Thorsten Pröhl, Jonas Repschläger, Koray Erek, Rüdiger Zarnekow

IT-Servicemanagement im Cloud Computing

Cloud Computing stellt einen fundamentalen Trend in der IT-Branche dar, der bei IT-Entscheidern sowohl positive als auch kritische Reaktionen hervorruft. Insbesondere werden der praktische Nutzen, die Datensicherheit sowie das für Unternehmen spezifische Anwendungsszenario nach wie vor kontrovers diskutiert. Der Bezug von Cloud-Services kann weitreichende Prozessveränderungen im IT-Servicemanagement (ITSM) zur Folge haben. Dabei ist aus Anwendersicht vor allem die zunehmende Bedeutung der Phasen Service Strategy und Service Design hervorzuheben. Demgegenüber ist zu erwarten, dass im Rahmen des Cloud Computing die Phasen Service Transition und Service Operation für die Leistungsabnehmer an Relevanz verlieren. Derweilen bleibt das Continual Service Improvement unverändert wichtig.

Inhaltsübersicht

1 Cloud-Services und IT-Servicemanagement

Kleinen und mittleren Unternehmen steht eine große Auswahl an Public-Cloud-Angeboten zur Verfügung [Repschläger et al. 2012]. Große Unternehmen bevorzugen häufig abgeschlossene Private-Cloud-Lösungen, um so Compliance-Richtlinien einzuhalten und einen Kontrollverlust zu vermeiden [Geczy et al. 2012; KPMG 2012; Marston et al. 2011; BITKOM 2010]. Dem Geschäftsbereich sind ein kostengünstiger IT-Betrieb und ein hohes Maß an Flexibilität wichtig [Rawal 2011]. In diesem Zusammenhang gewinnt das Management von IT-Services zunehmend an Bedeutung. Für die unternehmensinterne IT-Organisation und deren Ablaufsteuerung hat sich im IT-Servicemanagement das Framework ITIL (IT Infrastructure Library) als Defacto-Standard mit einer Ansammlung von Best Practices etabliert [Bause 2009]. Insbesondere liefert es »... Leitlinien für die Bereitstellung von IT-Services und zu den Prozessen, die für die Unterstützung von Geschäftsbereichen erforderlich sind« [APMG 2011].

Viele Unternehmen stehen dem Thema Cloud Computing aufgeschlossen und interessiert gegenüber [KPMG 2012]. Der Bezug von Cloud-Services kann hierbei fundamentale Prozessveränderungen im IT-Servicemanagement zur Folge haben. ITSM-Prozesse können komplett in die Verantwortung des Anbieters übergehen. Je nach Umfang der Cloud-Nutzung unterliegen auf Anwenderseite die prozessbezogenen Aktivitäten in der internen IT-Organisation kleinen bis sehr großen Änderungen. Vor diesem Hintergrund sollen in diesem Beitrag die folgenden Fragen adressiert werden:

- Wie verändert sich die Bedeutung von IT-Servicemanagementprozessen im Cloud Computing am Beispiel von ITIL aufseiten des Leistungsabnehmers?
- Welches Änderungspotenzial besitzen die bestehenden ITIL-Prozesse für den Leistungsabnehmer im Cloud Computing?

Für die weiteren Betrachtungen wird davon ausgegangen, dass der Leistungsabnehmer und der

Leistungsanbieter ein IT-Servicemanagement nach ITIL implementiert haben (vgl. Abb. 1). Des Weiteren werden nur die Auswirkungen auf die ITIL-Prozesse im Rahmen einer Cloud-Service-Nutzung betrachtet. Marktstudien belegen, dass Cloud-Services hauptsächlich ergänzend zu bestehenden Lösungen und internen Systemen eingesetzt werden. Deshalb legen wir die Annahme zugrunde, dass das abnehmende Unternehmen nur einen Teil seiner IT-Services und -Ressourcen aus der Cloud bezieht.

