Das Aufkommen des Cloud Computing hat gewaltige Auswirkungen auf die IT-Industrie. Unternehmen wie Google, Amazon und Microsoft, bieten immer leistungsfähigere, zuverlässigere und kostengünstigere Cloud Plattformen an.Unternehmen mit Rechenbedarf hinterfragen zunehmend den Nutzen ihrer eigenen IT-Infrastruktur und prüfen, inwieweit sie durch Nutzung von Cloud Computing Fixkosten abbauen und bedarfsgerecht gegen variable Kosten austauschen können.

Virtuelles Risiko oder Segen?

Cloud Computing in der Wirtschaftsprüfung

Von Ludwig Mochty und Michael Wiese

Cloud Computing gehört zweifelsohne zu den großen IT-Trends der letzten Jahre. Mit Hilfe des Cloud Computing[1] können IT-Ressourcen wie Rechnerleistung und Speicherplatz, über das Internet bedarfsgerecht angemietet und wieder an den IT-Dienstleister zurückgegeben werden. Dadurch wird die traditionelle Rolle des IT-Dienstleisters zweigeteilt: In einen Infrastrukturanbieter, der Rechnerplattformen betreibt und IT-Infrastruktur gegen nutzungsabhängige Preise vermietet, und einen IT-Dienstleister, der von einem oder mehreren Infrastrukturanbietern IT-Ressourcen anmietet, um IT-Dienstleistungen für einen End-User zu erbringen.

Das Aufkommen des Cloud Computing hat gewaltige Auswirkungen auf die IT-Industrie. Unternehmen wie Google, Amazon und Microsoft, bieten immer leistungsfähigere, zuverlässigere und kostengünstigere Cloud Plattformen an. Unternehmen mit Rechenbedarf hinterfragen zunehmend den Nutzen ihrer eigenen IT-Infrastruktur und prüfen, inwieweit sie durch Nutzung von Cloud Computing Fixkosten abbauen und bedarfsgerecht gegen variable Kosten austauschen können.

Tatsächlich kann eine solche Reorganisation der firmeneigenen IT-Landschaft eine Reihe von attraktiven Vorteilen mit sich bringen: (1) Es bedarf keiner investiven Vorleistungen. Der*Die Nutzer*in mietet je nach Bedarf IT-Ressourcen von der Cloud und zahlt für deren Nutzung. (2) Es lassen sich IT-Verarbeitungskosten senken, weil die in Anspruch genommene Kapazität nicht am Spitzenbedarf ausgerichtet sein muss. Angemietete IT-Ressourcen können wieder freigegeben werden, sobald der Bedarf sinkt. (3) IT-Dienstleistung wird auf diese Weise flexibel skalierbar: Mehrere IT-Infrastruktur-Anbieter können ihre Ressourcen zusammenlegen und erforderlichenfalls wieder entflechten. IT-Dienstleistungsanbieter sind durch den kurzfristigen Zugriff auf einen solchen Ressourcenpool in der Lage, sich geradezu blitzartig an Schwankungen in der Nachfrage nach IT-Dienstleistungen anzupassen. (4) Der Zugriff auf in der Cloud angebotene IT-Dienstleistungen ist üblicherweise sehr leicht realisierbar, weil er über das Internet erfolgt. (5) Ein IT-Dienstleistungsanbieter kann sein Hardware-Risiko an IT-Infra-

Ludwig Mochty. Foto: Vladimir Unkovic

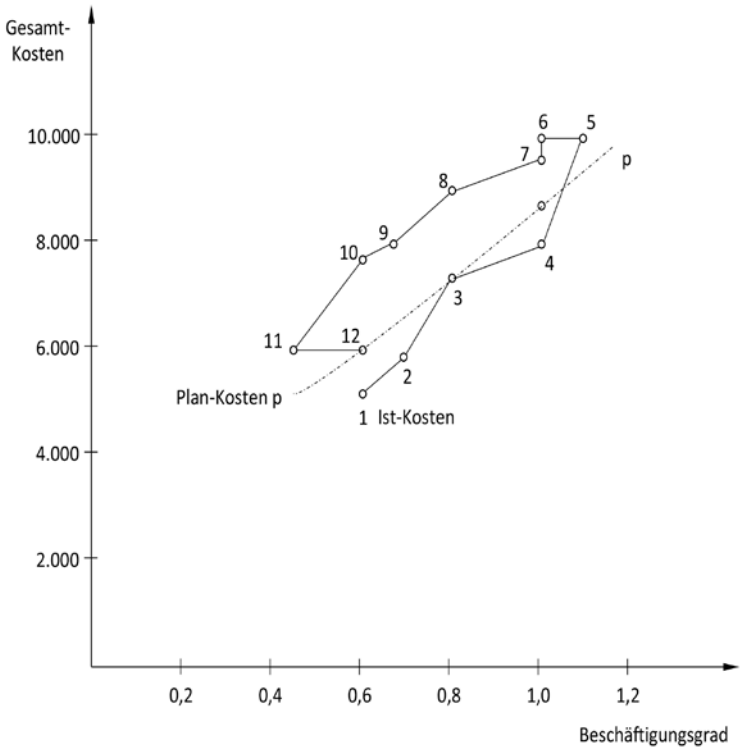
strukturanbieter outsourcen, die oftmals dafür besser ausgerüstet sind, und kann damit die hardwareabhängigen Instandhaltungs- und Personalkosten einsparen. Natürlich hat Cloud Computing für den End-User nicht nur Vorteile – aber davon später.

Betriebswirtschaftliche Fragestellungen

Für das Cloud Computing gibt es bisher zwar eine Reihe von Verbrauchserfassungssystemen, allerdings sind diese lediglich auf die mitlaufende Erfassung der Leistungs- und Ressourceninanspruchnahme anhand technischer Metriken (CPU-Zeiten, GigaByte, etc.) ausgerichtet, aber mangels betriebswirtschaftlicher Fundierung nicht geeignet, die kaufmännische Entscheidungsfindung zu unterstützen. Dies hat negative Auswirkungen auf die verursachungsgerechte Preis- und Produktpolitik, auf die betriebswirtschaftliche Optimierung des IT-Produktionsbetriebs sowie auf die Investitionspolitik von Cloud Computing-Dienstleistungsanbietern. Schließlich fehlen damit auch IT-Prozesskostensätze, die es einem Unternehmen erlauben würden, die Entscheidung zwischen Eigenfertigung und Fremdbezug (Eigene IT versus Cloud Computing) kaufmännisch fundiert zu fällen.

