FORSCHUNGSZENTRUM FZID

UNIVERSITÄT HOHENHEIM

FZID Discussion Papers

CC Health Care Management

Discussion Paper 74-2013

RISIKEN AUS CLOUD-COMPUTING-SERVICES: FRAGEN DES RISIKOMANAGEMENTS UND ASPEKTE DER VERSICHERBARKEIT

Andreas Haas,
Annette Hofmann

Universität Hohenheim | Forschungszentrum Innovation und Dienstleistung

www.fzid.uni-hohenheim.de

Discussion Paper 74-2013

Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit

Andreas Haas, Annette Hofmann

Download this Discussion Paper from our homepage:
https://fzid.uni-hohenheim.de/71978.html

ISSN 1867-934X (Printausgabe)
ISSN 1868-0720 (Internetausgabe)

Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit

Andreas Haas • Annette Hofmann

Zusammenfassung Unternehmen stehen heute aufgrund ökonomischer Anreize verstärkt vor der Entscheidung, die bisher intern gelagerte Datenverarbeitung und Geschäftsprozesse auf einen externen Anbieter von Cloud-Computing-Dienstleistungen auszulagern. Diese neuartige Form des IT-Outsourcing verändert jedoch die Risikosituation, der Anbieter und Nachfrager ausgesetzt sind, teilweise erheblich. Heutige Cyber-Versicherungsprodukte sind noch nicht auf versicherungstechnische und vertragsrechtliche Besonderheiten des Cloud-Computing ausgelegt. Zudem führen die stark interdependenten Netzwerkstrukturen von Cloud-Anbietern, verbunden mit einer fehlenden Unabhängigkeit der Einzelrisiken in einer Cloud-Infrastruktur zu starken Kumulproblemen im Schadenfall und eröffnen Fragen der grundsätzlichen Versicherbarkeit. Die Analyse zeigt, dass neben einer Anpassung heutiger Versicherungsprodukte auf den Kontext Cloud-Computing auch innovative Risikodiversifikationsmöglichkeiten geschaffen werden sollten, um Risiken aus Cloud-Computing-Services auf ein Versicherungsunternehmen zu transferieren. Dieser Artikel erörtert die Risikosituation bei der Nutzung von Cloud-Services, bietet eine Klassifikation der Risiken an und diskutiert zentrale Fragen der Versicherbarkeit sowie Lösungsansätze für das Risikomanagement.

Abstract Cloud-Computing services are changing the risk situation of IT-outsourcing and represent a challenge for the insurance industry. The most important problem to guarantee insurability of these emerging risks is that they are not stochastically independent. On the one hand, the interdependent network structure of these risks implies a significant contagion risk; on the other hand, new risks emerge that have not been addressed by existing (cyber risk) policies so far. Insurance concepts should be supported by innovative risk diversification concepts for cloud computing service. Addressing and classifying the new risks resulting from Cloud-Computing services, this article discusses insurability issues and risk management solutions.

Andreas Haas
Lehrstuhl für Versicherungswirtschaft und Sozialsysteme
Universität Hohenheim
Fruwirthstraße 48, 70599 Stuttgart
E-mail: a.haas@uni-hohenheim.de

Annette Hofmann
Institut für Versicherungsbetriebslehre
Universität Hamburg
Von-Melle-Park 5, 20146 Hamburg
E-mail: hofmann@econ.uni-hamburg.de

1 Einleitung

Der Begriff „Cloud-Computing“ beschreibt Geschäftsmodelle, die dem Nutzer Zugriff auf Rechenleistung, Speicherplatz, Betriebssysteme, Plattformen zur Softwareentwicklung, Datenbanken oder online-basierte Anwendungen gewähren. Eine Besonderheit bei dieser Form des IT-Outsourcing ist die Trennung der Computerressourcen von der zugrundeliegenden IT-Infrastruktur. Im Gegensatz zum klassischen Outsourcing erfolgt die Nutzung ad hoc und beliebig skalierbar.