2 Grundlagen

Cloud Computing ist ein aktueller Trend für viele Unternehmen. Es stellt eine Ansammlung von IT-Services und -Ressourcen dar, die dem Kunden flexibel und skalierbar über das Internet angeboten werden können, ohne eine langfristige Kapitalbindung und IT-spezifisches Know-how vorauszusetzen. Der Kunde kann, abhängig von der vertikalen Integrationstiefe, sowohl komplette Softwareanwendungen als auch nur die notwendige IT-Infrastruktur beziehen. Auf der untersten Ebene »Infrastructure as a Service« (IaaS) wird dem Kunden eine flexible IT-Infrastruktur, die sowohl nach oben als auch nach unten skaliert werden kann, zur Verfügung gestellt. Auf einer darüber liegenden Ebene »Platform as a Service« (PaaS) existieren Plattformen, die Schnittstellen zur Cloud-Infrastruktur und Tools für die Entwicklung von Cloud-Anwendungen bereitstellen. Auf der obersten Ebene »Software as a Service« (SaaS) werden komplette Anwendungen, wie z. B. Customer-Relationship-Management-(CRM-) oder Enterprise-Resource-Planning-(ERP-)Lösungen, angeboten. Cloud-Computing-Dienste lassen sich nach dem National Institute of Standards and Technology (NIST) im Wesentlichen durch die folgenden fünf Merkmale charakterisieren [Mell & Grance 2011]:

- Services sind ubiquitär über ein Netzwerk durch einen standardisierten Zugriff erreichbar (»Broad Network Access«).
- Es wird ein gemeinsamer, standortunabhängiger Pool aus multimandantenfähigen,

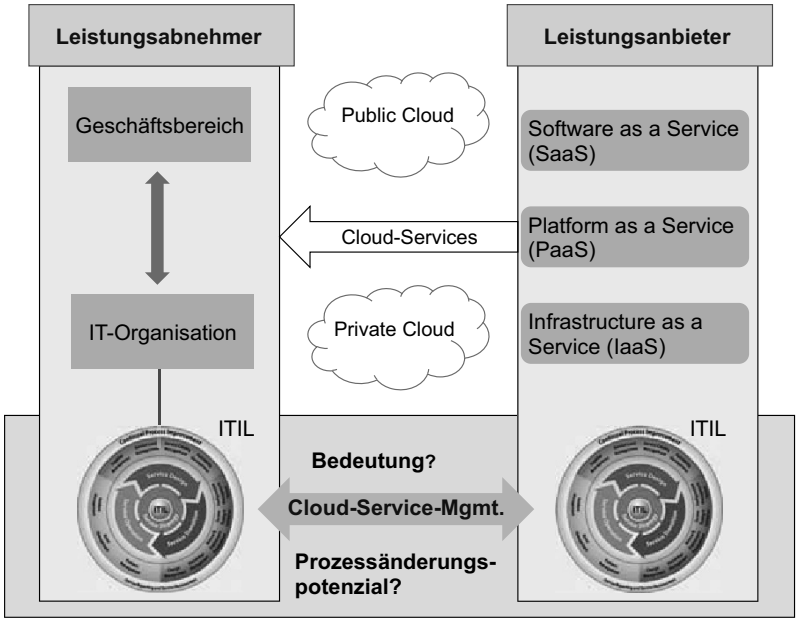


Abb. 1: Anwendungsszenario Cloud-Services und ITIL

virtualisierten Ressourcen verwendet (»Resource Pooling«).
- IT-Ressourcen können bedarfsorientiert und flexibel nach oben oder unten skaliert werden (»Rapid Elasticity«).
- Es findet eine verbrauchsorientierte Messung und Abrechnung der Leistungen statt (»Measured Service«).
- Die Servicebeschaffung erfolgt nutzergetrieben auf Abruf (»On-Demand Self-Service«).