Durch das Cloud Computing wird deshalb nicht nur die Computerwissenschaft, sondern auch die Betriebswirtschaftslehre (BWL) herausgefordert, denn durch seine dynamische Virtualität stellt Cloud Computing klassische betriebswirtschaftliche Fragestellungen in ein völlig neues Licht. Einige dieser Fragestellungen seien im Folgenden explizit angesprochen.

Das kaufmännische Management von Cloud Computing-Systemen verlangt nach einer Buchführung und insbesondere nach einer Kosten- und Leistungsrechnung, die geeignet ist, Prozesse in virtuellen Organisationen verursachungsgerecht abzubilden. Die traditionelle Kostenrechnung wurde ursprünglich für die arbeitsintensive Massenfertigung relativ homogener Erzeugnisse konzipiert. Sie ist nach betrieblichen Funktionen (Materialbeschaffung und -lagerung; Fertigung; Verwaltung und Vertrieb) und nicht nach Geschäftsprozessen gegliedert. Deshalb kommt es häufig zu einer nicht verursachungsgerechten Proportionalisierung großer Kostenanteile, wenn diese Art der Kostenrechnung auf flexible industrielle Fertigungsprozesse angewendet wird. Und zwar umso mehr, je heterogener, komplexer und variantenreicher die Erzeugnisstruktur ist und je stärker die Gemeinkosten von anderen Kostentreibern als den menschlichen Leistungsstunden abhängig sind. Von dieser Problematik ist die Kalkulation von Cloud Computing-Leistungen in extrem verschärfter Form betroffen. Da also die traditionelle Kostenrechnung nicht geeignet ist, Cloud Computing-Leistungen verursachungsgerecht abzubilden, bedarf es eines Kostenrechnungssystems, das speziell für Prozessstrukturen konzipiert ist. Ein solches wurde von der Betriebswirtschaftslehre in Form der Prozesskostenrechnung[2] (Activity Based Costing, ABC) entwickelt. Es konnte sich aber wegen des großen Arbeitsaufwands, der mit der Erhebung der Teilprozesse und Aktivitäten sowie mit der Erfassung der Prozessgrößen verbunden ist, nicht flächendeckend durchsetzen. Hier bringt das Cloud Computing ganz entscheidende Vorteile mit sich. Denn anders als bei konventionellen Geschäftsprozessen steht beim Cloud Computing ein mitlaufendes prozessorientiertes Verbrauchserfassungssystem zur Verfügung, auf das betriebswirtschaftliche Abrechnungs- und Entscheidungsunterstützungssysteme in Echtzeit zurückgreifen können. In dieser Hinsicht verfügt Cloud Com-



(1) Darstellung des asymmetrischen Kostenverlaufs (Hysteresis).
Quelle: in Anlehnung an Heinen, E.: Zum Problem der Kostenremanenz. In: Zeitschrift für Betriebswirtschaft (ZfB), 36. Jahrgang 1966, S. 1–18, hier: S. 3

puting gewissermaßen über eine Art von „Fahrtenschreiber“ (Meta-Daten, die wie Kuppelprodukte anfallen), sodass es einer aufwendigen und fehleranfälligen manuellen Erfassung der Prozessgrößen nicht bedarf. Es wird noch zu prüfen sein, welche Verfeinerungen der Prozesskostenrechnung durch die virtuelle Natur des Cloud Computing erforderlich werden. Sollte es aber gelingen, am Beispiel von Cloud Computing ein funktionsfähiges, betriebswirtschaftlich fundiertes Kosten- und Leistungssystem zu entwickeln, müsste dieses auch auf andere virtuelle Organisationen und Unternehmen übertragbar sein.

Mit dem Cloud Computing kann aus betriebswirtschaftlicher Sicht ein interessantes weiteres Phänomen verbunden sein, das erstmals 1927 beschrieben worden ist. Es handelt sich um das Phänomen der Kostenremanenz[3], das im Zusammenhang mit Beschäftigungsschwankungen zu beobachten ist: Der Zuwachs der Kosten nimmt bei einer Beschäftigungszunahme (hier: bei der Steigerung der nachgefragten Rechenleistung) einen anderen Verlauf als bei der Beschäftigungsabnahme (hier: Absenkung der nachgefragten Rechenleistung). Dieser asymmetrische Kostenverlauf in Form einer Hysteresis wurde ursprünglich in Analogie zur magnetischen Induktion beim Auf- und Abbau eines elektromagnetischen Felds beschrieben und vermutlich deshalb von der BWL bisher kaum beachtet. Sollte dieses Phänomen beim Cloud Computing auftreten, stünden erstmals Massendaten zur Verfügung, um umfangreiche und detailreiche Kostenanalysen durchführen zu können.

Allgemein ist die Kostenrechnung nur geeignet, um kurzfristige Entscheidungen zu fundieren. Für die Unterstützung langfristiger Investitions- und Desinvestitionsentscheidungen dient die Investitionsrechnung. Im Zusammenhang mit dem Cloud Computing interessiert dabei insbesondere die Fragestellung: In welchem Ausmaß soll im Kalkulationszeitpunkt bei der Wahl der Größe einer Anlage die in der Zukunft erwartete Steigerung der Nachfrage berücksichtigt werden? Die Wirtschaftlichkeit von erweiterbaren Anlagen unter Berücksichtigung einer zukünftigen Bedarfszunahme wurde bereits 1939 im Zusammenhang mit der Erweiterung eines Telefonnetzwerks analysiert[4]. Auch diese in der betriebswirtschaftlichen Ausbildung wenig beachtete Fragestellung erfährt im Zusammenhang mit Investitionen in dynamische virtuelle Organisationen ein Redivivum.

