Möglichkeit des Multiservice Sourcings auch neue Aufgaben für die IT-Abteilungen, da konsequenterweise eine Anpassung der Strukturen bzw. Prozesse, der Infrastruktur und des Betriebsmodelles auf die neuen Rahmenbedingungen erfolgen muss.

So erfolgt derzeit die Zurverfügungstellung von Cloud Services zumeist noch auf Basis bestehender Servicekataloge und der damit festgeschriebenen Provisionierungs- und Nutzungsprozesse, zumeist als technisches Cloud Service. Technisch, da zumeist die technische Machbarkeit der Zurverfügungstellung und prinzipiellen Nutzbarkeit im Vordergrund steht.

Im nächsten Schritt werden diese „technischen" Cloud Services zumeist über eine Selbstprovisionierungsplattform angeboten, für die bereits ersten Adaptionen der Provisionierungs-, Nutzungs- und Verrechnungsprozesse erfolgen. Weiters werden Servicequalitäten (z. B. StarAudit Self-Audit)[1] und Business-Modell für die konkreten Services definiert. Konsequenterweise entsteht daraus die Herausforderung, eine Neuausrichtung

[1] www.staraudit.org

bestehender Managementsysteme beziehungsweise die Evaluierung und Implementierung von organisationsadäquaten Multiprovider-Managementsystemen zu starten.

Diese Herausforderung der Neuausrichtung (digitale Transformation) erfordert eine organisatorische Begleitung mittels Innovationsmanagement, damit durch eine strategische Ausrichtung das Design der Transformation und Überführung in den Regelbetrieb gewährleistet wird.

Ziel dieses Leitfadens ist nun die Darstellung einer Herangehensweise für Unternehmen von der Vorbereitung bis hin zum laufenden Controlling, sobald Cloud Services eingesetzt sind. Die Darstellung der folgenden „digitalen Transformation" wird in einem weiteren Schritt im Rahmen der Cloud-Computing-Leitfäden erfolgen.

3 Vorbereitung im Unternehmen

3.1 Cloud Services im Unternehmen

Um die Möglichkeiten von Cloud Services objektiv zu evaluieren, ist es notwendig, die Analyse der innerbetrieblichen Anforderungen in funktionaler, organisatorischer und betriebswirtschaftlicher Hinsicht vorab im Sinne einer strategischen Entscheidung zu definieren. Dies bedeutet auch die prinzipielle strategische Entscheidung, welche Ausrichtung eine Unternehmens-IT haben wird. Der Einsatz von Cloud Services ist neben der Nutzung von technischen Möglichkeiten vor allem ein Projekt der Organisationsentwicklung, der organisatorischen Verankerung im Unternehmen.

Neben den prinzipiell zu identifizierenden und zu adressierenden Barrieren im unternehmerischen Kontext gegen die Nutzung von Cloud Services ist zu beachten, dass die Unternehmensgröße bzw. die potenzielle Anwenderanzahl von spezifischen Cloud Services die Vorbehalte und Hindernisse vervielfachen. Die Gründe dafür sind vielfältig und haben meistens mit Misstrauen oder Zweifel am Mehrwert zu tun:

- fehlende Verankerung in die bestehende IT-Strategie
- fehlendes Vertrauen im Sinne von Datenschutz und Sicherheit
- mangelnde Integrationsfähigkeit in Kernapplikationen
- rechtliche Rahmenbedingungen sind nicht zufriedenstellend geklärt
- Angst vor Kompetenzverlust
- Kostenvorteil ist zu gering
- unzureichende Kontrollfunktionen

Die Argumentation für Cloud Services aus Sicht der Anbieter hat natürlich mit den prognostizierten Wachstumszahlen, dem potenziellen Verdrängungswettbewerb und der tatsächlichen Nachfrage der Kunden zu tun.

3.2 Strategischer Rahmen

Vor der eigentlichen Auswahl von Cloud Services und Überlegungen zur deren organisatorischen und technischen Einbettung ins Unternehmen steht aber der strategische

Vor der eigentlichen Auswahl von Cloud Services und Überlegungen zur deren organisatorischen und technischen Einbettung ins Unternehmen steht aber der strategische Aspekt.

Aspekt. Dabei geht es nicht nur um eine Betrachtung der IT und der Technologie, sondern um den Konnex zur Unternehmensstrategie im Generellen. Die folgende Liste stellt generelle Ansatzpunkte für die Definition eines strategischen Rahmens vor:

- Welche Cloud Services werden von den Anwendern bereits in Eigenverantwortung genutzt und sind in Bezug auf Informationssicherheit zu bewerten?
- Für welche Anwendungsfälle kann und möchte die Unternehmens-IT kein entsprechendes „in-house"-Service anbieten?
- Welcher Nutzen wird durch den Einsatz von Cloud Services erwartet?
- Welche bestehenden Risiken können dadurch vermieden bzw. verringert werden?
- Welche zusätzlichen Risiken können durch den Einsatz von Cloud Services entstehen und müssen adressiert werden?
- Welche Prozesse sind im Unternehmen potenziell durch Cloud Services abdeckbar?
- Welche gesetzlichen und organisatorischen Rahmenbedingungen sind jedenfalls einzuhalten?
- Wie ist die aktuelle IT-Landkarte/-Architektur des Unternehmens und welche Komponenten (Infrastruktur, Anwendungen, Services) sind für eine Abdeckung durch welchen Typ von Cloud Services (IaaS, PaaS, SaaS) geeignet?
- Welche Sourcing-Modelle sind auf Basis der aktuellen IT-Landkarte/-Architektur des Unternehmens von Relevanz?

Neben einer Beschäftigung mit Cloud Services auf strategischer Ebene gibt es eine ganze Reihe unternehmensinterner Auslöser, durch die Cloud Services in das Unternehmen getragen werden.

3.3 Cloud und Cloud Services – Begriffe

Im Folgenden werden der Vollständigkeit halber einige wesentliche Begriffe im Zusammenhang mit Cloud und Cloud Services angeführt. Diese Begriffe werden hier nicht vertieft, sondern sollen einen Überblick geben (siehe auch Kapitel 8 Glossar Cloud Computing).

Cloud-Betriebsmodelle

Folgende Betriebsmodelle haben sich in der Cloud etabliert:

- Private Cloud

- Public Cloud
- Hybrid Cloud

Serviceebenen (Serviceplattformen)

Innerhalb der genannten Betriebsmodelle werden von den Cloud-Anbietern im Regelfall drei Serviceebenen angeboten. Diese Ebenen sind IaaS (Infrastructure as a Service), PaaS (Platform as a Service) und SaaS (Software as a Service) und bauen aufeinander auf, wobei IaaS die Basis für die anderen Ebenen darstellt. In ihrem Angebot spezialisieren sich Anbieter aber oft auf eine der Ebenen.

Weitere wesentliche Konzepte

Die folgenden Punkte stellen wesentliche Konzepte und Eigenschaften im Zusammenhang mit Cloud Services dar:

- Virtuelle Ressourcen: Die physische Realisierung des Dienstes ist dem Nutzer verborgen. Dies ermöglicht dem Betreiber die Optimierung des Dienstes hinsichtlich Effizienz und Standardisierung.
- Mandantenfähigkeit: Einzelne Ressourcen bedienen in einer gemeinsam genutzten Umgebung mehrere Benutzer, wobei Mechanismen zum Schutz und zur Isolierung jedes Mandanten angewendet werden. Dies ermöglicht dem Anbieter, Nutzen aus den unterschiedlichen Lastverhalten zu ziehen.
- Verbrauchsabhängige Bezahlung: Nutzer bezahlen nur für Ressourcen, die auch tatsächlich in Anspruch genommen wurden.
- Nutzergesteuerte Bereitstellung: Ressourcen können vom Benutzer selbst angefordert werden, die Bereitstellung läuft dann automatisch ohne Interaktion mit dem Dienstanbieter ab.
- Elastizität: Dienste können spontan und schnell auf Lastveränderungen reagieren. Für den Nutzer scheinen die Ressourcen unendlich zu sein.
- Programmatische Kontrolle: Der Nutzer kann mittels Schnittstelle Ressourcen konfigurieren, nutzen und steuern. Dies ermöglicht dem Nutzer, dynamisch den Verbrauch durch die Anwendung zu steuern, und dem Anbieter, das Ressourcenmanagement zu automatisieren.

Die genannten Konzepte sind u.a. Grundlage für Potenziale und Nutzenfaktoren im Zusammenhang mit Cloud Services (siehe „3.5 Potenziale und Nutzenfaktoren“).

3.4 Standardservices und Spezialservices

Möchte ein Unternehmen aus strategischen Gründen Cloud Services nutzen, dann können folgende Punkte für die Bestimmung von möglichen Cloud Services betrachtet werden, wobei in einem ersten Schritt aufgrund der geringeren Komplexität Standardservices empfohlen werden. In weiteren Schritten können spezielle Services beziehungsweise hybride Lösungen umgesetzt werden.

Standardservices

Cloud Standard oder Commodity Services sind jene Services, die im Normalfall keinen großen IT-technischen Integrationsaufwand bedeuten, für die eine ROI-Berechnung rasch erstellt werden kann und deren Einbindung in die unternehmerischen Kernprozesse nicht zwingend notwendig ist. Beispiele für Standardservices sind:

- E-Mail
- Terminkoordination
- Datensynchronisation und Datenaustausch
- Online-Dateispeicher
- Instant Messaging
- Portal- und Content-Management-Lösungen (CMS)
- Kollaboration und Projektmanagementlösungen
- Temporäre und kurzfristige Rechnerkapazitäten

Weitere Services sind im unternehmensspezifischen Kontext zu identifizieren.

Spezialservices

Unternehmensspezifische, hybride und integrationsintensive Cloud Services sollten dann evaluiert werden, wenn dadurch strategische und/oder organisatorische Mehrwerte adressiert werden können.

Sind diese identifiziert, kann im nächsten Schritt unter Zuhilfenahme des StarAudits die Festlegung der prinzipiellen Servicequalitäten erfolgen:

- Festlegung der Anforderungen an den Serviceanbieter
- Vertragsgrundlagen und kaufmännische Aspekte

- Fragen zur Sicherheit und zum Datenschutz
- Betriebs- und Supportprozesse
- Aspekte der tatsächlich genutzten Infrastruktur
- technische und servicespezifische Anforderungen

Beispiele für Spezialservices sind:

- Zeiterfassungssysteme
- Personalgeschäftsprozesse
- Identity- und Access-Management-Lösungen
- Customer Relationship Management (CRM)
- Enterprise Ressource Planning (ERP)
- Kernprozesse mit Integration in Backend-Systeme und Standardservices
- Dokumentenmanagement-Lösungen (DMS)

Im unternehmensspezifischen Kontext ergibt sich eine Vielzahl an Varianten, da hybride Modelle auch im Kontext mit Standardservices entstehen können.

3.5 Potenziale und Nutzenfaktoren

Die Potenziale und Nutzen, die sich durch den Einsatz von Cloud Services ergeben, sind vom angedachten Service und von unternehmensspezifischen Faktoren abhängig. Es lassen sich aber die folgenden wesentlichen Potenziale und daraus resultierenden Nutzen für ein Unternehmen ableiten:

Die Potenziale und Nutzen, die sich durch den Einsatz von Cloud Services ergeben, sind vom angedachten Service und von unternehmensspezifischen Faktoren abhängig.