Aufgrund der Vorteile und neuen Nutzungsmöglichkeiten die Cloud-Computing bietet, wird die IT- und Softwarelandschaft nachhaltig verändert. Viele neue Geschäftsmodelle sind erst aufgrund der Kostenvorteile und Flexibilität der Cloud-Infrastrukturen realisierbar geworden. Aber auch etablierte Standardanwendungen, wie bspw. Microsoft Office, werden zunehmend in „in die Cloud“ verlagert und sind dadurch für den Nutzer ubiquitär verfügbar – mit hoher Akzeptanz seitens der Nutzer.[1] Während die große Popularität von Cloud-Computing-Lösungen bei Privatpersonen auf attraktive Dienstleistungen[2] zurückzuführen ist, sind die Gründe für den zunehmenden Einsatz von Cloud-Computing-Services in Unternehmen vielfältiger. Preismodelle auf Basis eines nutzungsabhängigen Serviceentgelts reduzieren Investitionen in den Aufbau von IT-Infrastruktur und laufende IT-Administration. Bestehende IT-Landschaften können durch Rückgriff auf Cloud-Dienste schnell erweitert, Eintrittsbarrieren in neue Geschäftsfelder gesenkt und die Bildung neuer Unternehmensprozesse erleichtert werden. Insbesondere für kleine und mittelständische Unternehmen eröffnen Geschäftsmodelle auf Basis von Cloud-Computing die Möglichkeit, die Leistungsfähigkeit und Vorteile großer IT-Infrastrukturen für die eigenen Geschäftsprozesse zu nutzen. Allerdings gehen diese Vorteile mit Fragen der Dienstverfügbarkeit und Datensicherheit einher. Cloud-Kunden müssen sich intensiv mit der Fragestellung auseinandersetzen, welche wirtschaftlichen Konsequenzen der Ausfall bzw. die Fehlfunktion einer cloudbasierten IT-Infrastruktur für das eigene Unternehmen zur Folge haben kann und wie daraus resultierende Schäden abgesichert werden können. Ein prominentes Beispiel für das Risikopotential von Cloud-Computing-Services sind die Ausfälle der Amazon Cloud-Infrastruktur Ende 2012. Zahlreiche populäre Dienste wie Netflix, Pinterest, Instragram, The Guardian oder Urbanspoon waren von den Ausfällen bei dem weltweit größten Cloud-Service-Provider betroffen. Allein der Videostreaming-Dienst Netflix mit mehr als 25 Millio-

[1] Vgl. Hachmann (2013).

[2] Hierzu zählen bspw. Medienstreaming Dienste um Musik, Filme und Bücher jederzeit, fast unbegrenzt und ggü. des Einzelkaufs deutlich günstiger auf Notebooks und Mobiltelefonen zu konsumieren.

nen Abonnenten in den USA ist bei diesen Ausfällen erheblichen Reputationsschäden und Folgekosten – wie etwa der Erstattung der Nutzungsgebühr an seine Kunden - ausgesetzt. Liegen zudem kritische Unternehmens- oder personenbezogene Daten auf einer solchen Infrastruktur, sind bei Fehlfunktionen Schadenkosten aufgrund von Datenschutzverletzungen, Schadenersatzansprüchen oder Verlust des Kundenstamms möglich. Bislang finden die Risiken bei Nutzung von Cloud-Computing noch zu wenig Beachtung.

Die Risikolandschaft des Cloud-Computing ist aufgrund neuer technischer, rechtlicher und strategischer Risiken deutlich differenzierter als bei klassischen IT-Outsourcing-Lösungen. Die Unsicherheit hinsichtlich der mit Cloud-Computing verbundenen komplexen und neuartigen Risikosituation ist für Unternehmen immer noch ein wesentlicher Grund, Cloud-Dienste nicht zu nutzen.[3] Allerdings können die betriebswirtschaftlichen Vorteile des Cloud-Computing mittel- bis langfristig nicht ignoriert werden. Die Analyse der Risikosituation von Cloud-Computing-Dienstleistungen und eine Diskussion von Lösungsansätzen für den Risikotransfer mit einem Fokus auf versicherungstechnische Fragestellungen ist aus Sicht der Autoren elementar für den weiteren Erfolg des kommerziellen Cloud-Computing.