Besonders schwierig zu beantworten ist für die BWL zurzeit noch die Frage nach der zweckmäßigsten Gestaltung nutzungsabhängiger Preise für die „Rechenleistung aus der Steckdose“. Eine betriebswirtschaftlich fundierte Lösung dieser Aufgabenstellung setzt indes voraus, dass die Kosten von Cloud Computing-Serviceleistungen zuverlässig und verursachungsgerecht kalkuliert werden können. Und hier steht die BWL erst am Anfang.

Rechtliche Einordnung

Voraussetzung für den Einsatz der genannten Entscheidungsunterstützungskalküle ist die korrekte Erfassung der verschiedenen Aspekte des Cloud Computing in der Buchführung. Denn diese bildet die Datenbasis für alle weiteren Auswertungen. Deshalb soll zuerst eine grobe rechtliche Einordnung erfolgen, bis wir uns mit der Frage beschäftigen werden, welche Anforderungen an die Sicherheit und Ordnungsmäßigkeit des Rechnungswesens im Zusammenhang mit Cloud Computing zu erfüllen sind und wie die Einhaltung dieser Anforderungen durch den freien Beruf der Wirtschaftsprüfer überwacht wird.

Die Grenzen zwischen Cloud Computing und IT-Outsourcing verschwimmen zusehends, da klassische IT-Outsourcing-Dienstleistungsunternehmen zunehmend Techniken des Cloud Computing einsetzen.[5] Man kann Cloud Computing als eine besondere Form des IT-Outsourcings ansehen. Ein besonderer Vertragstyp für Cloud Computing-Leistungen existiert im deutschen Recht nicht. Relevant sind insbesondere der Mietvertrag (§§ 535ff. BGB), der Werkvertrag (§§ 631ff. BGB) und der Dienstvertrag (§§ 611ff. BGB). Für die Beurteilung von Cloud Computing-Verträgen ist auf die enthaltenen Teilleistungen abzustellen, denn in der Regel handelt es sich um gemischte Vertragstypen. Cloud Computing-Leistungen umfassen im Wesentlichen „Software as a Service“ (SaaS), „Infrastructure as a Service“ (IaaS) und „Platform as a Service“ (PaaS)[6].

- Bei SaaS besteht die Dienstleistung in der Bereitstellung einer IT-Anwendung auf dem Server des Anbieters. Das auslagernde Unternehmen hat keinen Einfluss auf die der genutzten IT-Anwendung zugrunde liegenden IT-Infrastruktur. Die Benutzeroberfläche der IT-Anwendung wird in der Regel innerhalb eines Browserfensters dargestellt, während die Anwendung selbst in Echtzeit auf dem Server des Anbieters ausgeführt wird. Die Installation der Software auf den Endgeräten des auslagernden Unternehmens ist nicht vorgesehen. SaaS-Verträge sind Dauerschuldverhältnisse[7]. Das Leistungsentgelt (Software-Miete) richtet sich regelmäßig nach der Anzahl der vereinbarten Softwarenutzern. Viele Unternehmen entscheiden sich für den Bezug von SaaS (z.B. ERP-Systeme oder Office-Dienste wie E-Mail-Programme), weil ihre eigene Software-Architektur den Anforderungen volatiler Märkte und der gestiegenen Innovationsgeschwindigkeit nicht mehr entspricht.
- IaaS-Servicemodelle bestehen in der flexiblen Anmietung von IT-Ressourcen (z.B. Rechenleistung und Speicherkapazität), die das auslagernde Unternehmen für seine Unternehmenszwecke nutzen kann. Diese Infrastruktur besteht nicht aus

realen, sondern aus virtuellen Servern, die physisch im Serverzentrum des Cloud Computing-Anbieters untergebracht sind. Die Mitarbeiter des auslagernden Unternehmens greifen über einen Internetbrowser oder mobile Endgeräte auf den IaaS-Service zu und nutzen diese Infrastruktur zum Aufbau eigener Services zum internen oder externen Gebrauch[8]. Das IaaS-Servicemodell wird in der Regel durch einen gemischten Vertragstyp abgebildet, der miet-, dienst- und werkvertragliche Elemente beinhaltet[9]. Das Leistungsentgelt richtet sich in der Regel nach dem Umfang der während der Abrechnungsperiode in Anspruch genommenen Ressourcen (z.B. Rechenleistung oder Speicherkapazität).

• PaaS bezeichnet die bedarfsorientierte Bereitstellung von IT-Infrastruktur (z.B. Rechenleistung, Speicherkapazität und Internetanbindung, Laufzeitumgebungen) und Entwicklerwerkzeugen zur Entwicklung und Ausführung von Cloud-basierten Softwarelösungen. Die primäre Zielgruppe von PaaS-Angeboten sind daher Software-Entwickler[10].

Cloud Computing-Anbieter bieten ihren Kunden in der Regel standardisierte Leistungen an. Daher werden insbesondere für den Online-Bezug dieser Leistungen anstelle von Individualvereinbarungen vorformulierte Allgemeine Geschäftsbedingungen (AGB) eingesetzt.

Service Level Agreements

Das Service Level Agreement stellt üblicherweise einen gesonderten Teil oder eine Anlage des Cloud Computing-Vertrags dar. Es bezieht sich auf die Leistungsbeschreibung und regelt, welche Service Levels gelten (d.h. welche Funktionalitäten und welche Qualität geschuldet sind) und welche Rechtsfolgen eine Vertragsverletzung auslöst. Standardbestandteile des Service Level Agreements sind Regelungen zur Verfügbarkeit der Cloud Computing-Leistung (üblicherweise ausgedrückt durch einen Prozentwert in Bezug auf einen bestimmten Betrachtungszeitraum), zu Entstörzeiten im Falle einer Störung der Cloud Computing-Leistungen, zu den Rechtsfolgen einer Schlechtleistung, zu Vertragsstrafen oder pauschaliertem Schadensersatz sowie zum Kündigungsrecht im Falle einer Nichteinhaltung von Service Levels[11]. Im Service Level Agreement sollten ebenfalls Regelungen zum Gerichtsstandort, dem anwendbaren Recht sowie die Vertragssprache enthalten sein. Darüber hinaus sind Eigentums- und Urheberrechte an Daten, Systemen, Software und Schnittstellen festzulegen[12].