- Kostenvorteile: geringe Initialkosten; Vermeidung Aufbau eigener IT-Infrastruktur, Verteilung Kosten auf größere Anzahl von Usern, Nutzung von Skaleneffekten (Rechenleistung, Speicher, ...) Reduktion von Kosten für bestehende IT-Lösungen, Reduktion von Kosten für Ausbauten an der bestehenden IT-Infrastruktur, Reduktion von Lizenzkosten
- Orientierung am Bedarf: nutzungsorientierte Verrechnung, Ausbaubarkeit der Funktionalität/Kontingente mit wachsendem Bedarf (z. B. verschiedene Leistungspakete, Speicherplatz, Rechenleistung, Funktionalität)

- Partizipation an Innovationen: Nutzung von Verbesserungen im Bereich der IT-Infrastruktur und der Anwendungen, Auslagerung des Aufwands für Analysen/ Trendbeobachtungen.

Wie einleitend beschrieben kann der Einsatz von Cloud Services auch bestehende Risiken reduzieren und somit zu weiteren Nutzenfaktoren führen. Ein Beispiel für die Reduktion bestehender Risiken ist, dass in einem Unternehmen eine interne IT-Lösung aus Kostengründen nur begrenzte Redundanzen aufweist und im Fall von Fehlern längere Wiederaufbau- und Fehlerbehebungszeiten verursacht.

Die Potenziale und Nutzenfaktoren von Cloud Services müssen im Zuge der Auswahl von Cloud Services als Kriterien formuliert bzw. auch vertraglich abgesichert werden.

Im Folgenden wird das Thema Risiko im Detail behandelt (siehe Kapitel „3.11 Risikomanagement“ und „3.12 Risiken“). Der Grund liegt nicht darin, dass die Risiken die Nutzenpotenziale von Cloud Services per se überwiegen. Erfahrungsgemäß gilt aber oft, dass das Eintreten eines einzigen Risikos, das nicht betrachtet bzw. nicht mit entsprechenden Vorsorgemaßnahmen begleitet wurde, sämtliche Nutzenaspekte zunichtemacht. Eine eingehende Betrachtung und Behandlung der Risiken ist somit auch die Grundlage für das Heben der vorhandenen Potenziale von Cloud Services.

3.6 Organisatorische Auswirkungen

Durch die Einführung von Cloud Services können sich in einem Unternehmen Änderungen auf verschiedenen Ebenen der Organisation ergeben. Diese Auswirkungen müssen frühzeitig adressiert werden, sodass das Unternehmen zum Zeitpunkt der Auswahl eines Cloud Services entsprechend vorbereitet ist.

Durch die Einführung von Cloud Services können sich in einem Unternehmen Änderungen auf verschiedenen Ebenen der Organisation ergeben. Diese Auswirkungen müssen frühzeitig adressiert werden, sodass das Unternehmen zum Zeitpunkt der Auswahl eines Cloud Services entsprechend vorbereitet ist.

Organisatorische Verantwortlichkeit im Unternehmen

Durch die Einführung von Cloud Services können sich die angestammten Rollen und Verantwortlichkeiten zwischen Fachbereichen und IT verändern. Es ist u. a. möglich, dass ein spezifisches Cloud Service aus der organisatorischen Entscheidungsgewalt der IT-Organisation in Richtung von Schlüsselanwendern (Key Usern) aus den Fachbereichen verlagert wird. Gleichzeitig sind jedoch übergelagerte Prozesse wie die unternehmensweite Erstellung und Überwachung der Informationssicherheit notwendig. Dafür ist eine klare

Verantwortlichkeit der Erstellung, aber auch ein Durchgriffsrecht zur Einhaltung der definierten Richtlinien festzulegen.

Business Value

Cloud Services stellen primär standardisierte Services dar. Daher bedeutet ihre Einführung oft eine Anpassung von bestehenden Abläufen und teilweise eine Einschränkung im Vergleich zu bestehenden Services im Sinne der bereichsspezifischen Bedürfnisse. Aus diesem Aspekt ist die Business-Value-Betrachtung auf der reinen Kostenebene zumeist zu kurz gegriffen. Die Aufbereitung und Kommunikation des Mehrwerts (schnelle und vereinfachte Einführung neuer Technologien; Flexibilität der Lizenzierung; Anbindung mobiler Mitarbeiter; ...) für die unterschiedlichen betroffenen Gruppen auf Basis ihrer Bedürfnisse ist somit neben einer „ehrlichen" Kostenbetrachtung notwendig.

Cloud Services stellen primär standardisierte Services dar. Daher bedeutet ihre Einführung oft eine Anpassung von bestehenden Abläufen und teilweise eine Einschränkung im Vergleich zu bestehenden Services im Sinne der bereichsspezifischen Bedürfnisse.

Weitere Auswirkungen

Weitere Auswirkungen können sich aus der individuellen Unternehmenssituation ergeben und müssen spezifisch z. B. im Rahmen des Assessments der internen Auswirkungen identifiziert werden.

3.7 Assessment der internen Auswirkungen

Die oben genannten organisatorischen Auswirkungen zeigen, dass es für ein Unternehmen ganz wesentlich ist, die Auswirkungen des Umstieges auf ein Cloud Service zu einem möglichst frühen Zeitpunkt zu kennen und zu definieren. Als konkreter Schritt kann ein internes Assessment helfen. Das Assessment kann in Form eines Workshops durchgeführt werden. Im Folgenden wird ein typischer Ablauf für das Assessment beschrieben, in dem ein bestehendes Service ersetzt wird:

Vorbereitung des Assessments

- Die internen Ansprechpartner für das abzulösende Service werden gebeten, die Betriebsprobleme und Benutzerprobleme aus dem letzten Jahr zusammenzufassen. Insbesondere sollten die Probleme aus Sicht der Endbenutzer beschrieben werden.
- Eine Gruppe von Benutzern wird eingeladen, am Workshop als Wissensträger

mitzumachen.

- Es sollten bekannte Annahmen und Rahmenbedingungen zusammengefasst werden wie z. B. fehlende interne Adminrechte, fremdbestimmte Wartungsfenster, Standardisierung in der Einmeldung von Fehlern, zumeist höhere Sicherheitsstandards usw. Diese Annahmen können z. B. aus den Betriebsstandards des Cloud-Servicebetreibers abgeleitet werden.

Ablauf des Assessments

- Die Problembeschreibungen werden im Team besprochen. Eventuell hat einer der Teilnehmer dieses Problem gehabt. Jeder Teilnehmer bekommt eine oder mehrere Problembeschreibungen und soll sich in die Situation aus Nutzersicht hineindenken.
- Die Teilnehmer werden zu ihrem Problem befragt: „Was tun Sie in dieser Situation?“, „Welche Schritte setzen Sie?“ Die Antworten dienen jeweils als Startaktivität für einen Lösungsweg. In der Regel werden die Teilnehmer in diesem Schritt die bisherigen Lösungswege nennen.
- Für jeden Lösungsweg wird für jeden Schritt evaluiert, ob dieser nach dem Umstieg auf das Cloud Service noch möglich ist. Ist ein Schritt nicht möglich, werden die Teilnehmer damit konfrontiert und befragt, was sie alternativ tun würden. Ziel ist es, Änderungen in den derzeitigen Prozessen sowie Bereiche zu identifizieren, in denen die Benutzer Schulung bzw. Information über Änderungen brauchen.
- Die Änderungen, erkannten Probleme, offenen Fragen und getroffenen Annahmen werden dokumentiert und die Planung übernommen.

Typische Themen, die u. a. im Rahmen des Assessments angesprochen werden, sind folgende: Auswirkungen des Verlustes der Adminrechte bzw. Übergang der Adminrechte an den Cloud-Anbieter, wie werden User durch den Cloud-Anbieter im Fall von Supportanfragen eindeutig identifiziert (z. B. für Rücksetzen eines Passworts), Vorgehen zur Vermeidung von Datenverlust und Wiederherstellungsmaßnahmen, Vorgehen bezüglich Beantragung, Änderung und Sperrung von Benutzerrechten.

Das Assessment liefert folgende Ergebnisse:

- Liste der erkannten Probleme
- Liste der offenen Fragen
- Liste der Parameter / Mengen und Verbräuche

- einen persönlichen Eindruck von der neuen Situation für die Beteiligten

Die oben angeführten Schritte sind nur ein grober Rahmen. Wichtigster Erfolgsfaktor ist die weitere Bearbeitung der Ergebnisse (z. B. Nutzung als Kriterien für die Auswahl).

3.8 Anpassung der Prozesse

Anhand der Ergebnisse des Assessments sollten jene Prozesse identifiziert worden sein, die beim Umstieg auf das Cloud Service geändert werden müssen. Bei der Anpassung der Prozesse sollte auf folgende Punkte Rücksicht genommen werden:

Anhand der Ergebnisse des Assessments sollten jene Prozesse identifiziert worden sein, die beim Umstieg auf das Cloud Service geändert werden müssen.

- Wie oft kommt der Prozess pro Jahr / pro Quartal vor? Ergeben sich durch die Nutzung des Cloud Services Änderungen in der Häufigkeit? Wird der Prozess dadurch wichtiger / weniger wichtig?
- Gibt es geänderte Ansprechpartner und Verantwortliche, von denen einige auch außerhalb des Unternehmens sitzen?
- Gibt es Schnittstellen und „Single Points of Contact" innerhalb des Unternehmens, über die möglicherweise die Kommunikation zu bündeln ist?
- Gibt es geänderte Voraussetzungen zur Nutzung eines Services (z. B. Kenntnis der Kundennummer, geänderte Identifikationsprozeduren)?
- Gibt es andere, in der Regel längere, Antwortzeiten als bisher? Dies kann auch dazu führen, dass Prozesse geteilt werden müssen.

Die Bereinigung der Prozesse kann mit Hilfe einer Prozessmodellierungsmethode durchgeführt werden. Die Dokumentation der geänderten Prozesse dient einerseits zur Vorbereitung der Kommunikation, andererseits zur möglichen Anpassung der Servicelevels.

3.9 Erhebung von Mengengerüsten und Bereinigung von Daten

Die IT ist in vielen Unternehmen historisch gewachsen. Dies bedeutet in den meisten Fällen, dass die Anforderungen sehr auf die Wünsche und Besonderheiten der User angepasst wurden. Insbesondere trifft dies auf die für IT-Services genutzten Mengen zu.

Die IT ist in vielen Unternehmen historisch gewachsen. Dies bedeutet in den meisten Fällen, dass die Anforderungen sehr auf die Wünsche und Besonderheiten der User angepasst wurden.