3 Portfolio des Cloud-Service-Managements

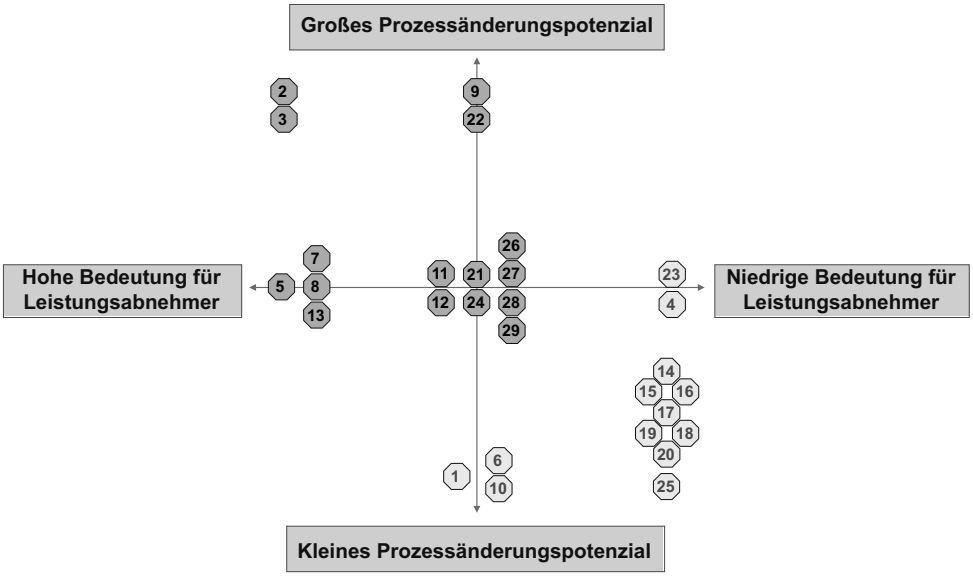
Der zunehmende Bezug von Cloud-Services in IT-Organisationen kann zu einer Veränderung der Bedeutung von ITIL-Prozessen beim Leistungsabnehmer führen. Gleichzeitig schafft die Einführung von Cloud-Services ein wesentliches Potenzial zur Prozessänderung. Darunter fallen Änderungen bei bestehenden Prozessen durch typische Formen des Reengineerings (z. B. Automatisierung, Eliminierung oder Parallelisierung von Prozessschritten). Es bestehen Unterschiede zwischen traditionellen IT-Services und den Cloud-Services. Dies lässt sich u.a. anhand der fünf NIST-Merkmale bemessen, die das Prozessänderungspotenzial der ITSM-Prozesse beeinflussen.

Unternehmen, die Cloud-Services nutzen, müssen im Rahmen des IT-Servicemanagements mit einer Prozessveränderung hinsichtlich Bedeutung und Ablauf rechnen (vgl. Abb. 2). Hierbei ist absehbar, dass die Phasen des Service Design und der Service Strategy an Bedeutung gewinnen. Aufgrund von hoher Standardisierung und Automatisierung bei Cloud-Services werden der Betrieb (Service Operation) und die Überführung (Service Transition) von IT-Services vereinfacht und können somit an Bedeutung verlieren. Für den Leistungsabnehmer wird es im Cloud Computing zunehmend wichtiger, den Einsatz von Services zu planen und strategisch im Unternehmen auszurichten. Insbesondere die Service-Strategy-Phase muss die individuell unterschiedlichen Potenziale des Cloud Computing nutzbar machen und die Herausforderungen verstehen. Als übergreifender Prozess zur nachhaltigen Verbesserung ist das Continual Service Improvement (CSI) im Rahmen des Cloud Computing für den Leistungsabnehmer sehr wichtig. Allerdings nimmt durch die Verlagerung von Aufgaben und Ressourcen der Einflussbereich an dieser Stelle ab.

4 Prozessbedeutung im Cloud Computing am Beispiel von ITIL

Um das Änderungspotenzial für die fünf Phasen des ITIL-Servicelebenszyklus im Cloud Computing diskutieren zu können, werden die ITIL-Prozesse näher beschrieben, die eine hohe Bedeutung oder/und eine maßgebliche Veränderung erfahren (in Abb. 2 die farblich dunkelgrau markierten Prozesse).

Das *Service Portfolio Management (2)* ist für die Verwaltung des Serviceportfolios zuständig und kümmert sich dabei um die richtige Zusammensetzung der IT-Services. Im Rahmen eines Cloud-Portfolios existieren klar definierte Bausteine (Services), sodass eine flexible Orchestrierung möglich ist [Cannon et al. 2011]. Hierbei entsteht ein großes Änderungspotenzial durch die sogenannten Self Services, die dem Leistungsabnehmer standortunabhängig und automatisiert zur Verfügung gestellt werden. Ebenso wird das Serviceportfolio durch die Anforderungen der Geschäftsbereiche beeinflusst, indem neue Cloud-Services vorgeschlagen werden. Infolgedessen ist eine schnelle Aktualisierung des Portfolios möglich, die den Bedarfen des Geschäftsbereichs genügt. Eine ganzheitliche Überwachung der Servicenutzung gestaltet sich bei Cloud-Services schwierig, da die Einflussmöglichkeiten der IT-Organisation nur beschränkt vorhanden sind (vgl. Beitrag zur »Schatten-IT« [Zimmermann & Rentrop 2012] in diesem Heft). Besonders die Folgen bei der Ablösung und der Abschaltung von Services stellen Unternehmen vor neuartige Herausforde-