Dafür wird zunächst eine Risikoanalyse basierend auf den wesentlichen Charakteristika von Cloud-Computing durchgeführt, um den Einfluss der am Markt verfügbaren Varianten auf die Risikosituation der Anbieter und Nutzer darzustellen. Darauf aufbauend werden die Besonderheiten von Cloud-Risiken diskutiert und als neue Form der Cyber-Risiken klassifiziert. Die Analyse identifiziert zudem versicherungstechnische und vertragsrechtliche Probleme, deren Ausmaß die grundsätzliche Versicherbarkeit beeinflussen kann. Insbesondere die komplexen Abhängigkeiten zwischen den Cloud-Anbietern bergen ein hohes Kumulpotential im Schadenfall. Damit verbunden ist ein hohes Gesamtschadenpotential, das vor allem von den führenden Cloud-Anbietern ausgeht. Dies ist ein wesentlicher Aspekt in der nachfolgenden Diskussion über die grundsätzliche Versicherbarkeit von Cloud-Computing. Es kann gezeigt werden, dass die Versicherbarkeit zwar grundsätzlich möglich ist, heutige Cyberrisk-Policen jedoch nicht ausreichend auf die spezielle Risikosituation des Cloud-Computing ausgelegt sind. Sowohl Anbieter als auch Nachfrager von Cloud-Dienstleistungen sind als Versicherungsnehmer geeignet - Versicherungsprodukte müssen jedoch Haftungslimits, Prämiendifferenzierung und Selbstbehalte beinhalten sowie die Cloud-Form berücksichtigt.

Abschließend werden weitere Möglichkeiten der Risikomanagements von Cloud-Risiken aufgezeigt. Eine Zusammenfassung rundet die Analyse ab.

[3] Vgl. *Deloitte* (2011), S. 9; vgl. *Symantec* (2011), S. 7; vgl. *KPMG* (2012), S. 17.

2 Definition und Formen von Cloud-Computing

Cloud-Computing verändert den Umgang mit IT-Outsourcing nachhaltig. Geschäftsmodelle auf Basis von Cloud-Computing haben das Potential, die heutigen Soft- und Hardwareressourcen in Unternehmen zu komplementieren oder sogar zu substituieren. Cloud-Computing ist allerdings keine grundsätzlich neue Entwicklung, sondern vielmehr die Verschmelzung bestehender und neuer Technologien, die sich für den Einsatz in großen Datenzentren eignen.

2.1 Definition und wesentliche Charakteristika von Cloud-Computing

In der Literatur ist die Definition von *Mell und Grance (2011)* verbreitet, die den Begriff Cloud-Computing für das National Institute of Standards and Technology (NIST) folgendermaßen umschreiben:

> *„Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[4]

Mit dem Einsatz von Cloud-Computing werden die in Datenzentren verfügbaren IT-Ressourcen zu einem verhältnismäßig einfach und flexibel handelbaren Gut. Vereinfacht dargestellt separiert Cloud-Computing die Hardwareressourcen (wie bspw. Rechenleistung oder Speicherplatz) von der bereitgestellten IT-Dienstleistung. Dem Cloud-Nutzer wird aus dem Pool von Hardwareressourcen ein virtuelles IT-Bündel zur Verfügung gestellt, das nur einen Teil der verfügbaren Leistung eines Servers oder ein Leistungsbündel aus mehreren Servern umfasst. Die Trennung von Hardware und Dienstangebot erfolgt mithilfe von Virtualisierungstechnologien und ermöglicht die gemeinsame Nutzung physischer IT-Ressourcen durch mehrere Anwender.

2.2 Klassifikation von Cloud-Computing-Service-Modellen

Cloud-Computing-Services lassen sich nach dem Funktions- und Bereitstellungsumfang differenzieren. Bei dem grundlegenden Service-Modell *Infrastructure as a Service* (*IaaS*) bieten Cloud-Provider einen Zugriff auf die in großen Datenzentren umfangreich verfügbaren IT-Ressourcen wie Rechenleistung, Datenspeicher, Datenbanken und Netzwerkkapazitäten.[5] Das *IaaS*-Modell ermöglicht die Nutzung und die vollständige Kontrolle standardisierter IT-Ressourcen ohne die i.d.R. hohen Investitions- und Wartungskosten für eigene Rechenzentren.