Beispiele sind:

- genutzter Speicherplatz auf Fileservern
- Speicherverbrauch für persönliche Dateien
- Größen von E-Mail-Postfächern
- Upload- und Download-Mengen

Beim Umstieg auf Cloud Services ergibt sich eine gute Gelegenheit, die gewachsenen Datenmengen zu bereinigen, d. h. es werden nur die tatsächlich für die laufenden operativen Tätigkeiten benötigten Informationen migriert. Die bereits bestehenden Daten können in geeigneter Form archiviert werden. Durch diese Bereinigung kann man die Nutzung des Cloud Services mit einer geringeren Ausgangsmenge beginnen und so die Startkosten reduzieren (z. B. Nutzung günstigerer Cloud-Service-Pakete). In Ausnahmefällen kann es auch sein, dass der Cloud-Anbieter Limits bezüglich der Nutzung von Ressourcen, z. B. Speicherplatz, definiert. Auch in diesen Fällen müssen vorab Datenbereinigungen stattfinden. Folgende Schritte sollten bei der Erhebung der IT-Mengen/Mengengerüste erfolgen:

- Identifikation der IT-Mengen für das Mengengerüst in Form einer Liste
- Einteilung, welche IT-Mengen vom Umstieg auf Cloud Services betroffen sind und welche nicht betroffen sind. Im Weiteren sollen nur die betroffenen IT-Mengen behandelt werden.
- Erhebung des tatsächlichen Verbrauches des letzten Jahres / der letzten Perioden
- Erhebung des Wachstums der Mengen monatlich / jährlich

Im Zuge der Bereinigung der Daten sollten folgende Schritte durchgeführt werden:

- Feststellen, ob man durch eine Bereinigung beim Start günstigere Pakete nutzen kann.
- Für den Fall, dass der Cloud-Anbieter Mengenlimits definiert hat:
  Feststellen, ob das Cloud Service überhaupt aufgrund der aktuellen IT-Mengen bzw. unter Berücksichtigung eines vorhersehbaren Mengenwachstums interessant ist.
- Klärung, ob die Prozesse wirklich diese Mengen an Daten brauchen. Identifikation von Alternativen für die Daten, die alternativ gelagert, archiviert bzw. gespeichert werden sollen.
- Vorbereitung und Planung, wie die jetzige Situation verändert werden soll, wie die

Daten – wenn notwendig – zu bereinigen sind. Projektmäßige Planung der weiteren Schritte.

Weniger Daten für die Migration zu haben bedeutet, eine einfachere Migration durchzuführen.

Weniger Daten für die Migration zu haben bedeutet, eine einfachere Migration durchzuführen.

3.10 Vorbereitende Kommunikation

Ein Umstieg bedeutet neben den technischen Änderungen eine ganze Menge an organisatorischen Änderungen. Diese Änderungen sollten begleitend zum gesamten Auswahl- und Umsetzungsprozess in geeigneter Form im Unternehmen kommuniziert werden.

Die Planung der Kommunikation kann in Form eines Kommunikationsplans dokumentiert werden. Folgende Themen sollten im Zuge der Kommunikation berücksichtigt werden:

- Vereinbarungen über Nutzungspakete wie z. B. E-Mail-Postfachgrößen
- Anleitung für die vorbereitenden Schritte zur Bereinigung der Daten
- Dokumentation von Interimsprozessen rund um die Migration
- Dokumentation der vom Benutzer durchzuführenden Schritte rund um die Migration
- Frequently Asked Questions (FAQ) mit Erfahrungen und Erkenntnissen
- Lösungen für bekannte Probleme

Die Kommunikation sollte bereits in ausreichendem Zeitabstand vor dem geplanten Umstieg erfolgen. Es empfiehlt sich, eine zentrale Anlaufstelle für Informationen einzurichten. Diese kann je nach Unternehmensgröße ein bestimmter Mitarbeiter, eine bestimmte Funktionsmailbox oder eine Support-Telefonnummer sein. An diese zentrale Anlaufstelle sollen die Mitarbeiter alle offenen Fragen richten und die Kommunikation sollte auch durch diese Stelle erfolgen.

3.11 Risikomanagement

Der Einsatz von Cloud Services umfasst eine Reihe von Risiken, die über das Risikopotenzial einer im Unternehmen betriebenen Anwendung hinausgehen. Es ist daher wesentlich, dass vor der Auswahl, dem Einsatz und dem Betrieb von Cloud Services eine Risikoanalyse für die konkrete Situation des Unternehmens durchgeführt wird.

Die Risk Management Association (RMA) definiert gemäß ihrer „Grundsätze eines ordnungsgemäßen Risikomanagements“ (GoR) folgende Hauptprozessschritte für den

Risikomanagementprozess:

- Risikoidentifikation: Die Chancen und Risiken müssen vollständig, richtig, zeitgerecht und geordnet erfasst, beobachtet und rückgemeldet werden.
- Risikobewertung: Aus den erkannten Risiken werden zumindest die existenzbedrohenden identifiziert und bewertet.
- Risikobewältigung: Die richtigen Maßnahmen werden entschieden und eingeleitet. Dies erfolgt zu einem Zeitpunkt, wo die Gegensteuerung unter Berücksichtigung der Verzögerungen noch schnell genug stattfindet.
- Risikodokumentation und Berichtswesen: Die identifizierten, bewerteten und mit Maßnahmen versehenen Risiken sind nachvollziehbar zu dokumentieren und zu berichten.

Bei der Risikobewältigung unterscheidet man Maßnahmen zur Vermeidung des Eintretens von Risiken, Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit eines Risikos und Maßnahmen zur Reduktion des Schadenspotenzials eines Risikos.

Bei der Risikobewältigung unterscheidet man Maßnahmen zur Vermeidung des Eintretens von Risiken, Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit eines Risikos und Maßnahmen zur Reduktion des Schadenspotenzials eines Risikos.

Wesentlich für ein effektives Risikomanagement ist, dass es nicht nur zu Beginn, sondern regelmäßig auch während der Nutzung des Cloud Services als Teil des Cloud Controllings stattfindet, da sich die Risiken und auch die geeigneten Maßnahmen im Nutzungszeitraum verändern können.

Auslöser für solche Veränderungen sind u. a.:

- Organisatorische Änderungen, z. B. Erhöhung/Reduktion des Personalstands, Ausweitung der Geschäftstätigkeit, Veränderungen in der Kundenstruktur und in den Kundenbedürfnissen
- Gesetzliche Änderungen, insbesondere Änderungen im Datenschutz
- Technische Änderungen, z. B. Sicherheitsaspekte, neue Technologien, Änderungen in der IT-Landschaft des Unternehmens
- Kommerzielle Änderungen, z. B. Cloud Services mit äquivalentem Funktionsumfang und preislichen Vorteilen

Die Abwägung, welche Art von Maßnahme die geeignetste zur Risikobewältigung ist, hängt von der Art des Risikos ab und erfolgt auf wirtschaftlicher Ebene durch

einen Vergleich der Höhe des Schadenspotenzials und der Kosten, die die jeweiligen Risikobewältigungsmaßnahmen verursachen.

3.12 Risiken

Die folgenden Hauptrisiken nennt ENISA (European Network and Information Security Agency) aufgrund von durchgeführten Studien (vgl. Höllwarth [Hrsg.], Der Weg in die Cloud [2011]):

- Unzureichende Servicelevel-Garantien
- Providerabhängigkeit (Lock-In-Situation)
- Unzureichende Datenabgrenzung
- Probleme bei der Einhaltung von Compliance-Vorgaben
- Unzureichende Absicherung der Administrationsfunktionen
- Datenschutzverletzungen
- Unzureichende Datenlöschung auf Kundenanforderung
- Angriff von innen durch nicht vertrauenswürdige Personen

Diese angeführten Risiken können der Ausgangspunkt für eine Risikobetrachtung sein. Es wird aber empfohlen, auch Risikobereiche zu adressieren, die über diese eher technischen Risiken hinausgehen. Dazu kann als Ausgangsbasis das Analyse-Framework von R. Wickart herangezogen werden.

Wickart identifiziert in seinem „Analyse-Framework Strategieentwicklung und Risikomanagement" die folgenden drei Analyseebenen mit den jeweiligen Themenbereichen (vgl. Wickart, R., Analyse-Framework Strategieentwicklung und Risikomanagement [2010]):

- Unternehmung (interne Umwelt): Management, Personal, Technologieentwicklung, Finanzen, Materialbeschaffung, Produktion / Dienstleistung, Ausgangslogistik, Marketing und Vertrieb, Kundendienst
- Interessengruppen (nahe Umwelt): Kunden, Lieferanten, Konkurrenten, Banken und Gläubiger, Inhaber und Investoren, Partnerschaften (Allianzen), Medien, sonstige Interessengruppen
- Makroökonomische Faktoren (ferne Umwelt): politische Faktoren, ökonomische Faktoren, soziokulturelle Faktoren, technologische Faktoren, ökologische Faktoren, rechtliche Faktoren

Im Folgenden werden typische Risiken aus den einzelnen Bereichen angeführt:

Risiken auf der Ebene des Unternehmens (interne Umwelt)

- Intransparenz: ein Cloud Service bietet keine oder keine transparente Möglichkeit, um Verbrauch zu dokumentieren und diesen in Relation zu den verrechneten Preisen zu setzen; keine transparente Verrechnung der Cloud Services
- Imageschaden: es kann ein Imageschaden im Fall von Datenverlusten oder Verletzungen des Datenschutzes entstehen
- Umsetzungsrisiken: Risiken im Rahmen der Umsetzung eines Einführungsprojekts für Cloud Services (z. B. Ressourcenengpässe)
- Kompetenzdefizite: es gibt keine/zu wenige entsprechend ausgebildete Mitarbeiter im Unternehmen, um das geplante Cloud Service im Unternehmen einzuführen
- Mangelnde Motivation: es besteht kein/wenig Interesse der Mitarbeiter, ein Cloud Service einzusetzen, da sich dadurch die Aufgaben des Mitarbeiters/einer Gruppe von Mitarbeitern ändern
- Keine verbindlichen Servicelevels: keine verbindliche/vertragliche Zusicherung von Verfügbarkeiten eines Cloud Services bzw. keine ausreichende Verfügbarkeit
- Migrationsrisiken: keine/sehr aufwendige Möglichkeit, bestehende Daten in das Cloud Service zu migrieren
- „Versteckte" Kosten: hohe Kosten bei Erhöhung/Reduktion der Verbrauchsmengen (je nach Verrechnungsmodell können die Verbrauchsmengen Anzahl der User, Anzahl der Transaktionen, Datenvolumina etc. sein)

Risiken auf der Ebene der Interessensgruppen (nahe Umwelt)

- Betreiberrisiko: geringe wirtschaftliche Stabilität des Betreibers des Cloud Services (z. B. Unternehmen ist noch nicht lange am Markt tätig, Cloud Service hat noch keinen hohen Reifegrad)
- Verminderung Kundenservice: Cloud Service soll in einem Bereich eingesetzt werden, der ein potenzielles Risiko für den Kunden zugesicherte Leistungen darstellt; Cloud Service soll in einem Bereich eingesetzt werden, der die Kommunikation mit Kunden beeinflusst

Risiken auf der Ebene von makroökonomische Faktoren (ferne Umwelt)

- Standortrisiko: Cloud-Anbieter ist in einem Land angesiedelt, das abweichende Richtlinien und Gesetze z. B. im Zusammenhang mit Datenschutz hat

- Wechselkursrisiko: Wechselkursrisiken durch Verrechnung des Cloud Services in einer Fremdwährung
- Compliance-Verletzungen: die Leistungserbringung des Cloud-Anbieters folgt nicht/nicht nachweislich dem ökologischen Standard des eigenen Unternehmens
- Gesetzliche Risiken: sämtliche Risiken, die sich daraus ergeben, dass gesetzliche Rahmenbedingungen nicht eingehalten werden können, z. B. Datenschutz, Datensicherheit, Aufbewahrungs- und Nachweispflichten

4 Auswahl des Cloud-Anbieters und des Cloud Services

Auf Basis der vorangegangenen Überlegungen sollte es möglich sein, eine Liste von potenziellen Services mit wesentlichen Anforderungen und zu betrachtenden Eignungskriterien zu erstellen. Diese Punkte dienen als Grundlage für die Definition der Kriterien zur Auswahl von Anbietern.