Service Strategy

1) Strategy Management for IT Services
2) Service Portfolio Management
3) Financial Management for IT Services
4) Demand Management
5) Business Relationship Management

Service Design

6) Design Coordination
7) Service Catalogue Management
8) Service Level Management
9) Capacity Management
10) Availability Management
11) IT Service Continuity Management
12) Information Security Management
13) Supplier Management

Service Transition

14) Change Management
15) Change Evaluation
16) Transition Planning and Support
17) Release and Deployment Management
18) Service Validation and Testing
19) Service Asset and Configuration Management
20) Knowledge Management

Service Operation

21) Event Management
22) Incident Management
23) Request Fulfilment
24) Access Management
25) Problem Management

CSI

26) Service Review
27) Process Evaluation
28) Definition of CSI Initiatives
29) Monitoring of CSI Initiatives

Abb. 2: Portfoliodarstellung des Cloud-Service-Managements

rungen (»Retired Services«). Dabei gilt es, Fragen in Bezug auf Datenhaltung, -archivierung und -löschung, z.B. bei IaaS-Angebot wie Dropbox, zu beantworten.

Das *Financial Management for IT Services (3)* kümmert sich um die Finanzplanung, -analyse, -reporting und die Leistungsverrechnung der IT-Services [itSMF 2010; Cannon et al. 2011]. Gerade Cloud-Services werden unter der Prämisse eingesetzt, dass sich Kostenersparnisse ergeben [Marston et al. 2011]. Eine transparente Kostenaufschlüsselung wird durch eine verbrauchsorientierte Abrechnung im Cloud Computing gewährleistet, sodass nur die tatsächlich abgerufene Leistung vom Geschäftsbereich bezahlt wird [Fry 2010]. Die interne Fakturierung von selbst gebuchten Cloud-Services, z.B. dem SaaS-Angebot Sales Cloud von Salesforce, setzt voraus, dass die Rechnungsinformationen zwischen Leistungsanbieter und -abnehmer in elektronischer Form (z.B. EDIFACT) ausgetauscht werden. Somit finden weitreichende Prozessänderungen statt, um im Cloud Computing eine flexible und kurzfristige Abrechnung von Services zu ermöglichen. Bei dem Modell der Community Cloud (gemeinsame Benutzung von Ressourcen durch die Mitglieder) gilt es, geeignete Abrechnungsmechanismen zu definieren, die eine konsolidierte Leistungsverrechnung für den virtuellen Ressourcenpool der Community sicherstellen.

Das *Business Relationship Management (5)* pflegt Kundenbeziehungen, führt Umfragen zur Zufriedenheit durch und kümmert sich um die Anforderungen des Geschäftsbereichs. Aufgrund von geringfügigen Restriktionen, die bei der Nutzung gelten (z.B. Firewall-Einstellungen), ist der Zugriff auf externe Daten und Anwendungen außerhalb des geschlossenen Systems möglich. Hierbei stellt sich die Frage, inwieweit die IT-Organisation die Cloud-Services unterstützt oder gemäß unternehmensinterner Compliance-Vorgaben strikt ablehnt. Zum anderen wird es im Rahmen des Cloud Computing für Geschäftsbereiche zunehmend einfacher, IT-Services direkt zu bestellen. Dies führt dazu, dass sich viele kleine Insellösungen sowohl bei Applikationen als auch bei Endgeräten im Unternehmen etablieren, die allerdings nicht von der IT-Organisation unterstützt bzw. an die notwendigen Unternehmensanforderungen angepasst werden können. Dieses Phänomen stellt eine Herausforderung für viele IT-Organisationen dar, die den Anforderungen der Geschäftsbereiche nur begrenzt entgegenkommen. Durch klar definierte Servicepakete im Cloud Computing ist eine transparente Kommunikation zwischen der IT-Organisation und dem Geschäftsbereich möglich, die durch eine hohe Nutzerzentrierung und -integration begünstigt wird.