Datenschutzrecht und Compliance

Charakteristisch für Cloud Computing ist die Weitergabe von Daten vom auslagernden Unternehmen an den Dienstleister. Das deutsche Datenschutzrecht kommt zur Anwendung, sobald personenbezogene Daten im Inland erhoben oder verwendet werden. Sofern die Datenerhebung oder -verarbeitung durch ein Unternehmen mit Sitz in der EU oder im EWR erfolgt, gilt nach § 1 Abs. 5 BDSG das Datenschutzrecht im Ansässigkeitsstaat dieses Unternehmens. Nach §§ 4b, 4c BDSG werden Datenverarbeitungen innerhalb der EU beziehungsweise des EWR wie Datenverarbeitungen im Inland behandelt. Wenn Cloud Computing-Dienstleistungen durch Unternehmen oder durch physische Rechenzentren in Drittstaaten erbracht werden, ist unter Datenschutzgesichtspunkten die Zulässigkeit des Auslandstransfers zu klären[13]. Das auslagernde Unternehmen hat sich als Auftraggeber nach § 11 BDSG bereits vor Beginn der Datenverarbeitung und im Anschluss regelmäßig von der Einhaltung der Bestimmungen des Datenschutzes zu überzeugen.

Zusätzlich zu den datenschutzrechtlichen Anforderungen ist sicherzustellen, dass sich der Dienstleister an die sonstigen rechtlichen Bestimmungen (Compliance) des auslagernden Unternehmens hält. Hierbei liegt es in der Verantwortung des auslagernden Unternehmens, die konkreten rechtlichen Anforderungen zu benennen. Anforderungen können sich zum Beispiel ergeben aus dem Telekommunikationsgesetz (TKG), der Abgabenordnung (AO) bei der Verarbeitung steuerrechtlicher Daten, dem Handelsgesetzbuch (HGB) bei der Verarbeitung buchführungsrelevanter Daten und dem Strafgesetzbuch (StGB).

Anforderungen an die Sicherheit und Ordnungsmäßigkeit

Die gesetzlichen Vertreter müssen die Einhaltung der gesetzlichen Anforderungen an die Sicherheit und Ordnungsmäßigkeit der IT-gestützten Rechnungslegung sicherstellen. Die Sicherheitsanforderungen umfassen Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit[14]. Zu den Ordnungsmäßigkeitskriterien zählen Vollständigkeit (§ 239 Abs. 2 HGB), Richtigkeit (§ 239 Abs. 2 HGB), Zeitgerechtheit (§ 239 Abs. 2 HGB), Ordnung (§ 239 Abs. 2 HGB), Nachvollziehbarkeit (§ 238 Abs. 1 Satz 2 HGB), Unveränderlichkeit (§ 239 Abs. 3 HGB)[15]. Das Management implementiert zu diesem Zweck Grundsätze, Verfahren und Maßnahmen (Regelungen), die gerichtet sind auf: die Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen), zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften. Die Gesamtheit dieser Regelungen wird als internes Kontrollsystem bezeichnet. Das interne Kontrollsystem

umfasst die Komponenten Risikobeurteilung, Kontrollumfeld, Risikobeurteilungen, Kontrollaktivitäten, Information und Kommunikation und Überwachung des internen Kontrollsystems durch das Management des Unternehmens[16]. Relevante Standards, die für eine Implementierung herangezogen werden können, sind COBIT©, COSO©, ISO EC 27001 und IDW RS FAIT 1.

Die gesetzlichen Ordnungsmäßigkeitsanforderungen einschließlich der Beachtung der Grundsätze ordnungsmäßiger Buchführung (§ 239 Abs. 4 HGB) und die damit verbundenen Anforderungen an die Sicherheit der IT-gestützten Rechnungslegung gelten uneingeschränkt auch für den Fall des IT-Outsourcings. Mit der Auslagerung von betrieblichen Funktionen im Rahmen des IT-Outsourcings müssen die im IDW RS FAIT 1 formulierten Sicherheits- und Ordnungsmäßigkeitsanforderungen auch im Zusammenspiel mit den Dienstleistungsunternehmen – einschließlich eventueller Subdienstleistungsunternehmen – erfüllt werden. Aufgrund der zunehmenden Auslagerung von Prozessen und Daten auf Subdienstleister wurde der IDW RS FAIT 5 in Zusammenarbeit mit dem Fachausschuss IT entwickelt, um den Risiken aus der Auslagerung der Daten und Prozesse nach den Sicherheits- und Ordnungsmäßigkeitsanforderungen des HGB zu genügen. IDW FAIT 5 ergänzt und konkretisiert die aus den §§238, 239 und 257 HGB sowie der IDW RS FAIT 1 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie) resultierenden Anforderungen an die Führung der Handelsbücher mittels IT-gestützter Systeme. FAIT 5 ist ab dem 1. Januar 2016 anzuwenden.

Die gesetzlichen Vertreter haben die Aufgabe, das Cloud Computing von der Entscheidung zur Auslagerung bis zur Beendigung zu steuern. Das interne Kontrollsystem muss auch im Hinblick auf die ausgelagerten Funktionen angemessen ausgestaltet und wirksam sein. Ausgehend von der Risikobeurteilung muss das auslagernde Unternehmen den sich durch das IT-Outsourcing ergebenden Risiken durch eine entsprechende Ausgestaltung des internen Kontrollsystems begegnen. Alle involvierten Subdienstleister sind ausnahmslos Bestandteil des internen Kontrollsystems.

Service Level Agreements

Die mit dem Dienstleister getroffenen Vereinbarungen müssen die Sicherheit und Ordnungsmäßigkeit der ausgelagerten Daten und Prozesse sicherstellen. Risiken aus nicht getroffenen Vereinbarungen müssen durch kompensierende Kontrollen adressiert werden.

Administration

Die gesetzlichen Vertreter des auslagernden Unternehmens sind für die Änderungen an den Programmen und Zugriffsberechtigungen des Dienstleisters verantwortlich. Das auslagernde Unternehmen muss sicherstellen, dass nur solche Änderungen durchgeführt und Berechtigungen vergeben werden, die die Sicherheit und Ordnungsmäßigkeit der gespeicherten, transportierten oder verarbeiteten Daten nicht gefährden.