4.1 Definition von Kriterien

Bei der Auswahl eines Cloud Services und damit verbunden eines Cloud-Anbieters ist es in der Praxis sinnvoll, in zwei Schritten vorzugehen: Definition von Eignungs- und Auswahlkriterien.

Bei der Auswahl eines Cloud Services und damit verbunden eines Cloud-Anbieters ist es in der Praxis sinnvoll, in zwei Schritten vorzugehen:

- Definition von Eignungskriterien (Musskriterien): Musskriterien, die ein Cloud-Anbieter bzw. dessen Service erfüllen muss, um in die engere Wahl zu kommen – „Short List". Die Short List bildet dann jene Angebote, die man im Detail miteinander über die Auswahlkriterien vergleicht.
- Definition von Auswahlkriterien: bewertbare Anforderungen, die es ermöglichen, das am besten geeignete Cloud Service auf Basis der Short List auszuwählen.

Die Definition von Eignungskriterien und Auswahlkriterien ist insbesondere für Ausschreibungen öffentlicher Auftraggeber relevant, die nach dem Bundesvergabegesetz („BVerG") beschaffen müssen (siehe auch „EuroCloud-Austria Leitfaden Nr. 2 Cloud Services Öffentliche Auftragsvergabe"). Die Unterscheidung in diese beiden Arten von Kriterien hat sich aber auch für Beschaffungen im privatwirtschaftlichen Umfeld bewährt, da dadurch ein schrittweises Vorgehen möglich ist und sich bereits zu Beginn jene Anbieter ausfiltern lassen, die tatsächlich die wesentlichen Musskriterien erfüllen.

4.2 Eignungskriterien (Musskriterien)

Bei der Definition der Eignungskriterien (Musskriterien) ist es wesentlich, jene Kriterien zu definieren, die jedenfalls erfüllt sein müssen. Es empfiehlt sich bei der Definition der Musskriterien, insbesondere auf Themen zu achten, die „Showstopper" darstellen, d. h. deren Nichterfüllung den Einsatz von Cloud Services im Unternehmen komplett verhindern. Die Identifikation von Showstoppern sollte frühzeitig erfolgen, d. h. in der Phase der Vorbereitung muss prinzipiell geklärt werden, ob z. B. Cloud Services mit den gesetzlichen

Verpflichtungen und strategischen Rahmenbedingungen eines Unternehmens in Einklang gebracht werden können.

Es sollten auch alle Mussanforderungen genannt werden, die sich aus der Bewältigung identifizierter Risiken ergeben, z. B. im Bereich des Datenschutzes (siehe auch „3.12 Risiken"). Im Folgenden werden relevante Eignungskriterien beschrieben und nach den Bereichen Anbieter, Vertrag, Datenschutz und Datensicherheit, Rechenzentrum und Betriebsprozesse beispielhaft beschrieben. Um eine umfassende Prüfung der Eignungskriterien durchzuführen, sollte z. B. der StarAudit-Katalog herangezogen werden.

Anbieterkriterien

Bei der Auswahl eines Cloud-Service-Anbieters ist es wichtig, darauf zu achten, dass dieser ein vertrauenswürdiger Partner ist, der für ein Unternehmen auch längerfristig das benötigte Cloud Service anbieten kann. D. h. es sollten solche Anbieter ausgesucht werden, die schon länger am Markt sind, deren Cloud Services sich bereits etabliert haben, die einen soliden Kundenstock aufweisen und ein längerfristiges und auf Bestand ausgerichtetes Business-Modell haben.

Ein weiteres relevantes Kriterium ist, welche Partnermodelle bei den Cloud-Anbietern zur Anwendung kommen. Cloud-Anbieter können international oder national unterschiedlich agieren. Manche Cloud Services können direkt beim „Hersteller" bezogen werden oder aber bei einem Cloud-Anbieter, der als Partner des „Herstellers" agiert (z. B. kann ein lokaler Partner die Datenhaltung innerhalb Österreichs oder innerhalb der EU sicherstellen und eventuell auch noch zusätzlich Betreuungsleistungen anbieten).

Oft steht hinter einem Cloud Service eine ganze Reihe von weiteren Anbietern, die einzelne Funktionalitäten des Services oder eines Servicepakets abdecken. Diese Zusammenhänge sind oft nicht unmittelbar ersichtlich. Wichtig ist dieser Aspekt bei der Vertragsbeziehung, d. h. es muss genau geprüft werden, wer der Vertragspartner ist und durch wen die vereinbarten Servicelevel sichergestellt werden, wie die Subunternehmer durch den Cloud Service Provider eingebunden werden usw.

Ein anderer Aspekt bei der Wahl des geeigneten Partners kann sein, zu prüfen, ob ein Cloud Service durch einen Cloud-Anbieter angeboten wird, der bereits bestehende Geschäftsbeziehungen zum Unternehmen hat und man hier Synergien nutzen kann (z. B. Umwandlung von Lizenzen, Know-how bezüglich Schnittstellen).

Weiters ist zu klären, wie weit die Beschreibung des konkreten Services den definierten funktionalen Mindestanforderungen des Unternehmens entspricht, damit diese in

einem ersten Auswahlschritt als die unbedingt erforderlichen Musskriterien und Rahmenbedingungen definiert werden, die ein Cloud Service bzw. dessen Anbieter jedenfalls zu erfüllen hat, und in der Folge geprüft werden können. Ein kurzer Auszug relevanter Beispiele:

- verwendetes Betriebssystem
- Client-Anforderungen (Office-Pakete, Java oder .Net Releases)
- Browser-Anforderungen
- User-Identity-Verwaltung
- administrative Berechtigungen an den Endgeräten
- Netzwerkverfügbarkeit (Bandbreite)
- Verfügbarkeit technischer Schnittstellen

Die definierten Kriterien sollen sicherstellen, dass die von einem Unternehmen benötigten Funktionalitäten (Software Features), aber auch weitere Services (wie z. B. Hotline, Migrationsaufgaben) durch einen Cloud-Anbieter nachweislich abgedeckt werden können.

Zur Verifikation ist es sinnvoll, von den Anbietern geeignete Referenzen anzufordern oder verfügbare Kundenlisten und Referenzangaben zu erheben. Auch hier ist die Vorgehensweise im Detail davon abhängig, welche Art von Cloud Service benötigt wird. Referenzen anzufordern, diese im Internet zu recherchieren bzw. angegebene Referenzen nachzufragen ist in jedem Fall empfehlenswert. Wenn Referenzen von einem Cloud-Anbieter angefordert werden, dann sollte man darauf achten, dass diese Kriterien erfüllen, die der eigenen Unternehmenssituation entsprechen (z. B. Anzahl Mitarbeiter, Anzahl Arbeitsplätze, Standorte, benötigte Leistungen, Branche).

Vertragskriterien und kaufmännischer Bezug

In Bezug auf die zu definierende Liste der Mussanforderungen und Rahmenbedingungen sind die folgenden Aspekte vorab zu definieren und zu dokumentieren (im Kapitel 7, Checkliste Vertragselemente, werden konkrete Vertragsinhalte angeführt):

- Welche Rechtsstandorte sind für das Unternehmen akzeptabel?
- Verfügbarkeit von Verträgen, um vorab einzusehen, welche wesentlichen Inhalte mögliche Ausschließungsgründe darstellen (z. B. nicht zustimmungspflichtige Änderungen in laufenden Verträgen)
- Datenschutzanforderungen und damit einhergehende Nutzungsrechte der Unternehmensdaten

- Nutzung von Subunternehmern in der Erbringung des Services

Der kaufmännische Bezug der Services ist an eine Reihe von Fragen geknüpft, die wesentlich über die üblichen vertraglichen Punkte eines Softwarekaufes hinausgehen.

- Wie wird die Lizenzierung im Falle von bestehenden Rahmenverträgen mit einem Cloud-Anbieter durchgeführt?
- Welche Vertragslaufzeiten ermöglichen dem Unternehmen die gewünschte Flexibilität?
- Welche Regelungen sind vorgesehen bei Serviceunterbrechung oder Insolvenz?
- Welche Servicelevels und Performancekennzahlen werden vom Cloud-Anbieter geboten, welche Kosten sind damit verbunden und wie können diese proaktiv überprüft werden?
- Welches Recht wird im Falle eines Disputes zur Anwendung kommen?

Die kommerziellen Punkte haben starke Verbindung zu den Anforderungen und vertraglichen Rahmenbedingungen und sind daher immer in einem größeren Zusammenhang zu sehen.

Informationen bezüglich Datenzugriff und -schutz im Falle einer einvernehmlichen Servicebeendigung, aber insbesondere bei einer notwendigen einseitigen Beendigung sind vorab zu definieren.

Kriterien des Datenschutzes und der Datensicherheit

Beinahe ein Hotspot in den Grundsatzüberlegungen bei der Definition der Musskriterien sind die organisatorischen Fragen zum Datenschutz und zur Datensicherheit.

Um die Anforderungen und die Eignung in Bezug auf den Datenschutz prinzipiell klären zu können, wurde die Cloud Privacy Check[2] (CPC) Methodik entwickelt. Mittels des CPC werden 90 Prozent der komplexen Anforderungen abgedeckt, die notwendig sind, um in vier Schritten ein Grundverständnis über das notwendige Vorgehen zu entwickeln. Der besondere Charme des CPC liegt darin, dass bei der Auswahl des jeweiligen rechtlichen Themas eine mittlerweile landespezifische Information aus 32 Ländern abgerufen werden kann.

Die vier Schritte sind:

- Klärung, ob im konkreten Sachverhalt personenbezogene Daten betroffen sind, z. B. mit dem Cloud Privacy Check[3],

[2] Siehe www.cloudprivacycheck.eu
[3] www.cloudprivacycheck.eu

- ob Personendaten von dem potenziellen Cloud Service Provider verarbeitet oder diesem zugänglich gemacht werden,
- ob die Daten das Land des Kunden verlassen und
- Prüfung, ob der Cloud Provider sich eines Subauftragnehmers bedient.