Das *Service Catalogue Management (7)* plant, entwickelt und pflegt den Servicekatalog der IT-Organisation. Durch den Einsatz von Cloud-Services steigt die Bedeutung des Servicekatalogs, da es zum zentralen Planungsinstrument wird und so der »Schatten-IT« entgegenwirken kann [Cannon et al. 2011]. Im Idealfall werden die Service Level Agreements (SLAs) der Cloud-Services automatisiert übernommen (Importschnittstelle/standardisierter Datenaustausch), sodass sich ein mittleres Prozessänderungspotenzial ergibt. Gerade die automatisierte Informationsbeschaffung stellt den Leistungsabnehmer vor große Herausforderungen, da Cloud-Services standardisiert und je nach Cloud-Ebene nur begrenzt über existierende Schnittstellen anzusprechen sind. In den Fällen, in denen Informationen automatisch ausgelesen werden können, ist der Informationsgehalt auf grundlegende, meist technische Daten beschränkt (Latenzzeit, Status der virtuellen Maschine, Anzahl der Nutzer etc.) [Labes et al. 2012]. Eine Überprüfung von SLAs oder des Orts der Datenverarbeitung ist nicht möglich. Zudem wird eine Überwachung von Cloud-Services in verteilten und globalen Nutzungsszenarien wesentlich komplexer.

Durch das *Service Level Management (8)* werden SLAs mit den Geschäftsbereichen ausgehandelt. Bei dem Bezug von Cloud-Services müssen alle Parameter des Service Design, wie beispielsweise Verfügbarkeiten und Kapazitäten, in die Verträge aufgenommen und im Prozess überwacht werden. In den Verträgen sollten Kennzahlen für die Anwendungen (End-to-End-Service-Levels) berücksichtigt werden, da diese eine höhere Aussagekraft besitzen [Morin et al. 2012; itSMF 2010]. Bei (Public-)Cloud-Services gibt es in der Regel nur standardisierte SLAs [BITKOM 2010], die durch das Service Level Management an den Geschäftsbereich weitergereicht werden. Damit eine angemessene Servicequalität gewährleistet werden kann, gilt es, diese zu überwachen und Verantwortlichkeiten für die Cloud-Services zu bestimmen, die die Kompetenzen und die Machtbefugnis haben, Serviceveränderungen durchzusetzen. Im Cloud Computing wird es zunehmend wichtiger, mehrere Provider und deren Services zu steuern und zu überwachen. Durch die Vielzahl von Cloud-Providern bietet sich ein SLA-Dashboard an [Cannon et al. 2011] bzw. die Anpassung der Prozesse hinsichtlich Multi-Vendor-Strategien.

Im Rahmen des *Capacity Management (9)* wird sichergestellt, dass die Kapazitäten der IT-Services und der Infrastruktur ausreichen, um die Ziele (Performance und Kapazität) wirtschaftlich zu erbringen. Im Cloud-Szenario beschränkt sich der Prozess auf das Bestimmen (Unterstützung bei der Identifikation von passenden Cloud-Providern) und Überwachen der Kapazitäten (für eine Rückmeldung zum Financial Management). Bei Cloud-Services lässt sich eine unzutreffende Bestimmung des Bedarfs durch eine flexible Erhöhung der Kapazitäten korrigieren (Elastizität). Im Idealfall skalieren die Cloud-Services automatisch, wodurch sich ein hohes Maß an Prozessänderungspotenzial ergibt, da Aktivitäten aus dem traditionellen Capacity-Management-Prozess entfallen. Die Bedeutung des Prozesses wird größtenteils gleich bleiben, da eine Überwachung der Kapazitäten weiterhin notwendig sein wird. Zum Beispiel können bei den Amazon Web Services (AWS) fehlende oder überflüssige virtuelle Maschinen innerhalb weniger Minuten hinzugebucht oder abgeschaltet werden. Die Überwachung allerdings bleibt in der Verantwortung des Leistungsabnehmers, der in diesem Zusammenhang häufig Unterstützungstools vom Provider angeboten bekommt (z. B. Amazon CloudWatch).

Das *IT Service Continuity Management (11)* managt Risiken und implementiert Mechanismen für die Sicherstellung der Kontinuität, sodass bei Eintritt außergewöhnlicher Ereignisse die in den SLAs vereinbarten Minimalanforderungen erreicht werden können. Im Kontext von Cloud-Services sind die vertragliche Fixierung dieser Anforderungen und das Aufstellen eines Notfallplans unter Einbeziehung von alternativen Providern notwendig. Hierbei sind Restriktionen bei der Interoperabilität von Cloud-Providern (möglicher Lock-in-Effekt) ein nicht zu unterschätzendes Problem [Repschläger et al. 2012]. Aufgrund von komplexeren Strukturen (fehlende Interoperabilität oder verteilte Ressourcenpools) stellt gerade die Entwicklung von Notfallplänen eine zunehmende Herausforderung dar. Durch den Kontrollverlust des Leistungsabnehmers beim Bezug von Cloud-Services kann ein Notfallmanagement nur eingeschränkt durchgeführt werden. Im Falle von Speicherdiensten aus der Cloud ist eine redundante Nutzung bzw. Wiederherstellung durch den Leistungsabnehmer denkbar. Ein Cloud-ERP-System (z. B. die SaaS-Lösung BusinessByDesign von SAP) dagegen bedingt bei einem Ausfall den Verlust oder die Nichtverfügbarkeit der Daten und lässt dem Leistungsabnehmer keinen Handlungsspielraum.