[4] *Mell/Grance* (2011), S. 3.
[5] Detailliertere Kategorisierungen von *IaaS* kann der interessierte Leser bspw. *Youseff et al.* (2008) entnehmen.

Es dient heute zahlreichen populären Geschäftsmodellen (bspw. Mediastreaming-[6] oder Datenspeicher-Diensten) als technologische Grundlage.[7] *Platform as a Service* (*PaaS*) stellt eine online-basierte Entwicklungsumgebung bereit, um cloudfähige Software programmieren, installieren und anbieten zu können. *PaaS* ist darauf ausgelegt das Zusammenspiel von Cloud-Hardware und -Software bestmöglich zu realisieren, mit dem Ziel die IT-Ressourcenauslastung zu optimieren.[8] *Software as a Service* (*SaaS*[9]) bezeichnet im Cloud-Computing online-basierte Anwendungen auf Basis einer Cloud-Infrastruktur. Insbesondere bei ressourcenintensiven Anwendungen können *SaaS*-Anbieter verhältnismäßig einfach Wachstums- und Kostenpotentiale ausschöpfen, da sich die zur Nutzung notwendigen Hardwareressourcen stets der Nachfrage anpassen. Auf den drei Cloud-Service-Modellen *IaaS*, *PaaS* und *SaaS* aufbauend entwickeln sich zunehmend auch neue Cloud-Dienste, wie bspw. der speziell auf Unternehmenskunden ausgerichtete *Business-Process-as-a-Service* (*BPaaS*). Darunter wird die Abbildung organisationsübergreifender Geschäftsprozesse in *SaaS*-Applikationen verstanden.

Cloud-Service-Modell	Bereitgestellte Dienstleistung	Anbieter-/ Produktbeispiel
Infrastructure as a Service (IaaS)	Basis IT-Infrastruktur und Hardware-Komponenten als Service	AppNexus, Amazon EC2, Google Sungard Enterprise Cloud
Platform as a Service (PaaS)	Technische Frameworks, Entwicklungsplattformen	Google App Engine, Microsoft Azure Services, Force.com
Software as a Service (SaaS)	online-basierte Anwendungen	Microsoft Windows Live Services, Google Mail, Dropbox, Spotify, Netflix
Business Process as a Service (BPaaS)	Abbildung organisations- übergreifender Geschäftsprozesse als SaaS	Microsoft Office 365, Salesforce.com, SAP, Plex.com

Tabelle 1: Übersicht Cloud-Service-Modelle und Dienstleistungen[10]

SaaS ist momentan der attraktivste Cloud-Service für deutsche Unternehmen.[11] Die Gründe hierfür liegen insbesondere in den niedrigen Eintrittsbarrieren zur Nutzung, in der flexiblen Verfügbarkeit von Anwendungen auf diversen Endgeräten, den Möglichkeiten zur Kollaborati-

[6] Mediastreaming Dienste, wie beispielsweise Spotify oder Netflix, stellen Musik oder Filme über das Internet als Dienstleistung bereit.
[7] Vgl. *Bitkom* (2010), S. 16.
[8] Vgl. *CSA* (2011), S. 15.
[9] Im folgenden wird SaaS auch vereinfacht als Cloud-Software bezeichnet.
[10] Eigene Darstellung in Anlehnung an *Bitkom* (2010), S. 16; *Wouter/Lambrette* (2012), S. 2-4; *CSA* (2011); S. 15-19, *Rhoton* (2011), S.61-71.
[11] Vgl. *Mell/Grance* (2011), S. 3; vgl. *Jansen/Grance* (2011), S. 4; vgl. *Youseff et al.* (2008), S. 4.

on sowie einer Veränderung der Kostenstruktur. Die bisherigen fixen Lizenz- und Wartungskosten können gegen eine (niedrigere) variable, monatliche Nutzungsgebühr substituiert werden.[12] Einen Überblick über die Nutzung von Cloud-Services in deutschen Unternehmen gibt *Abbildung 1*.