Des Weiteren wird ein „rechtlicher Werkzeugkasten" angeboten, der wesentliche Basisinformationen zu folgenden Themen enthält:

- Cloud-Nutzungsvertrag, der die Leistungspflichten des potenziellen Cloud Service Providers und des Cloud Service Consumers regelt
- Vereinbarung betreffend Auftragsverarbeitung, in der die jeweils nationalen Regelungen für Auftragsdatenverarbeitung zu regeln sind
- Maßnahmen bei Grenzüberschreitung, die die Leitlinien zur datenschutzkonformen Ausgestaltung der grenzüberschreitenden Datenverarbeitung definieren
- Maßnahmen zur Einbindung von Subunternehmern durch den Cloud Service Provider
- Mitteilung zur Erhöhung der Transparenz

Kriterien des technischen Betriebs

Die Nutzung von Cloud Services bedingt neben dem Verständnis der Nutzungsanforderungen und der in Frage kommenden Bezugsmodelle (siehe Kapitel 3.3) sowie einer detaillierten Klärung der zugrundeliegenden Funktionsbeschreibung auch die Klärung des Cloud-Anbieter-Profils. Hier sind neben prinzipiellen Anbieterinformationen die physische Lokation des Rechenzentrumbetriebs und die Klärung des Partnermodells für die Bewertung wesentlich. Davon sind die entsprechenden Datenschutzmaßnahmen abzuleiten (siehe Euro Cloud Leitfaden „Recht, Datenschutz & Compliance"), um dem Bedürfnis nach Datenschutz, Datensicherheit und Transparenz zu entsprechen.

Nachweise und Zertifizierungen stellen ein weiteres Kriterium dar, das bei der Vorauswahl von geeigneten Cloud-Anbietern unterstützt. Je nach benötigtem Cloud Service sind unterschiedliche Zertifikate relevant, z. B.:

- unabhängige Zertifizierungen wie ISO27001, ITIL-Zertifizierungen für das Service Management, EU-Standardvertragsklausel (EU Model Clauses) für Datenschutz
- cloudspezifische Zertifizierungen wie das StarAudit

- Sicherheitsaspekte (z. B. physischer Zutrittsschutz in Rechenzentren, Firewall, Autorisierung/Authentifizierung, Verschlüsselung des Datenverkehrs)

Die Relevanz der Zertifikate – insbesondere der cloudspezifischen – liegt darin, dass durch die zugrundeliegenden (externen) Audits bereits Vorgehensweisen des Cloud-Anbieters geprüft wurden, die für einen Kunden schwer bis gar nicht prüfbar sind.

Die Relevanz der Zertifikate – insbesondere der cloudspezifischen – liegt darin, dass durch die zugrundeliegenden (externen) Audits bereits Vorgehensweisen des Cloud-Anbieters geprüft wurden, die für einen Kunden schwer bis gar nicht prüfbar sind.

Kriterien der Betriebsprozesse

Die Bereiche Betrieb und Betriebsprozesse sind ganz wesentlich im Zusammenhang mit Cloud Services.

Wiederkehrende Themen und Fragestellungen sind:

- Verwaltung von Zugriffsbeschränkungen, welche Sicherheitsmaßnahmen sind verfügbar (Daten, Anwendungen, Host, Netzwerk und Transfer)?
- Verschlüsselung der in der Cloud gelagerten Daten
- zugesichertes, periodisches Backup und Recovery der Daten sowie Handling der Backupmedien
- Zugesicherte Antwortzeiten und Reaktionszeiten im Falle notwendiger Supportanfragen wie für die Sperrung oder Rücksetzung von Accounts
- Verfügbarkeit von Problemmanagementprozessen und -systemen
- Proaktive Informationspflichten an den Enduser / an die Kunden

Neben der Sicherheit ist auch noch die Compliance zu berücksichtigen. Da diese stark vom Unternehmenszweck abhängt, wird sie hier nicht weiter ausgeführt.

4.3 Auswahlkriterien

Mit Hilfe der Auswahlkriterien werden die vorausgewählten Cloud Services näher analysiert und miteinander verglichen. In diesem Schritt geht es z. B. bei SaaS darum, welche Funktionalitäten im Detail vorhanden sind oder wie z. B. Hotline-Erreichbarkeit, Sprache der Hotline usw. sind.

Für die Auswahl sind folgende Kriterien relevant:

- Verfügbarkeit der benötigten Funktionalitäten
- Verfügbarkeit/Abdeckbarkeit der benötigten Zusatzservices wie z. B. Hotline
- Detaillierung der benötigten Dienstleistungen wie z. B. Datenmigration, Einführungsbegleitung, Schulung
- Preise/Verrechnungsmodell

Wichtig ist, die Kriterien so definieren, dass man die eingeholten Angebote und Informationen der einzelnen Cloud Services/Cloud-Anbieter auch tatsächlich vergleichen kann.

Wichtig ist, die Kriterien so definieren, dass man die eingeholten Angebote und Informationen der einzelnen Cloud Services/ Cloud-Anbieter auch tatsächlich vergleichen kann. Weiters sind an dieser Stelle auch die erhobenen Mengengerüste (siehe „3.9 Erhebung von Mengengerüsten und Bereinigung von Daten“) relevant, um in Folge die Preise / Verrechnungsmodelle der Cloud-Anbieter gegenüberstellen zu können.

Vergleich der Angebote

Der Vergleich der angebotenen Cloud Services ist umso besser möglich, je klarer die Anforderungen und Rahmenbedingungen definiert wurden. Es muss aber auch darauf hingewiesen werden, dass erfahrungsgemäß eine vollständige Prüfung aller Aspekte und Details sehr aufwendig werden kann bzw. kaum möglich ist und hier eine Vorgehensweise gewählt werden sollte, die den Aufwand in einem vertretbaren Rahmen hält.

Mit dem Abschluss der Auswahlphase muss eine Entscheidungsgrundlage vorliegen, auf deren Basis das benötigte Cloud Service angeschafft wird und die Umstiegsphase geplant werden kann.

5 Umstieg auf das Cloud Service

Eine gute Vorbereitung und eine adäquate Wahl der Migrationsmethode sind genauso wichtig wie eine besondere Aufmerksamkeit während der Migration.

Ein Umstieg (Migration) auf ein Cloud Service ist für die meisten Unternehmen etwas, was nicht zum „Tagesgeschäft" gehört. Eine gute Vorbereitung und eine adäquate Wahl der Migrationsmethode sind genauso wichtig wie eine besondere Aufmerksamkeit während der Migration. Manche der nachfolgenden Schritte können bereits sehr früh – parallel zu den strategischen Überlegungen und der Auswahl des Cloud-Anbieters – begonnen werden.

5.1 Wahl der Migrationsmethode

Grundsätzlich stehen je nach Unternehmensgröße und Service folgende unterschiedliche Migrationsarten zur Verfügung.

- Big Bang (Umstieg in einem Schritt): In einer Big-Bang-Migration wird das gesamte Service für alle Benutzer zum gleichen Zeitpunkt umgestellt. Eine Umstellung dieser Art verlangt gute Planung und normalerweise eine bis zwei Testmigrationen. Insbesondere sind Migrationsaktivitäten mit langer Laufzeit kritisch für eine Big-Bang-Migration (z. B. Kopieren der gesamten Dateien etc.). Der besondere Vorteil dieser Migrationsvariante liegt im Entfall eines etwaigen Doppelbetriebes. Die Big-Bang-Migration wird dort angewendet, wo ein Doppelbetrieb kostenintensiv und organisatorisch schwer durchzuführen ist.
- Schrittweise Migration: Die phasenweise Migration erfolgt in mehreren Schritten. Bei den einzelnen Schritten werden bestimmte Gruppen von Benutzern migriert. Durch die Größe dieser Schritte kann die Komplexität gut gesteuert werden. Während der Gesamtmigration ist ein Doppelbetrieb der Services aufrechtzuerhalten. Die Schritte werden in der gleichen Form durchgeführt, d. h. die Migrationsmannschaft gewinnt mit jedem Schritt mehr Erfahrung und die Qualität der Migration steigt daher.
- Optionaler Pilotbetrieb: Der Pilotbetrieb kann sowohl vor einer Big-Bang-Migration als auch vor einer schrittweisen Migration verwendet werden. In dieser Phase wird das Service für eine Gruppe von „friendly usern" bereitgestellt. Anhand der Erfahrungen dieser Pilot-User werden Erkenntnisse für die Migration erarbeitet. Die gewonnenen Erkenntnisse fließen in die Dokumentation sowie auch in den technischen Migrationsablauf ein

Die Wahl der Migrationsmethode sollte so früh wie möglich erfolgen. Bei der Wahl sollten sich die Verantwortlichen sowohl vom Cloud-Anbieter als auch von internen und externen Experten beraten lassen. Bei jedem Cloud Service gibt es Erkenntnisse, was in der Vergangenheit gut bzw. weniger gut funktioniert hat.

Ist die Migrationsart festgelegt, ist die Entscheidung über einen optionalen Pilotbetrieb zu treffen. Der Pilotbetrieb sollte so gestaltet sein, dass die Benutzer das Service anstatt des alten Services nutzen. Eine Nutzung zusätzlich zum bisherigen Service hat sich als nicht besonders erkenntnisbringend herausgestellt.

Ist die Migrationsart festgelegt, ist die Entscheidung über einen optionalen Pilotbetrieb zu treffen.

5.2 Planung der Migration

In einer Migration wird ein System von einem Ausgangszustand erfolgreich in einen Zielzustand versetzt. Die Migration umfasst alle Schritte, die notwendig sind, um diese Transformation zu ermöglichen.

Wichtige Voraussetzungen sind, dass man den Ausgangszustand sowie den Zielzustand kennt und in geeigneter Form beschreiben kann. Information über den Ausgangszustand bekommt man in der Regel:

- von der internen IT-Abteilung
- von Spezialisten als Migrationsbegleiter
- mithilfe eines Fragekataloges, den der Cloud-Anbieter zur Verfügung stellt

Wichtig ist, dass alle relevanten Fakten, Konfigurationen, Einstellungen, Mengen etc. berücksichtigt werden. Aus der Erfahrung ist der Ausgangszustand auch bei guter Dokumentation nur in den seltensten Fällen ausreichend detailliert erfasst.

Eine Beschreibung des Zielzustandes bekommt man:

- von der internen IT-Abteilung in Zusammenarbeit mit den Spezialisten des Cloud-Anbieters
- von Spezialisten als Migrationsbegleiter
- vom Cloud-Anbieter aufgrund seiner Erfahrung. In diesem Fall muss jedoch ein Quercheck mit dem Planungsteam auf Vollständigkeit und Verständlichkeit erfolgen.

Sind der Zielzustand und die Ausgangslage ausreichend beschrieben, so ist der nächste Schritt die Planung der Migration. Dabei sind zu berücksichtigen:

- Alle technischen und organisatorischen Schritte vor der Migration. Ziel sollte sein, alle Vorbedingungen für den Start der Migration zu erarbeiten.
- Alle Schritte während der Migration. Hier ist empfohlen, mehrere Meilensteine an markanten oder kritischen Punkten der Migration zu identifizieren. Diese Schritte enden in der Regel in einer „GO"-Entscheidung.
- Alle Schritte, die nach einer „GO"-Entscheidung notwendig sind bis zur Aufnahme des Regelbetriebes.
- Alle Schritte, die nach einer „NO-GO"-Entscheidung notwendig sind, um den ursprünglichen Zustand wiederherzustellen.

Diese Planung kann in mehreren Workshops erfolgen, wo neben „Best Practices" der Beteiligten auch der Plan iterativ verfeinert wird. Nach den Workshops sollte der Gesamtplan immer an alle Teilnehmer kommuniziert werden.

Diese Planung kann in mehreren Workshops erfolgen, wo neben „Best Practices" der Beteiligten auch der Plan iterativ verfeinert wird. Nach den Workshops sollte der Gesamtplan immer an alle Teilnehmer kommuniziert werden.