Im Cloud-Computing-Szenario spielt das *Information Security Management (12)* eine Schlüsselrolle, da der Leistungsabnehmer hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit jederzeit geschützt sein muss [Morin et al. 2012; itSMF 2012]. Der Prozess spielt bei der

Auswahl der möglichen Cloud-Provider eine wichtige Rolle, indem er die Sicherheitsanforderungen an das Supplier Management kommuniziert. Die Aufzeichnung von sicherheitsrelevanten Vorkommnissen beim Cloud-Provider sollte – wenn möglich – hier geschehen. Dieser Prozess hat im Kontext der Cloud-Services vorrangig einen planenden und überwachenden Charakter. Die neuen Herausforderungen liegen in der Überwachung des externen Providers und in einem komplexen Sicherheitskonzept, das eine orts- und geräteunabhängige Nutzung berücksichtigt. Bei Cloud-Services steht der IT-Organisation, im Vergleich zum internen Betrieb oder dem klassischen IT-Outsourcing, nur ein Teil der Steuerungsoptionen (Datenverschlüsselung, sichere Transferprotokolle, Rechtevergabe etc.) zur Verfügung.

Das *Supplier Management (13)* ist für die Verträge mit den Lieferanten zuständig. Gerade bei Cloud-Services sind »saubere« Regelungen zwischen beiden Parteien notwendig, damit die gestiegenen Anforderungen an Compliance (Services, Prozesse und Systeme) adressiert werden [itSMF 2010; Morin et al. 2012]. In diesem Szenario sinkt die Anzahl traditioneller Verhandlungen, weil die Verträge elektronisch geschlossen werden (Prozessveränderung). Doch ist eine sorgfältige Prüfung der Verträge von größter Bedeutung, damit der Cloud-Provider u.a. die gesetzlichen (z.B. Serverstandort im Ausland) und organisationalen Anforderungen tatsächlich erfüllt. Ein Verhandeln von Verträgen bzw. ein Nachverhandeln im herkömmlichen Sinne wird sowohl bei Private-Cloud-Providern als auch bei Public-Cloud-Providern möglich sein. Dieser Prozess stellt ein zentrales Element dar, weil im Cloud-Computing-Szenario zunehmend externe Cloud-Services von unterschiedlichen Anbietern bezogen werden (Multi-Vendor-Strategien) [itSMF 2012].

Das *Event Management (21)* überwacht die Configuration-Items (CIs) und IT-Services. Darüber hinaus findet eine Filterung von Events statt. Beim Bezug von Cloud-Services sinkt der Überwachungsaufwand von CIs, wohingegen die Überwachung von Cloud-Services wiederum zunimmt (proaktive Überwachung). Die Netzwerk-Monitoring-Software Nagios bietet Möglichkeiten zur Überwachung von Cloud-Services, wie die Amazon Web Services EC2 und S3. Nagios kann wiederum per Schnittstelle beispielsweise an OTRS (Open Ticket Request System), ein ITSM-Ticketsystem, angebunden werden (Leistungsabnehmer). Entsprechende Maßnahmen können nur über eine Anfrage an den Provider weitergeleitet werden, da die IT-Organisation selbst keinen Zugriff auf die IT-Ressourcen besitzt. Vor allem bei SaaS-Lösungen gestaltet sich eine Überwachung aufgrund des hohen technischen Abstraktionslevels schwieriger als bei IaaS- und PaaS-Diensten. Im Idealfall werden Wartungsarbeiten (Einschränkung im Hinblick auf Erreichbarkeit) aufseiten des Cloud-Providers gegenüber dem Leistungsabnehmer automatisiert kommuniziert, damit das Event-Management-System nicht unnötig Incidents erhebt.