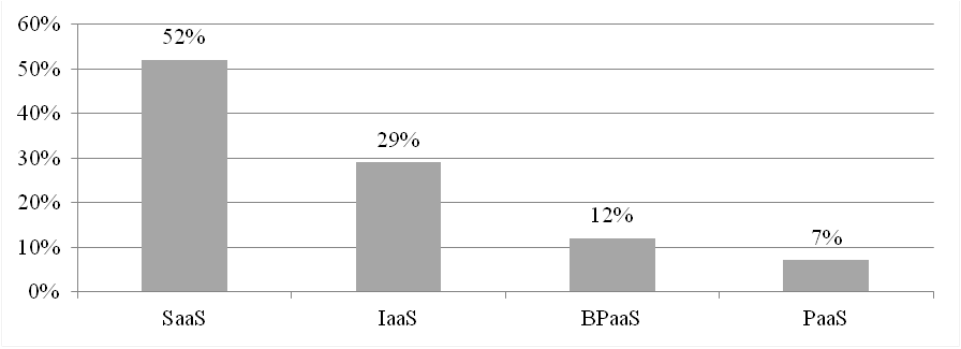

Abbildung 1: Nutzungsanteil von Cloud-Dienstleistungen in deutschen Unternehmen.[13]

2.3 Cloud-Computing-Deployment-Modelle

Cloud-Computing-Angebote können grundsätzlich in *Public- und Private-Clouds* eingeteilt werden. Diese beiden sog. *Cloud-Deployment-Modelle* unterscheiden sich hinsichtlich der Betreiber-, Eigentümer- und Nutzerstruktur sowie des Standortes des Rechenzentrums. Diese Differenzierung ist vor allem bei der späteren Betrachtung der Risikosituation und des Risikomanagements von Bedeutung.

Eine *Public-Cloud* ist die ursprüngliche Form des Cloud-Computing. Zur Bereitstellung eines Public-Cloud-Services werden die IT-Ressourcen mehrerer weltweit verteilter Datenzentren eines Anbieters genutzt. Dieser Service ist darauf ausgelegt, dass die Ressourcen automatisiert und innerhalb kurzer Zeit dem Cloud-Kunden zur Nutzung zugänglich sind. In einer *Public-Cloud* werden die Kundendaten meist nur logisch, d.h. mithilfe von Software-Mechanismen, voneinander getrennt. Dieses Konzept der Ressourcenvirtualisierung ermöglicht eine sehr hohe Auslastung der Rechenzentren und bildet die Grundlage für die Realisierung hoher Skaleneffekte im Cloud-Computing. *Public-Cloud-Infrastrukturen* verfügen gegenüber den privaten Cloud-Infrastrukturen i.d.R über ein niedrigeres garantiertes Sicherheitsniveau, standardisierte und nicht verhandelbare Dienstvereinbarungen, nicht definierbare Datenstandorte oder Nutzerbeschränkungen. Der Online-Datenspeicherdient Dropbox und Anwendungen wie Google Mail sind bekannte Beispiele für *Public-Cloud-Anbieter*.

Die *Private-Cloud* ist eine Spezialform des Cloud-Computing, die starke Parallelen zum

[12] Vgl. *Furht/Escalante* (2010), S. 22-24; *Deloitte* (2011), S. 12.
[13] Eigene Darstellung in Anlehnung an *Deloitte* (2011), S.12.

klassischen IT-Outsourcing aufweist. In einer Private-Cloud kann beispielsweise die exklusive Nutzung der Cloud-Infrastruktur durch eine physisch getrennte Datenhaltung oder durch die Wahl des Standortes der Datenspeicherung und -verarbeitung garantiert werden. Die Dienstverfügbarkeit und das allgemeine Sicherheitsniveau sind in der Regel *stärker* ausgeprägt als bei Public-Cloud-Strukturen. Der größte Nachteil gegenüber einer Public-Cloud ist in den für Unternehmen deutlich höheren Nutzungs- und Transaktionskosten zu sehen. Preisliche, vertragliche und rechtliche Gestaltungselemente der *Private-Cloud* wirken wie Eintrittsbarrieren zur Nutzung der Dienste. Der Kundenkreis einer *Private-Cloud*-Infrastruktur ist daher in der Regel definierbar und kleiner.