Hat der Plan eine finale Version erreicht, so sollte über die Migrationstests entschieden werden. Fragestellungen sind hier:

- Wie viel wird getestet? Viele / wenige Systeme? Viele / wenige Daten?
- Wird ein voller Migrationszyklus getestet (inklusive Probebetrieb)?
- Anhand welcher Kriterien wird eine GO-Entscheidung gegeben?
- Wird der NO-GO-Fall (Rückstieg) geprobt?

Endergebnis sind ein Migrationsplan und ein Plan für den Ablauf der Test- und Echtmigrationen.

5.3 Durchführung der Migration

Jede Migration ist individuell, daher lassen sich an dieser Stelle nur allgemeine Grundsätze zur Durchführung der Migration geben. Diese sind aus der Erfahrung vieler Migrationsprojekte zusammengetragen worden. Die wichtigsten Punkte für Migrationen zu Cloud Services sind:

- Bauen Sie in den Migrationsplan Puffer ein und nutzen Sie diese in der Migration.
- Folgen Sie Ihrem Plan und improvisieren Sie nicht. Der Plan ist deswegen erstellt worden!
- In der Planung neigen Experten dazu, zu optimistische Durchlaufzeiten anzugeben. Schrecken Sie sich nicht, wenn die tatsächlichen Zeiten länger sind!

- Wenn Sie einen „Point-of-Decision" für das Treffen der GO / NO-GO-Entscheidung definiert haben, dann treffen Sie diese auch dort (etwaige zeitliche Puffer sollten daher vor diesem Punkt liegen).
- Nutzen Sie die Erfahrung Ihres Cloud-Anbieters, er macht die Dinge nicht zum ersten Mal. Vertrauen Sie aber auch auf Ihre interne IT. Die Wahrheit liegt bei gegensätzlichen Aussagen meist irgendwo in der Mitte.

Erwarten Sie für den ersten Betriebstag trotz aller Vorbereitung und Kommunikation ein kleines Chaos: Insbesondere ein verstärktes Supportteam und eine schnelle Eingreiftruppe haben sich für den ersten Tag danach gut bewährt. Da es sich um IT-Services handelt, ist ein Handout mit den wichtigsten Informationen ein wertvoller Begleiter der Benutzer durch die ersten Stunden nach der Migration.

5.4 Nachbereitung der Migration

Nach der erfolgreichen Migration werden kleinere Probleme und Unschönheiten zum Nachbessern bleiben. Für diese Probleme ist die Einrichtung von Frequently Asked Questions (FAQs) eine große Hilfe für die Benutzer. In der Nachbereitung liegt ebenfalls großes Augenmerk auf dem Rückbau der Alt-Infrastruktur.

Während die Migration bei vielen Projekten ausreichend geübt wird, so wird der Rückbau der Alt-Infrastruktur in vielen Fällen ohne vorherige Probe gemacht (O-Ton: „Es kann eh nichts mehr passieren"). Neben Seiteneffekten der Abschaltung von Services oder Hardware ist hierbei ein wichtiges Risiko der eventuelle Verlust von Daten. Sind diese Risiken jedoch bekannt, so kann der Rückbau in kleinen Schritten und risikovermeidend geplant, getestet und durchgeführt werden.

6 Betrieb und Cloud Controlling

Nach der Umsetzung des Cloud Services und dessen Übernahme in einen produktiven Betrieb sind die nachfolgenden Themen relevant.

6.1 Support

Der Einsatz von Cloud Services bedeutet vorrangig eine Änderung des Serviceprozesses. Diesbezüglich ist zu definieren, wie Serviceanforderungen erfasst, kommuniziert sowie möglicher Weise eskaliert werden und wer das macht. Die unterschiedlichen Möglichkeiten des Supports wurden bereits in der Auswahl des Cloud Services und des Cloud-Anbieters geklärt und sind den Anwendern zu kommunizieren.

6.2 Performance

Potenzielle Engpässe sollten einerseits durch den Cloud-Anbieter proaktiv kommuniziert und bei Bedarf durch unternehmensinterne Performancemessungen kontrolliert werden. Durch die definierten Servicelevel-Vereinbarungen ist in diesem Punkt der Serviceverantwortliche gefordert, sowohl die Einhaltung der Performance und Verfügbarkeitsgarantien zu verifizieren als auch mögliche weitere Ressourcen zu skalieren.

6.3 Verfügbarkeit

Der Service-Anbieter wird in kontinuierlichem Zyklus Patches und Updates zum Einsatz bringen. Die entsprechenden Informationen müssen vom Service-Anbieter zur Verfügung gestellt werden und sind vom Service-Kunden mit dessen Updatezyklen in Synchronisation zu bringen.

6.4 Verbesserung des Services

Für Cloud Services, die unternehmenskritische Prozesse abdecken, kann es sinnvoll sein, bereits bei der Auswahl eines Cloud-Anbieters die Anforderung und das Kriterium zu definieren, dass eine regelmäßige Evaluierung des Services stattfinden soll.

Diese Evaluierung und deren Ergebnisse können je nach Anforderung im Sinne eines Reportings (Servicelevel-Reporting, durch den Cloud-Anbieter durchgeführte Audits, durchgeführte Verbesserungen) erfolgen oder – soweit der Cloud-Anbieter diese Möglichkeit auch vorsieht – im Rahmen eines Feedbackgesprächs stattfinden. Im Meeting selbst liegt das Hauptaugenmerk auf der zukünftigen Verbesserung des Betriebes und Vermeidung

der aufgetretenen Fehler und weniger in der Feststellung, wer an den Vorkommnissen Schuld hatte.

Die Möglichkeit einer persönlichen Betreuung wird eher der Ausnahmefall sein, sollte aber bei unternehmenskritischen Services als Möglichkeit in Betracht gezogen werden. Bei Services, die von globalen Anbietern bezogen werden, sind kontinuierliche Änderungen, Erweiterungen und Verbesserungen durch das jeweilige Produktmanagement in Planung und Umsetzung. Daher ist es empfehlenswert, sich eine Kommunikationsmöglichkeit mit diesen Ansprechpartnern zu sichern.

6.5 Cloud Controlling

Das Controlling-Viereck gliedert sich in:

- Planung: Welche Messgrößen sollten welche Werte haben?
- Information: Welche Werte ergeben sich tatsächlich und wie groß ist die Abweichung zwischen Soll und Ist?
- Analyse / Kontrolle: Warum kommt es zu Abweichungen / Überschreitungen?
- Steuerung: Was tut man gemeinsam mit dem Cloud-Anbieter für eine Verbesserung?

Das Service durchläuft im Controlling-Regelkreis die vier Stufen. Idealerweise wird bei jedem Durchlauf bei Abweichungen das Gesamtsystem verbessert.

Das Service durchläuft im Controlling-Regelkreis die vier Stufen. Idealerweise wird bei jedem Durchlauf bei Abweichungen das Gesamtsystem verbessert.

Controlling-Viereck

Die Planung der geforderten Werte wird sich nach der Erstplanung nur durch eine Änderung der Anforderungen verändern. Die Information über die Einhaltung der geforderten Werte ist in der Regel vom Cloud-Anbieter zu liefern. Die Analyse und Kontrolle obliegt dem Unternehmen selbst. Die Maßnahmen selbst werden zwischen Unternehmen und Cloud-Anbieter abgestimmt und sollten auf die Einhaltung der SLAs abzielen. Die Wirksamkeit der Maßnahmen wird in der nächsten Periode überprüft.

Identifikation von Kennzahlen

Die für das Controlling von Cloud Services notwendigen Kennzahlen und Parameter sollten bereits in der Vorbereitung als „IT-Mengen" erfasst worden sein. Man kann sie ebenfalls durch ein aufmerksames Studium der Verträge mit dem Cloud-Anbieter identifizieren. Diese Parameter werden in Servicelevel Agreements (SLAs) dokumentiert und festgeschrieben.

Übliche Kennzahlen für Cloud Services sind:

- Verfügbarkeit in % der Betriebszeit des Services, aufgegliedert nach Normalarbeitszeiten, Betriebszeiten, Servicezeiten und geplanten Ausfallszeiten
- garantierte Bandbreiten für Up- und Download
- Reaktionszeiten und Wiederherstellungszeiten im Fehlerfall

Reaktionszeiten werden entsprechend definierter Fehlerklassen eingestuft, entsprechend dieser Einstufung werden die Prioritäten zur Wiederherstellung bzw. Fehlerbehandlung vom Cloud Service Provider gesetzt.

Die Verfügbarkeit eines Services wird zumeist als Verhältniszahl in Prozent mit bis zu vier Kommastellen angegeben und stellt die maximale Verfügbarkeitszeit zur konsolidierten Ausfallszeit in der jeweiligen Serviceperiode in ein Verhältnis.

Insbesondere Definitionen von der Verfügbarkeitszeit reduzierender Ereignisse sind zu beachten. Dies können unter anderen sein:

- angekündigte Wartungsfenster
- Nichtverfügbarkeit durch höhere Gewalt
- Notfallwartungsfenster, z. B. aus sicherheitsrelevanten Gründen (Denial-of-Service-Attacke, Hacker-Attacke, ...)
- Ausfälle von 3rd-Party-Systemen, die nicht im Einfluss des Auftragnehmers stehen (Internet Service Provider, ...)

Der beliebte Parameter Antwortzeit, insbesondere „garantierte Antwortzeit", sollte vermieden werden, da diese durch die Struktur des Internets nicht garantiert werden können. Nur bei der Verwendung von Spezialprotokollen kann dies garantiert werden.

Controlling-Tätigkeiten

Das wiederkehrende Controlling des Cloud Services sollte folgende Punkte zur Leistungsüberprüfung umfassen:

- Einhaltung der vereinbarten funktionalen und nicht funktionalen Leistungen. Wird der Leistungsumfang auch nach Updates und Anpassungen erfüllt?
- Werden die rechtlichen Rahmenbedingungen eingehalten? Werden die vereinbarten Parameter im Rahmen des Servicelevels eingehalten und werden die vereinbarten Messwerte geliefert?
- Werden die gelieferten Mengen korrekt verrechnet? Entsprechen die Preise den vereinbarten Preisen? Werden Index-Steigerungen korrekt vereinbart? Erfolgte die Zuordnung zu Nutzern korrekt?

Neben den eigentlichen Prüfungen der Leistung sollten insbesondere auch folgende Aspekte nicht außer Acht gelassen werden:

- Periodische Prüfung der Anbieterbewertung: Haben sich die Eigentumsverhältnisse des Cloud-Anbieters geändert? Gab es grobe Änderungen im Nutzerfeedback? Kam es zu Sicherheitsvorfällen?
- Periodische Überprüfung der Wettbewerbsfähigkeit des Vertrages: Bietet der Cloud-Anbieter günstigere Konditionen / mehr Leistung? Gibt es im Bereich des Services technische Neuerungen, die zu günstigeren Konditionen im Markt führen?

Die getroffenen Maßnahmen im Cloud Controlling sichern die Leistungsfähigkeit des Services und damit die Realisierung des Nutzens für das Unternehmen. Ein erfolgreiches Controlling kann den Weg für die Umsetzung von weiteren Cloud Services eröffnen und sicherstellen, dass die gesetzten Erwartungen eintreffen.