Überwachung

Eine regelmäßige Berichterstattung und Auswertung des Dienstleisters hinsichtlich der Vereinbarungen in den Service Level Agreements ist erforderlich. Die unternehmenseigenen Risiken aus der Auslagerung und die dafür entwickelten Kontrollen müssen regelmäßig überwacht werden. Das auslagernde Unternehmen sollte ein umfassendes Bild vom Dienstleistungsunternehmen haben, zum Beispiel durch Einsichtnahme in aktuelle Service Organization Control (SOC) Berichte (IDW PS 951 n.F., ISAE 3402) oder in Prüfungsberichte der internen Revision.

Netzwerke

Die Infrastruktur des Dienstleisters muss separiert sein in vertrauenswürdige Netzwerke (z.B. Lokales Administrationsnetzwerk) und nicht sichere Netzwerke (z.B. End-User-Netzwerk). Deren Einstellungen sind durch das auslagernde Unternehmen regelmäßig zu überprüfen. Die für die Übermittlung der Daten relevanten Komponenten und die relevante Infrastruktur unterliegen den gleichen Integritäts- und Verfügbarkeitsanforderungen wie die Orte der Speicherung der Daten.

Nationale Besonderheiten

Die Behandlung von rechnungslegungsrelevanten Daten in Drittländern muss den Sicherheits- und Ordnungsmäßigkeitsanforderungen des HGB genügen. Besonderheiten im Steuer-, Straf- und Zivilrecht sowie des Datenschutzes dürfen zu keinem Wiederspruch mit der deutschen Gesetzgebung führen. Die gesetzlichen Vertreter des auslagernden Unternehmens sind auch nach Beendigung der vertraglichen Beziehungen mit dem Dienstleister für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen verantwortlich. Darunter fallen beispielsweise Anforderungen an die Archivierung rechnungslegungsrelevanter Daten oder an die Datenlöschung auf Seiten des Dienstleistungsunternehmens.

Risikoorientierter Prüfungsansatz

Gegenstand der Abschlussprüfung ist neben dem Jahresabschluss die Ordnungsmäßigkeit der Buchführung. Hierbei untersucht der Abschlussprüfer in der Regel das eingerichtete interne Kontrollsystem. Da eine lückenlose Prüfung von Buchhaltung und Rechnungslegung wirtschaftlich nicht möglich ist und vom Gesetzgeber in § 317 HGB auch nicht verlangt wird, erfolgt die Abschlussprüfung auf Basis einer risikoorientierten Auswahl von

Geschäftsvorfällen und Abschlussposten. Durch Kombination von Art, Zeitpunkt und Umfang der Prüfungshandlungen sollen hinreichend viele (ausreichend) beweiskräftige (angemessene) Prüfungsnachweise erhalten werden, um das Prüfungsurteil im Bestätigungsvermerk zu begründen.

Ausgelagerte Dienstleistungen sind für die Prüfung des internen Kontrollsystems relevant, wenn sie dazu dienen, Daten über Geschäftsvorfälle oder betriebliche Aktivitäten zu speichern oder zu verarbeiten, die entweder direkt in die Rechnungslegung einfließen oder dem Rechnungslegungssystem als Grundlage für Buchungen zur Verfügung gestellt werden. Typische ausgelagerte Unternehmensfunktionen umfassen Beschaffung, Einkauf, Materialwirtschaft/Logistik, Produktion, Entwicklung, Buchhaltung, Vertrieb oder Personalabrechnung. Die Auslagerung dieser Funktionen hat zum Teil erhebliche Auswirkungen auf Aufbau- und Ablauforganisation, IT-Infrastruktur, IT-Anwendungen und IT-gestützte Geschäftsprozesse. In jüngerer Vergangenheit finden sich auch Auslagerungen von Analysekapazitäten im Bereich Controlling und Management („Big Data in der Cloud“) mit teilweise erheblichen unmittelbaren Risiken für die Steuerung von Unternehmen und die Finanzberichterstattung.

Beim Cloud Computing ergeben sich neben IT-Sicherheitsrisiken, Ordnungsmäßigkeitsrisiken besondere rechtliche Risiken in Bezug auf Organisation und Aufgabenteilung, Schnittstellen und genutzte Übertragungswege, eingesetzte Technologien, Datenspeicherung und Speicherort. Hierzu gehören auch Maßnahmen für den Not- und Katastrophenfall sowie Kontrollen, die eine Funktionsfähigkeit dieser Maßnahmen gewährleisten. Als Teil der Prüfung des internen Kontrollsystems hat der Prüfer die Wirksamkeit der dafür eingerichteten Kontrollen zu beurteilen.