Im *Incident Management (22)* werden sämtliche Vorfälle (Incidents) verwaltet. Dieser Prozess hat das primäre Ziel, die IT-Services für die Geschäftsbereiche möglichst schnell wiederherzustellen. Dem Prozess kommt im Cloud-Szenario eine mittlere Bedeutung zu, da die für Cloud-Services relevanten Incidents (Cloud Incidents) an den Cloud-Provider weitergeleitet werden. Die Übertragung der Cloud Incidents kann über eine Verzweigung im Incident-Management-Prozess erfolgen. Aus Compliance-Gründen ist die IT-Organisation des Leistungsabnehmers ebenfalls in den Prozess einzubinden [itSMF 2010]. Des Weiteren gewinnen Self-Service-Portale (OTRS Help Desk) beispielsweise für die Erstellung von Tickets oder das Wiederherstellen von Passwörtern an Bedeutung, wobei diese Portale im Idealfall eine direkte Anbindung an die Informationssysteme des Cloud-Providers haben sollten. Dem Service Desk kommt die Aufgabe zu, Informationen über die eingesetzten Cloud-Services bereitzustellen,

wenn diese Informationen nicht als Self Service zur Verfügung stehen.

Im Rahmen des *Access Management (24)* werden Anwender (bspw. aus dem Geschäftsbereich) für die Nutzung von IT-Services autorisiert. Darüber hinaus führt das Access Management die Vorgaben des Information Security Management aus. Der Prozess hat eine unveränderte Bedeutung, da Single-Sign-on-Mechanismen zwischen den bestehenden IT-Services und den verschiedenen Cloud-Services nur schwer bis gar nicht zu realisieren sind. Ferner muss nach wie vor eine übergeordnete Autorität existieren, die das Rollenmanagement in der Cloud überwacht und umsetzt. Ein Prozessänderungspotenzial ergibt sich durch die verschiedenen Rollenkonzepte in einer Multi-Cloud-Provider-Umgebung.

Durch das Continual Service Improvement (CSI) wird mithilfe von Qualitätsmanagementmethoden die Effizienz und Effektivität von Services und Prozessen fortwährend verbessert. Durch den *Service-Review*-Prozess *(26)* werden Vorschläge zur Optimierung von Services gemacht mit dem Ziel, die Servicequalität zu erhöhen und die Services wirtschaftlicher zu gestalten. In den Prozessen *Process Evaluation (27)*, *Definition of CSI Initiatives (28)* und *Monitoring of CSI Initiatives (29)* werden Initiativen zur Verbesserung von Prozessen und Services definiert und überwacht. Cloud-Services müssen auch den kontinuierlichen Verbesserungsanforderungen (CSI-Anforderungen) genügen, die mit dem Cloud-Provider vertraglich fixiert werden sollten [itSMF 2010]. Eine derart vertragliche Ausgestaltung ist bei Private-Cloud-Providern durchaus möglich, wohingegen bei Public-Cloud-Providern üblicherweise keine individuellen Gestaltungsmöglichkeiten gegeben sind [BITKOM 2010]. In den Anforderungen ist vor allem festzuhalten, in welchem Intervall was gemessen, analysiert und verbessert werden soll. In diesem Fall ist die IT-Organisation als transparent anzusehen. Sie gibt die Anforderungen des Geschäftsbereichs an den Cloud-Provider weiter [itSMF 2010]. Die Prozesse des CSI behalten die gleiche Bedeutung, da auch bei zunehmendem Bezug von Cloud-Services die ITSM-Prozesse kontinuierlich verbessert werden müssen.

5 Neubewertung der IT-Servicemanagementprozesse in Cloud-Szenarien

Unternehmen sollten bestehende ITIL-Prozesse im Hinblick für einen Einsatz von Cloud Computing neu bewerten und an veränderte Bedingungen anpassen. Damit der Einsatz von Cloud-Services dem Unternehmen einen Nutzen bringt, ist die individuelle Ausgangssituation (existierende ITIL-Prozesse und IT-Landschaft) und das geplante Cloud-Szenario zu berücksichtigen. Hierbei sollten die Cloud-Szenarien nach dem Nutzungsbereich (SaaS, PaaS oder IaaS) und dem Bereitstellungsmodell (Public oder Private Cloud) differenziert werden, da sich dementsprechend unterschiedliche Auswirkungen ergeben.