Die getroffenen Maßnahmen im Cloud Controlling sichern die Leistungsfähigkeit des Services und damit die Realisierung des Nutzens für das Unternehmen. Ein erfolgreiches Controlling kann den Weg für die Umsetzung von weiteren Cloud Services eröffnen und sicherstellen, dass die gesetzten Erwartungen eintreffen.

7 Checkliste Vertragselemente

In Anlehnung an das StarAudit werden die wichtigsten Fragen hinsichtlich der vertraglichen Ausgestaltung angeführt. Abgeleitet werden die Fragen aus den Prüfkriterien des Gütesiegels. Weitere rechtliche Informationen können den EuroCloud Leitfäden entnommen werden.

Anbieter, die sich einem StarAudit (als Zertifizierung) unterzogen haben, erfüllen die Anforderungen für die Bereitstellung von vertrauenswürdigen Cloud Services in den Bereichen Software, Plattform und Infrastruktur entsprechend dem gewählten Qualitätslevel, wobei die Güteaussagen in drei Qualitätsstufen (3, 4 und 5 Sterne) differenziert werden.

7.1 Vertragsabschluss und Vertragsgestaltung

Der Vertrag bedarf für seine Wirksamkeit der Schriftform, wobei ebenso ein Online-Abschluss mit qualifizierter elektronischer Signatur möglich ist.

Zu beachten ist, dass die im Datenschutzgesetz geregelten Pflichten des Dienstleisters kraft Gesetzes gelten. Soweit der Umgang mit personenbezogenen Daten betroffen ist, bedarf es einer detaillierten Beschreibung. Die Leistungsbeschreibung des Auftragsgegenstandes muss nur grob ausgeführt werden.

Für Vereinbarungen mit Anbietern, deren Sitz und Leistungserbringung im Europäischen Wirtschaftsraum und/oder in der EU erfolgt, gelten die Datenschutzregelungen und Anforderungen der privilegierten Dienstleistungsverhältnisse.

Bei Beauftragung von Anbietern außerhalb von EU und/oder EWR müssen zusätzliche Anforderungen erfüllt werden, die z. B. durch den von der Europäischen Union abgesegneten Standardvertrag zur Auftragsdatenverarbeitung geregelt werden (sog. „Standard Contract Clauses“ für „Data Processing“). Dies ist insbesondere bei der Nutzung von Subunternehmern zu beachten, da die Geschäftsmodelle der Cloud-Service-Dienstleister zumeist selbst die Möglichkeiten von Cloud Services nutzen.

7.2 Leistungsverrechnung

- Wird die Nutzung des Services pauschal zeitabhängig berechnet?
- Wird die Nutzung des Services nach Verbrauch berechnet?
- Existieren Mengenrabatte/unterschiedliche Tarife in Abhängigkeit von der

abgenommenen Servicemenge?

- Kann der Auftragnehmer seinen Tarif bei signifikanter Änderung des Nutzungsumfangs ändern?
- Gibt es eine Best-Price-Option?
- Wird optional eine Flatrate oder per-user-Flatrate angeboten?
- Gibt es extra zu verrechnende Sonderleistungen?

7.3 Leistungsstörungen

Leistungsstörung beim Auftragnehmer oder dessen Unterauftragnehmern

- Bestehen Regelungen zum Schadenersatz bei Leistungsstörungen?

Streit über Leistungserbringung/Zahlungsverzug

- Ist ein Zurückbehaltungsrecht an Daten des Auftraggebers oder ihm gegenüber zu erbringenden Leistungen vertraglich ausgeschlossen?
- Ist auch im Fall von Streitigkeiten zur Leistungserbringung oder bei Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?

7.4 Vertragskündigung

Welche Kündigungsfristen sind für den Auftraggeber und den Auftragnehmer definiert?

Gibt es eine demonstrative Liste der möglichen (außerordentlichen) Kündigungsgründe?

Wenn ja, für wen?

- Auftraggeber
- Auftragnehmer

Ist eine Vorankündigung von Änderungen bei der Diensterbringung von Subunternehmern vertraglich geregelt?

Existieren Regelungen zur Mitwirkung des Auftragnehmers bei der Datenbereitstellung nach einer Vertragskündigung?

7.5 Insolvenz des Auftragnehmers

Existieren Regelungen zum Schutz der Daten des Auftraggebers und der Verfügbarkeit der

Anwendung bei Insolvenz des Auftragnehmers?

- Besteht eine angemessene Betriebsgarantie durch Sicherungszusage an dritte zentrale Leistungserbringer (z. B. Rechenzentrumsbetreiber)?
- Ist die Datenportabilität spezifiziert und können die Kundendaten verlustfrei exportiert werden?
- Wird dem Auftraggeber ein Recht auf Herausgabe der letzten Datensicherung und Dokumentation eingeräumt?

7.6 Compliance

Datenarchivierung

- Es gibt eine Reihe von Sondernormen zu unternehmens- und steuerrechtlichen Aufbewahrungspflichten und Aufbewahrungsfristen bei der Verwendung von Datenträgern, so etwa die §§ 189, 190, 212 und 216 UGB sowie die §§ 131 und 132 BAO. Sowohl nach § 212 Abs. 1 UGB als auch nach § 132 Abs. 1 BAO beträgt die Aufbewahrungsfrist grundsätzlich 7 Jahre. Im Fall von SaaS muss somit bei elektronischer Verarbeitung und Archivierung beim SaaS-Anbieter sichergestellt sein, dass die betroffenen Daten (etwa elektronische Rechnungen, Bücher, Aufzeichnungen und sonstige Unterlagen) während der gesetzlichen Aufbewahrungsfristen sicher aufbewahrt werden und deren vollständige, geordnete und inhaltsgetreue Wiedergabe, auch an die Behörden, möglich ist. Weiters muss ein Prozess einer kontinuierlichen Rückübermittlung solcher Daten an den Auftraggeber gewährleistet sein.

Datenschutzrelevanz

- Werden innerhalb der Anwendung personenbezogene Daten im Sinne des DSG verwendet?

Zu beachten ist, dass der Begriff der „personenbezogenen Daten“ im Sinne des DSG sehr weit gefasst ist. Alle Daten, die einen Personenbezug haben oder bei denen der Auftraggeber, der Auftragnehmer oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht der Datenschutzbehörden als „personenbezogene Daten“, und zwar sowohl bezüglich natürlicher als auch bezüglich juristischer Personen. In der Praxis wird es nur sehr wenige IT- und Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

Datenschutzorganisation

- Ist die Datenverwendung – soweit erforderlich – beim Datenverarbeitungsregister (DVR) registriert?
- Sind die Mitarbeiter des Auftragnehmers nachweislich zur Einhaltung des Datengeheimnisses nach § 15 DSG verpflichtet?
- Ist geregelt, welche Seite gegenüber den Kunden des Auftraggebers den Ansprechpartner für den Datenschutz darstellt?
- Sind Regeln für die Berichtigung, Löschung und Sperrung von Daten auf Antrag eines Betroffenen definiert?

Auswahl Auftragnehmer und Subunternehmer

- Bietet der Auftragnehmer genügend Informationen zu seinem Unternehmen und seinen Unterauftragnehmern, um dem Auftraggeber eine fundierte Auswahl des Auftragnehmers gemäß § 10 DSG zu ermöglichen?
- Werden die Unterauftragnehmer bekanntgegeben?

Datenschutzniveau

- Ist – soweit einschlägig – auch außerhalb der EU (auch bei beteiligten Unterauftragnehmern) ein angemessenes Datenschutzniveau (z. B. über EU-Standardvertrag) hergestellt?
- Besteht die Möglichkeit, wenn aufgrund von gesetzlichen oder behördlichen Auflagen an den Auftraggeber erforderlich, die Orte der Datenhaltung auf einzelne Länder oder die EU einzugrenzen?

Beauftragung und Weisungsrecht

- Sind die Verantwortlichkeiten zwischen Auftraggeber (grundsätzliche datenschutzrechtliche Verantwortlichkeit) und Auftragnehmer (Umsetzung von Weisungen, technischen Schutzmaßnahmen etc.) sauber definiert?
- Ist der Umfang des Auftrags zur Datenverarbeitung hinreichend klar spezifiziert, insbesondere:
- Ist der Dienst grob beschrieben? Sind in der Beschreibung der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen dokumentiert?

- Sind die Dauer der Verarbeitung und die Löschung der Daten exakt definiert?
- Ist ein Entscheidungsspielraum des Dienstleisters zur Verarbeitung der Daten ausgeschlossen?
- Ist dokumentiert, ob und, wenn ja, wie sensible Daten im Sinne des § 4 Z 2 DSG erhoben, verarbeitet oder genutzt werden?
- Ist das Weisungsrecht des Auftraggebers eindeutig definiert?

Kommunikation

- Ist eine Kommunikationsregel etabliert für den Fall, dass Weisungen des Auftraggebers nach Meinung des Auftragnehmers gegen den Datenschutz verstoßen?
- Sind Sachverhalte definiert, die als mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen dem Auftraggeber angezeigt werden müssen?

Umsetzung technischer und organisatorischer Datenschutzmaßnahmen

- Existiert eine Dokumentation/ein Konzept, welche technischen und organisatorischen Maßnahmen umgesetzt werden, um die Vorgaben des Anhangs zu § 14 DSG zu erfüllen?
- Hat der Auftraggeber diesem Konzept (und Änderungen daran) zuzustimmen?

Kontrollmöglichkeiten des Auftraggebers

- Existieren Regelungen zu Kontrollrechten des Auftraggebers und zu den entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, insbesondere:
- Ist ein Kontrollrecht des Auftraggebers und/oder eines vom Auftraggeber beauftragten Dritten vor Ort beim Auftragnehmer oder seinen Subauftragnehmern ausdrücklich vereinbart?
- Existieren (kumulativ oder alternativ zu Kontrollen durch den Auftraggeber) regelmäßige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Auftragnehmer und die Verpflichtungen gegenüber dem Auftraggeber kontrollieren und zertifizieren?

- Ist eine Regelung zur Mitwirkung des Auftragnehmers und zu den dadurch entstehenden Kosten getroffen?

Datenlöschung bei Vertragsende

- Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags?
- Wird gewährleistet, dass die Daten auf Wunsch des Auftraggebers tatsächlich gelöscht werden?

8 Glossar Cloud Computing

1. Was ist unter Cloud Computing zu verstehen?

„Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Folgende fünf Eigenschaften charakterisieren gemäß der NIST-Definition ein Cloud Service:

- On-demand Self Service: Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service Provider ab.
- Broad Network Access: Die Services sind mit Standardmechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
- Resource Pooling: Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant-Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
- Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
- Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

2. Bereitstellungs- und Bezugsfunktionen von Cloud Services

Es existieren vielfältige Möglichkeiten der Bereitstellung und des Bezugs von Cloud-Computing-Leistungen. Daher ist zwischen den folgenden Rollen zu differenzieren:

1. Bereitstellung

» Cloud-Service-Anbieter – Unternehmen, das die Cloud-Leistungen gegenüber dem Kunden als Vertragsgeber anbietet.