Private-Clouds können in verschiedenen Formen umgesetzt werden. Bei einer *On-Premise Private-Cloud* werden die Daten im unternehmenseigenen Rechenzentrum gespeichert und selbst verwaltet. In einer weiteren Variante, der *Managed-Private-Cloud*, wird die Administration an einen spezialisierten Cloud-Dienstleister übertragen, während die Daten weiterhin im Unternehmensrechenzentrum verbleiben. Darüberhinaus kann, wie bei einer *Public-Cloud*, auf die IT-Infrastruktur eines spezialisierten Private-Cloud-Providers zurückgegriffen werden. Dieser ist dann für Speicherung und Verwaltung der Daten zuständig (*Off-Premise* oder *Outsourced-Private-Cloud*). Die Begriffe *Community-Cloud* und *Hybrid-Cloud* subsumieren weitere Kombinationen der hier aufgezeigten Modelle und sind somit keine eigenständigen Cloud-Typen.[14] Eine Übersicht der unterschiedlichen Ausprägungen von Cloud-Modellen unter Berücksichtigung wesentlicher Abgrenzungskriterien und traditioneller IT-Umgebungen bietet *Abbildung 2*.

	Hybrid Cloud				
			Community Cloud		
	Traditionelle IT-Umgebung	Private Cloud	Managed Private Cloud	Outsourced Private Cloud	Public Cloud
Verwaltung	Unternehmen		externer IT-Dienstleister		
Standort	Unternehmen			externer IT-Dienstleister	
Skalierbarkeit	eingeschränkt			(quasi) uneingeschränkt	
Bezahlmodell	Fixkosten unabhängig von Nutzung			Nutzungsabhängige Kosten (pay as you go)	
Zugriff	internes Unternehmensnetzwerk			Internet & VPN	
Nutzung	individuelle Anpassung				standardisierte Prozesse
Nutzer	Einzelnes Unternehmen				Mehrere Unternehmen

Abbildung 2: Ausprägungen von Cloud-Computing-Modellen[15]

[14] Vgl. *Armburst et al.* (2010), S.52-53; vgl. *Bitkom* (2010), S. 18; vgl. *Mell/Grance* (2011), S. 3.
[15] Eigene Darstellung in Anlehnung an *CSA* (2011), S.19; *Mell/Grance* (2011), S. 3.

2.4 Cloud-Computing-Akteure in der Wertschöpfungsbetrachtung

Cloud-Provider können ihre Dienstleistungen alleinstehend oder in Kombination mit anderen Cloud-Anbietern vermarkten. Die Geschäftsmodelle im Cloud-Computing entsprechen einer Wertschöpfungskette, wobei die Dienste stets aufeinander aufbauen. Darüber hinaus kann es auch zu Austauschprozessen zwischen den Anbietern bzw. Diensten vor- oder nachgelagerten Wertschöpfungsstufen kommen, so dass die Bereitstellungsstrukturen einem *Wertschöpfungs-netzwerk* entsprechen.[16]