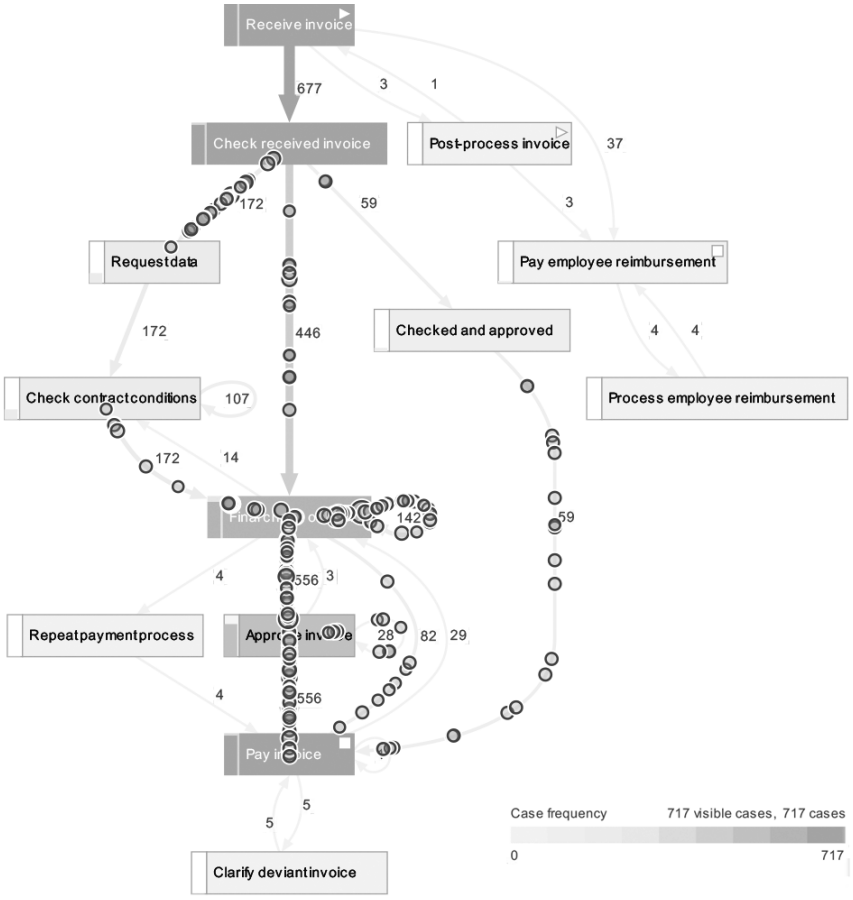
Verlust der Transparenz

Mit der IT-gestützten Automatisierung, dem Outsourcing und dem Schritt in die Cloud („Digitalisierung“) versuchen Unternehmen vor allem, die Kosten interner Abläufe zu reduzieren und interne Abläufe zu beschleunigen. Das kann dann gelingen, wenn Aktivitäten innerhalb der Prozesse häufig und gleichartig sind und daher standardisiert werden können. Durch Standardisierung lässt sich die Anzahl von Prozessvarianten reduzieren. Die IT-Integration zieht jedoch auch eine erhöhte Komplexität der Abläufe und damit einhergehend eine erhöhte Intransparenz nach sich. Für den Nicht-Standardfall sind Mitarbeiter häufig gar nicht ausgebildet oder es existiert systemseitig keine Möglichkeit, den Fall abzubilden. Für Prüfer IT-gestützter Systeme und Prozesse stellt sich das Prüfproblem deutlich schärfer als das Ausführungsproblem dar. Denn der Prüfer verfügt in der Regel nicht über die Detailkenntnisse der internen Prozesse wie beispielsweise eine interne Revision. Durch Beobachtungen von Prozessabläufen und Befragungen der beteiligten Mitarbeitern lässt sich diese Wissenslücke in komplexen IT-gestützten Systemen nicht schließen. Denn beobachten lässt sich nur der Standardfall. Sonderfälle sind entweder nicht vorgesehen, sind noch nicht aufgetreten oder werden nicht offengelegt, zum Beispiel im Fall vorsätzlicher Eingriffe. Aufgabe der Prüfer ist es aber, die tatsächliche Umsetzung der definierten Abläufe und die Zuverlässigkeit des Systems auch im Sonderfall zu beurteilen. Das gelingt zunehmend schlechter und hat negative Auswirkungen auf das Risikomanagement. Klarerweise sind moderne IT-Prüfer darin geschult, Risiken auf Ebene der IT-Infrastruktur und innerhalb der IT-Anwendung zu erkennen. Doch gerät der Bezug zur individuellen Ausführung der Prozessaktivitäten und zum Jahresabschluss als Prüfungsgegenstand oftmals aus dem Blick. Mitunter unterminiert die IT die Fähigkeit der Prüfer, die wesentlichen Risiken zu erkennen.

Process Mining

Digitale Systeme und Prozesse haben aber auch eine Eigenschaft, die sich zur Lösung des Problems der Komplexität und Intransparenz nutzen lässt. Um den gesetzlichen Ordnungsmäßigkeits- und Sicherheitsanforderungen gerecht zu werden, speichern moderne Enterprise Ressource Systeme (ERP) nahezu alle relevanten digitalen Verarbeitungsschritte von Geschäftsvorfällen, Systemaktivitäten und durchgeführten Kontrollen. Die Datentabellen mit den individuellen Verarbeitungsschritten (sogenannte Event Logs) für jeden Geschäftsvorfall können für Prüfungszwecke extrahiert werden. Unter Einsatz entsprechender Algorithmen werden diese Events zeitlich sortiert und zu gleichartigen Aktivitäten zusammengefasst. So gelingt es, die tatsächlichen Prozessabläufe zu rekonstruieren, zu visualisieren und für prüferische Zwecke zu analysieren. In Anlehnung an den Begriff „Data Mining“, dem „Schürfen“ nach Informationen aus Massendaten, wird der Ansatz als „Process Mining“ bezeichnet.

Erkennbar ist, dass die individuellen Rechnungen (dargestellt als kleine Kreise) unterschiedliche Wege durch das Verarbeitungssystem nehmen. In der dynamischen Anwendung werden außerdem die unterschiedlichen Durchlaufzeiten erkennbar. Bislang war der Prüfer auf Schilderungen der prozessbeteiligten Mitarbeiter nur eines typischen Falles, zum Beispiel einer Rechnungsprüfung, beschränkt. Durch die Komplexität sind bei der konventionellen Prüfung des internen Kontrollsystems Unvollständigkeiten und Irrtümer kaum zu vermeiden.



(2) Ablauf eines Kontrollprozesses für Eingangsrechnungen, beginnend mit dem Rechnungseingang bis zum Zahlungsausgang und zur Differenzenklärung.
Quelle: eigene Darstellung

Unser Forschungsschwerpunkt ist die methodische Integration des Process Mining in die Ablaufmodelle betriebswirtschaftlicher Prüfungen mit besonderem Schwerpunkt auf die Abschlussprüfung durch Wirtschaftsprüfer. Für die praktische Anwendbarkeit ist hierbei besonders relevant, inwieweit das Process Mining geeignet ist, die Ziele der internationalen Prüfungsstandards des IAASB für die Prüfung des internen Kontrollsystems zu erreichen. Die Prüfungsstandards geben ein zweistufiges Vorgehen vor. ISA 315 verlangt ein grundlegendes Verständnis für die Komponenten des internen Kontrollsystems: Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung des internen Kontrollsystems durch das Management.