- Cloud-Service-Subunternehmer – Vorlieferant von Cloud Services, die vom Cloud-Service-Anbieter als Teilfunktion integriert werden.
- Cloud (Managed) Hosting Provider – Cloud-Service-Subunternehmer, der technische IT-Leistungen, die dem klassischen IT-Outsourcing entsprechen (Rechner, Speicher, Netzwerk), erbringt und die nicht als vollwertige Cloud-Service-Leistung bezogen werden.
- Co-Location Provider – Vorlieferant von Infrastrukturkomponenten, der Gebäude, Strom, Klima, Kommunikation etc. als Grundversorgung bereitstellt.
- Cloud-Service-Vermittler – Unternehmen, das für den Cloud-Service-Anbieter Kunden wirbt (und rechtlich die Stellung eines Handelsvertreters einnimmt).
- Cloud Service Reseller – Wiederverkäufer von Cloud Services, der selbst keine Anpassung des Cloud Services erbringt, sondern sämtliche Leistungen der Serviceerbringung vom Cloud-Service-Anbieter bezieht (und rechtlich als Vertragshändler zu qualifizieren ist).
- Cloud-Lösungsanbieter – Cloud Service Reseller, der mehrere Cloud Services bündelt und als integriertes Paket weiterverkauft.

> Der Begriff „Broker“ wird hier bewusst nicht verwendet, da dieser im Markt in unterschiedlichen Bedeutungen verwendet wird, d. h. sowohl im Sinne von Vermittler als auch im Sinne von Lösungsanbieter.
>
> Auch der Begriff „Marktplatz“ wird im Markt in unterschiedlichen Bedeutungen verwendet, d. h. im Sinne von „Vermittler“ oder „Reseller“.

2. Bezug

- Cloud-Service-Abnehmer –Vertragspartner des Cloud-Service-Anbieters, der als Unternehmen das Service nutzen will.
- Cloud-Service-Nutzer – einzelner Benutzer eines Cloud Services, in der Regel ein Arbeitnehmer des Cloud-Service-Abnehmers.
- Cloud-Service-Administrator – Fachbereich des Cloud-Service-Abnehmers, der mit der Verwaltung von Identitäten und Nutzungsoptionen des Cloud Services betraut ist.

3. Cloud Services und deren Eigenschaften

Als weitere typische Eigenschaften für ein Cloud Service treten häufig die folgenden

Merkmale auf:

- Selbstverwaltung des Services und der damit verbundenen Leistungen durch den Anwender.
- Technisch uneingeschränkter Netzwerkzugriff mit Standardanwendungen (z. B. Web-Browser) des Anwendergerätes (z. B. Notebook, Smart Phone).
- Multimandantennutzung der technischen Ressourcen, zumeist über ganze Rechenzentrumsbereiche oder mehrere verteilte Rechenzentren als Ressourcenpool.
- Unmittelbare Elastizität, das heißt die automatische Bereitstellung von technischen Ressourcen aus dem Ressourcenpool bei Spitzenanforderungen oder Erweiterung der Zahl der Benutzer.
- Kontinuierliche Messung der tatsächlichen Nutzung pro Mandant und leistungsgerechte Abrechnung.

4. Cloud Services und Betriebsmodelle

Bei der Bereitstellung von Cloud Services gibt es zwei Unterscheidungsebenen, die Art der Cloud Services und die verschiedenen Betriebsmodelle, die in freier Kombination verwendet werden können.

Bei der Bereitstellung von Cloud Services unterscheidet man in erster Linie drei Arten:

- SaaS – Software as a Service

  Sämtliche Angebote von Anwendungssoftware, die den Kriterien des Cloud Computings entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

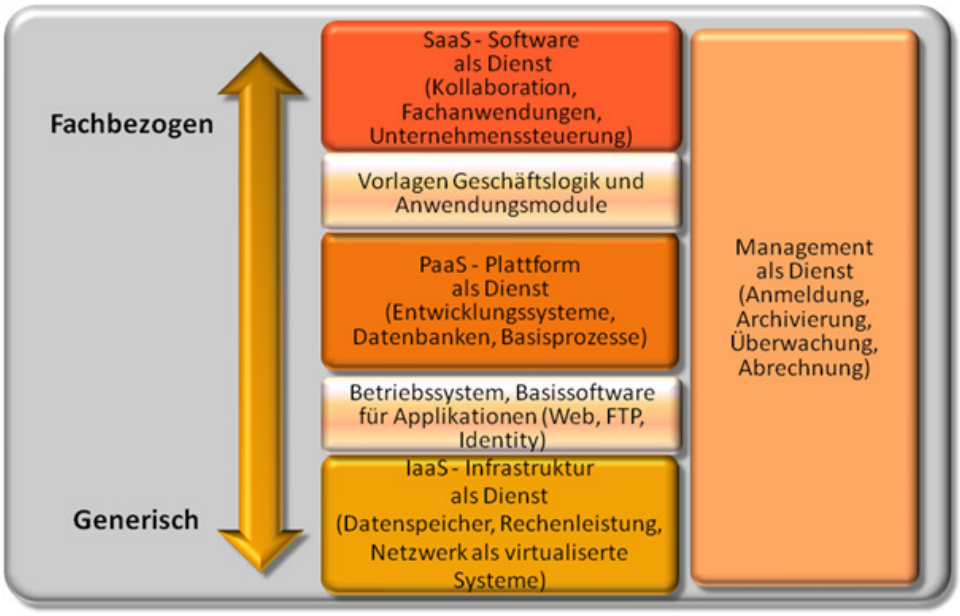
- PaaS – Platform as a Service

  Ein PaaS-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. als Service zur Verfügung stellen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen,

für deren Entwicklung der PaaS-Anbieter in der Regel eigene Werkzeuge anbietet. Als Beispiel kann force.com der Firma Salesforce oder Azure der Firma Microsoft genannt werden.

- IaaS – Infrastructure as a Service

  Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Service angeboten. Ein Cloud-Service-Abnehmer kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Service-Abnehmer z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.



Daneben gibt es weitere Ausprägungen als Sonderform, wie zum Beispiel Security, Business Process, Storage, Monitoring oder Communication as a Service, die zusammenfassend oftmals auch als XaaS benannt werden.

Cloud-Betriebsmodelle

Bei den Betriebsmodellen ist zu unterscheiden, wer der Betreiber ist und wer generell Zugriff auf die Services hat:

Private Cloud: Dedizierte Bereitstellung der Services für einen definierten Kunden unter Verwendung von abgrenzbaren Hardware-Ressourcen (also in der Regel Rechenzentren, abgeschlossene Bereiche innerhalb des Rechenzentrums) und Netzwerkbereiche, die nicht von Dritten genutzt werden.

Virtual Private Cloud: Im Gegensatz zur Private Cloud erfolgt die Mandantenabgrenzung lediglich auf der logischen Netzwerkebene bei gleichzeitiger Nutzung der Hardware über mehrere Kunden.

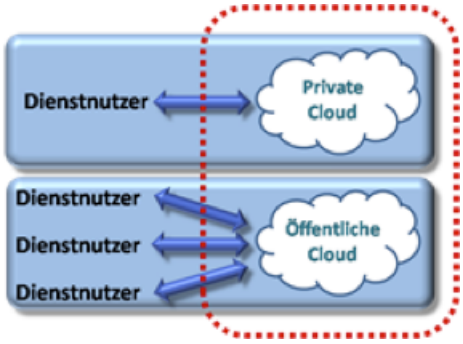
Öffentliche Cloud: Generelle Bereitstellung der Services für einen unbeschränkten Kundenkreis, der Hardware-Ressourcen gemeinschaftlich nutzt. Die von den Kunden in Anspruch genommenen Cloud-Leistungen werden mittels logischer Mandantenzuordnung separiert.

Daneben existieren noch Sonderformen wie:

Community Cloud: Kombination mehrerer Cloud Services für bestimmte Anwendergruppen. Dies kann zum Beispiel im Bereich Logistik, Fertigung, Forschung oder Branchenvereinigungen definiert werden. Der Zugang ist nicht öffentlich, sondern erfordert zusätzliche Autorisierung durch die Betreiber der Community Cloud. Die an einer Community Cloud teilnehmenden Unternehmen haben meist ähnliche Anforderungen an Verfügbarkeit, Compliance und Sicherheit der bereitgestellten Ressourcen. Als Beispiel seien hier Banken oder Regierungsstellen genannt.

Hybrid Cloud: Kombination von Private und Public Cloud. Hierbei erfolgt ein kombinierter Betrieb von Cloud Services, bei denen ein Teil in einer privaten Umgebung (zum Beispiel ein ERP-System) und ein Teil aus einem öffentlichen Bereich (z. B. CRM) technisch und logisch zusammengeführt werden. Ein Beispiel für die Entstehung einer Hybrid Cloud ist die Verlagerung einer öffentlichen Firmenwebseite aus der Private Cloud in die Public

Cloud. Da die Firmenwebseite ohnehin aus dem Internet erreichbar sein muss, kann eine Verlagerung in die Public Cloud unter Umständen sogar für höhere Sicherheit sorgen



9 Rechtlicher Hinweis

9.1 Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung spezieller rechtlicher Aspekte im Zusammenhang mit Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

9.2 Inhalt des Leitfadens

Der Herausgeber/die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen den Herausgeber/die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

9.3 Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z. B. „Links"), die außerhalb des Verantwortungsbereichs des Herausgebers/der Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem der Herausgeber/die Autoren von den Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Der Herausgeber/die Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben der Herausgeber/die Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotenen Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht derjenige, der über Links auf die jeweilige Veröffentlichung lediglich verweist.

9.4 Urheberrecht

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Graphiken oder Bilder sind nach dem österreichischen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

9.5 Vergütung

Dieser Leitfaden wird den Adressaten/Empfängern kostenlos zur Verfügung gestellt.

10 Autoren

Die Autoren dieses Leitfadens sind:

Dr. Tobias Höllwarth

Sourcing International
Palais Savoy, Johannesgasse 15
1010 Wien, Osterreich

E-Mail: tobias.hoellwarth@sourcing-international.org
Web: www.sourcing-international.org

Dipl. Ing. Ulrike Huber
Partner

42virtual Business Services GmbH, Wien

E-Mail: ulrike.huber@42virtual.com
Web: www.42virtual.com

Michael Kramer
Senior Consultant

42virtual Business Services GmbH, Wien

E-Mail: michael.kramer@42virtual.com
Web: www.42virtual.com

Dr. Christian Laux, LL.M.

LAUX LAWYERS AG

E-Mail: christian.laux@lauxlawyers.ch
Web: www.lauxlawyers.ch

Oliver Lindlbauer

Sourcing International
Palais Savoy, Johannesgasse 15
1010 Wien, Osterreich

E-Mail: oliver.lindlbauer@sourcing-international.org
Web: www.sourcing-international.com

Dr. Werner Schönfeldinger
Partner

42virtual Business Services GmbH, Wien

E-Mail: werner.schoenfeldinger@42virtual.com
Web: www.42virtual.com

Andreas Weiss
CEO

ICTAN GmbH
Montnausstr. 86a
D-41515 Grevenbroich

E-Mail: andreas.weiss@ictan.eu
Web: www.ictan.eu

SOURCING | INTERNATIONAL
Digital Transformation Advisors

Sourcing International

Palais Savoy, Johannesgasse 15
1010 Wien, Osterreich

E-Mail: office@sourcing-international.org
Web: www.sourcing-international.org