Dieser Beitrag gibt erste Anhaltspunkte, wie sich die Bedeutung von IT-Servicemanagementprozessen aufseiten des Leistungsabnehmers im Cloud Computing verändert. Dabei ist vor allem die zunehmende Bedeutung der Phasen Service Strategy und Service Design hervorzuheben. Demgegenüber ist zu erwarten, dass im Rahmen des Cloud Computing die Phasen Service Transition und Service Operation an Relevanz verlieren. Derweilen bleibt das Continual Service Improvement für den Leistungsabnehmer unverändert wichtig. Kritische Erfolgsfaktoren für den Einsatz von Cloud-Services können durchgängige Prozessketten (vom Geschäftsbereich über die IT-Organisation bis hin zu dem Cloud-Provider), Schnittstellen für den Datenaustausch (zwischen Leistungsabnehmer und -anbieter), Automatisierungen, Self-Service-Portale und klare vertragliche Regelungen sein. Das ITIL-Framework eignet sich mit einigen Anpassungen sehr gut für das Management von Cloud-Services.

6 Literatur

[APMG 2011] *APMG:* ITIL-Glossar und Abkürzung, 2011, *www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx*.

[Bause 2009] *Bause, M.:* ITIL und Cloud Computing: Welchen Mehrwert bietet ITIL mit seinem Service Lifecycle-Ansatz für Cloud Computing, 2009.

[BITKOM 2010] *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM):* Cloud Computing – Was Entscheider wissen müssen: Ein ganzheitlicher Blick über die Technik hinaus. Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance. Berlin, 2010.

[Cannon et al. 2011] *Cannon, D.; Wheeldon, D.; Lacy, S.; Hanna, A.:* ITIL Service Strategy. TSO, London, 2011.

[Fry 2010] *Fry, M.:* 5 questions about ITSM and cloud computing. Whitepaper, 2010.

[Geczy et al. 2012] *Geczy, P.; Izumi, N.; Hasida, K.:* Cloudsourcing: Managing Cloud Adoption. Global Journal of Business Research 6 (2012), 2, pp. 57-70.

[itSMF 2010] *itSMF:* Positionspapier Cloud Computing und IT Servcie Management, 2010.

[itSMF 2012] *itSMF:* At your Service 2 (2012), 1.

[KPMG 2012] *KPMG:* Cloud Monitor 2012: Eine Studie von KPMG in Zusammenarbeit mit BITKOM – durchgeführt von PAC, 2012.

[Labes et al. 2012] *Labes, S.; Stanik, A.; Repschläger, J.; Kao, O.; Zarnekow, R.:* Standardization Approaches within Cloud Computing: Evaluation of Infrastructure as a Service Architecture. Federated Conference on Computer Science and Information Systems (FedCSIS), 2012.

[Marston et al. 2011] *Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A.:* Cloud computing — The business perspective. Decision Support Systems 51 (2011), 1, pp. 176-189.

[Mell & Grance 2011] *Mell, P.; Grance, T.:* The NIST Definition of Cloud Computing. National Institute of Standards and Technology, NIST Special Publication 800-145, 2011.

[Morin et al. 2012] *Morin, J.-H.; Aubert, J.; Gateau, B.:* Towards Cloud Computing SLA Risk Management: Issues and Challenges. 45th Hawaii International Conference on System Sciences. IEEE, 2012, pp. 5509-5514.

[Rawal 2011] *Rawal, A.:* Adoption of Cloud Computing in India. Journal of Technology Management for Growing Economies 2 (2011), 2, pp. 65-78.

[Repschläger et al. 2012] *Repschläger, J.; Zarnekow, R.; Wind, S.; Turowski; K.:* Cloud Requirement Framework: Requirements and Evaluation Criteria to Adopt Cloud Solutions. 20th European Conference on Information Systems, 2012.

[Zimmermann & Rentrop 2012] *Zimmermann, S.; Rentrop, C.:* Schatten-IT. HMD – Praxis der Wirtschaftsinformatik 49 (2012), 288, S. 60-68.

Dipl.-Phys. Thorsten Pröhl
Dipl.-Inf. Jonas Repschläger
Dr. Koray Erek
Prof. Dr. Rüdiger Zarnekow
Technische Universität Berlin
Fachgebiet Informations- und Kommunikationsmanagement
Straße des 17. Juni 135
10623 Berlin
{t.proehl, j.repschlaeger, koray.erek}@tu-berlin.de
ruediger.zarnekow@ikm.tu-berlin.de
www.ikm.tu-berlin.de

Pröhl et al., IT-Servicemanagement im Cloud Computing. HMD – Praxis der Wirtschaftsinformatik, Heft 288, 2012, S. 6-14.