Kontrollumfeld

Das Kontrollumfeld stellt den Rahmen dar, innerhalb dessen die Grundsätze, Verfahren und Maßnahmen der internen Kontrolle eingeführt und angewendet werden[17]. Es wird unter anderem bestimmt durch die Unternehmenskultur, Fachkompetenz der Mitarbeiter und die Aufbau- und Ablauforganisation. Unter Einsatz von Process Mining ist es möglich, viele der relevanten Eigenschaften des Kontrollumfelds, die besonders bei der Auslagerung von Funktionen nur schwer beobachtbar sind, indirekt prüfbar zu machen. Weil ERP-Systeme neben den reinen Events auch den Systemnutzer speichern, ist es möglich, große Teile der Aufbauorganisation zu rekonstruieren. Ein anschließender Vergleich mit der in Organigrammen und Arbeitsplatzbeschreibungen festgelegten Organisation zeigt oftmals erstaunliche Unterschiede zwischen dem, was Mitarbeiter tun, und dem, was sie eigentlich tun sollten. Identifiziert werden kritische Aktivitäten und Mitarbeiter, bei deren Ausfall Schaden droht. Gegebenenfalls sind Vertretungsregeln zu überarbeiten. Anhand von überdurchschnittlichen Bearbeitungszeiten werden Engpässe sichtbar, die auf Mängel in der Personalplanung schließen lassen. Häufige Wiederholungen von Aktivitäten und Rückkopplungen zeigen Nachlässigkeit oder mangelnde fachliche Eignung auf. Für den Prüfer wird erkennbar, ob das Management seiner Verantwortung für die Überwachung der Aufbau- und Ablauforganisation gerecht wird. Gerade in Krisenzeiten einer Unternehmung zeigt sich, dass interne Abläufe zunehmend degenerieren. Das Kontrollumfeld kann durch Process Mining wie ein Film beobachtet werden.

Risikobeurteilungsprozess

Unternehmen sind einer Vielzahl von finanziellen, rechtlichen, leistungswirtschaftlichen oder strategischen Risiken ausgesetzt. Diese Risiken müssen vom Unternehmen erkannt, analysiert und beurteilt werden[18]. Process Mining unterstützt hier in zweifacher Hinsicht. Zum einen können Risiken aus der Ablauforganisation identifiziert werden, die bisher regelmäßig erst zu spät erkennbar werden. Beispielsweise können Mängel im Prozess des Forderungsmanagements das Unternehmen in die Zahlungsunfähigkeit treiben. Zum anderen kann der Risikobeurteilungsprozess selbst mit Process Mining analysiert werden. Besonders relevant ist diese Anwendung für kapitalmarktorientierte Unternehmen, die verpflichtet sind, ein Risikofrüherkennungssystem einzurichten und permanent zu überwachen. Der Risikobeurteilungsprozess ist sicherlich für Outsourcing wenig geeignet. Diejenigen Risiken

Michael Wiese. Foto: Vladimir Unkovic

aber, die sich aus Outsourcing und Cloud Computing ergeben, müssen zwingend Bestandteil permanenter Überwachung auf Basis des Process Mining sein.

Kontrollaktivitäten

Als eigenständige Kontrollaktivität, beispielsweise im Rahmen der internen Revision, und bei der Aufbau- und Ablaufprüfung von Kontrollaktivitäten spielt Process Mining seine Stärke aus. Kontrollaktivitäten sind Grundsätze und Verfahren, die sicherstellen sollen, dass die Entscheidungen des Managements beachtet werden. Sie tragen dazu bei, dass notwendige Maßnahmen getroffen werden, um den Unternehmensrisiken zu begegnen[19]. Beispielsweise dienen Kreditwürdigkeitsprüfungen von Kunden dazu, Zahlungsausfällen und Bewertungsrisiken im Jahresabschluss vorzubeugen. Mit Process Mining kann beobachtet werden, wann und durch wen für welche Geschäftsvorfälle welche Verarbeitungsschritte durchgeführt wurden. Daraus abgeleitet wird offensichtlich, welche unterschiedlichen Varianten es gibt. Basierend auf dem vorgegebenen Ablauf können die zulässigen von den potentiell schädlichen Varianten getrennt werden. Es wird nicht nur bestimmt, dass Schwächen in der internen Kontrolle existieren, sondern auch, mit welcher Eintrittswahrscheinlichkeit, welche Schäden zu erwarten sind. Auf diese Weise kann das interne Kontrollsystem einem Stresstest unterzogen werden, wie er im Bankensektor bereits üblich ist.

Unternehmenskommunikation

Information und Kommunikation dienen dazu, dass die für die unternehmerischen Entscheidungen des Managements erforderlichen Informationen in geeigneter und zeitgerechter Form eingeholt, aufbereitet und an die zuständigen Stellen im Unternehmen weitergeleitet werden[20]. Mit Process Mining kann der Informationsaustausch anhand von Log-Files der Netze und Server analysiert werden. Durch Kombination mit Methoden der sozialen Netzwerkanalyse kann der Informationsfluss zwischen Systemnutzern visualisiert und analysiert werden. Entwicklungen hierzu stehen noch an ihrem Anfang, haben aber großes praktisches Potential.

Überwachung

Durch die Unternehmensleitung ist permanent zu beurteilen, ob das interne Kontrollsystem sowohl angemessen ist als auch kontinuierlich funktioniert. Darüber hinaus hat das Management dafür Sorge zu tragen, dass festgestellte Schwächen im internen Kontrollsystem in geeigneter Weise abgestellt werden[21]. Die dargestellten Aktivitäten und Merkmale des internen Kontrollsystems können durch das Process Mining im Zeitverlauf dargestellt werden. Durch Kombination mit den Hauptbuch- und Nebenbuchjournalen können Kennzahlen zur Vermögens-, Finanz- und Ertragsentwicklung mit prozessbezogenen Kennzahlen ergänzt werden. Durch

Definition von Grenzwerten für die Ausprägung bestimmter Kennzahlen erhält der Prüfer einen guten Überblick, ob das Management seiner Überwachungsfunktion gerecht wird und wie es auf problematische Entwicklungen reagiert hat.

Ausblick

Das Verständnis für die internen Prozesse und Kontrollen geht bei zunehmender Digitalisierung verloren. Durch Einsatz des Cloud Computing wird diese Problematik sogar noch verschärft. Dies geschieht durch die Virtualität des Cloud Computing, wodurch der Prüfer die Zuordnung zwischen den virtuellen und realen Ressourcen und Dienstleistungen nicht mehr direkt beobachten kann. Diese Zuordnung ändert sich beim Einsatz des Cloud Computing ständig.

Durch Process Mining ist es möglich, die Übersicht wieder zu erlangen und die Zuordnung zwischen realer und virtueller Organisation im Zeitverlauf zu rekonstruieren und damit prüfbar zu machen. Es besteht jedoch Bedarf, das Process Mining zu ergänzen und zu verfeinern, insbesondere durch die Integration von Events aus der Cloud. Denn für Unternehmen und Prüfer gelten die Ordnungsmäßigkeits- und Sicherheitsanforderungen unabhängig davon, ob es sich um eine reale oder eine virtuelle Organisation handelt. Wir kooperieren mit einer Reihe internationaler Experten, um die notwendige betriebswirtschaftliche Forschung voranzutreiben und Anwendungsbarrieren aus Sicht der Praxis zu reduzieren.

Summary

To date, Cloud Computing has primarily been subject to research in the area field of Computer Science. We describe the managerial challenges with an emphasis focus on cost accounting, capital budgeting, and auditing when outsourcing internal functions to the cloud. In a cloud environment, activities of the real organization and the virtual organisationorganization are interrelated and not directly observable. Further, the interrelationship between real and virtual components changes quickly. Both, management and auditors are challenged by an increasing complexity and lack in of transparency of in processes outsourced to the cloud. Complexity and non-transparency cause risks in regard to security and compliance requirements. We propose to use Process Mining to handle complexity and non-transparency for to mitigateing the risks. Process Mining facilitates an enhanced understanding of processes through visualization and detailed analysis. Process Mining can be used by auditors to assess the operating effectiveness of internal controls. However, additional event data are necessary in order to apply Process Mining in the general form of Event Mining for auditing cloud computing systems, additional event data are necessary.

Anmerkungen/Literatur

1) Zur Abgrenzung von Cloud Computing gegenüber den verwandten Technologien Grid Computing, Utility Computing, Virtualisierung und Autonomic Computing siehe Zhang, Qi; Cheng, Lu; Boutaba, Raouf (2010): Cloud computing: state-of-the-art and research challenges. In: Journal of Internet Services and Applications 1, S. 7–18.
2) Glaser, H. (1992): Prozesskostenrechnung – Darstellung und Kritik. In: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung (ZfbF) 44. (3), S. 275–288.
3) Brasch, H.D. (1927): Zur Praxis der Unkostenschwankungen und ihrer Erfassung. In: Betriebswirtschaftliche Rundschau, 4 (4–5), 65–72; Günther, Th. W.; Riehl, A.; Rößler, R. (2014): Cost stickiness: state of the art of research and implications. In: Journal of Managerial Control 24, S. 301–308.
4) Rapp, Y. (1939): Economic Stages of Extension of a Telephone Network. Ericsson Technics, Stockholm 1939, Nr. 5, zitiert nach: Schneider, E. (1973): Wirtschaftlichkeitsrechnung, 8. Aufl., Tübingen u. Zürich 1973, S. 121.
5) Eine Abgrenzung wird vom BSI vorgenommen, vgl. Bundesamt für Sicherheit in der Informationstechnik, Eckpunktepapier (2012): Sicherheitsempfehlungen für Cloud Computing Anbieter, S. 18f.
6) Vgl. BSI, S. 17f.
7) BGH-Urteil 15.11.2006, XII ZR 120/04.
8) Lissen/Brünger/Damhorst (2014): IT-Services in der Cloud und ISAE 3402 – Ein praxisorientierter Leitfacen für eine erfolgreiche Auditierung, Heidelberg, Springer Gabler, S. 15f.
9) BGH-Urteil vom 4.3.2010, III ZR 79/09.
10) Lissen/Brünger/Damhorst, S. 16f.
11) Bundesministerium für Wirtschaft und Energie, Kompetenzzentrum Trusted Cloud (2014): Leitfaden – Haftungsrisiken beim Cloud Computing 10, S. 18f.
12) BSI, S. 69f.
13) Für Einzelheiten zum Datenschutz siehe BSI, S. 73ff.
14) Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW): Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), Tz. 23.
15) IDW RS FAIT 1 Tz. 25.
16) Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW): Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n.F.) Tz. 29.
17) IDW PS 261.30.
18) IDW PS 261.31.
19) IDW PS 261.32.
20) IDW PS 261.33.
21) IDW PS 261.34.

Die Autoren

Ludwig Mochty studierte Technische Mathematik an der TU Wien, wo er auch promovierte, Betriebswirtschaftslehre und Operations Research am Institut für Höhere Studien in Wien und Wirtschaftsinformatik an der Universität Wien. Seit 1994 hat er den Lehrstuhl für Wirtschaftsprüfung, Unternehmensrechnung und Controlling an der Universität Duisburg-Essen inne. Neben seiner akademischen Tätigkeit ist er seit 1982 in verschiedenen Funktionen in der Wirtschaftsprüfunspraxis tätig, wo er unter anderem zeitgemäße computergestützte Prüfungsverfahren entwickelt und anwendungsbezogen testet.

Michael Wiese studierte Wirtschaftswissenschaften an der Universität Duisburg-Essen und promovierte am Lehrstuhl für Wirtschaftsprüfung, Unternehmensrechnung und Controlling. Er ist Wirtschaftsprüfer bei der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Dort leitet er die Forschung und Entwicklung für die Serviceline Assurance in Deutschland, Österreich und der Schweiz. Sein Entwicklungsfokus liegt auf dem Einsatz computergestützter Verfahren in der Prüfungspraxis, zum Beispiel dem Process Mining.

DOI: 10.17185/duepublico/70379
URN: urn:nbn:de:hbz:464-20190813-123547-4

Erschienen in: UNIKATE 50 (2017), S. 76-85