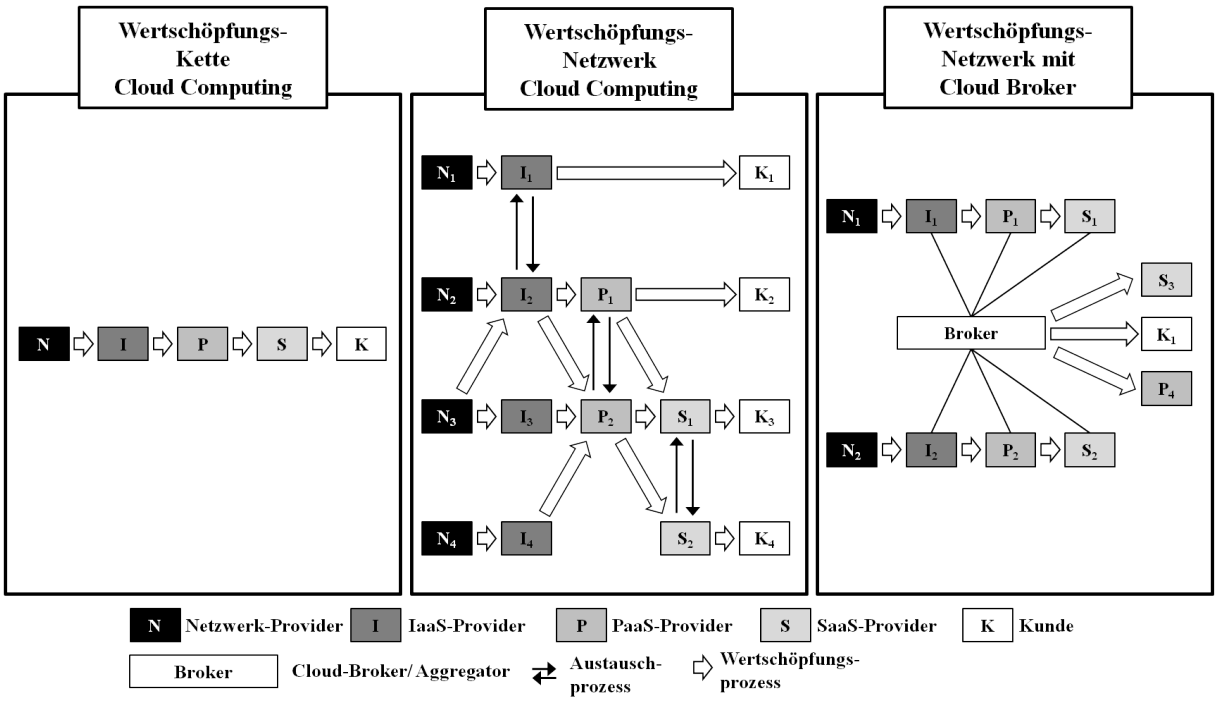

Abbildung 3: Wertschöpfungsnetzwerk Cloud-Computing[17]

Zu den Akteuren im Cloud-Computing zählen die Netzbetreiber, die Cloud-Anbieter, Kunden und ggfs. neue Intermediäre am Markt. Den Kern eines Cloud-Computing-Netzwerkes bilden Unternehmen wie bspw. Amazon, Google oder Microsoft (*IaaS-Provider)*, die IT-Ressourcen aus ihren Datenzentren als Cloud-Service bereitstellen. Diese werden auf einer späteren Wert-schöpfungsstufe von Unternehmen (*SaaS-Provider*) genutzt, um darauf laufende Cloud-Anwendungen anbieten zu können. Zwischen diesen beiden Akteuren stehen Anbieter von Entwicklungsumgebungen (*PaaS-Provider)* und bilden die Schnittstelle zwischen cloudfähiger Software und Hardware. *Netzbetreiber* verbinden mit der Bereitstellung des Zugangs zu ihren Kommunikationsnetzen Nachfrager und Anbieter im Cloud-Computing.

[16] Vgl. *Sydow* (1992), S. 79; vgl. *Leimeister et al.* (2010), S. 7.
[17] Eigene Darstellung in Anlehnung an *Leimeister et al.* (2010), S.7.

Die Strukturen von komplexen Lieferketten bzw. Liefernetzwerken (*Supply Chains*), wie sie hier vorzufinden sind, führen zu starken Abhängigkeiten zwischen den Anbietern bei der Dienstbereitstellung und erschweren das Risikomanagement. Neue Intermediäre am Markt (Cloud-Broker) können durch die Vermittlung von Anbieter und Nachfrager auf jeder Wertschöpfungsstufe und die Aggregation von Dienstleistungen die Abhängigkeiten im Cloud-Computing verringern. Deren Bedeutung für das Risikomanagement wird bei der späteren Risikobewertung wieder aufgegriffen.

Cloud-Kunden sind mögliche Interdependenzen des Marktes in der Regel nicht bekannt. Sie bekommen die jeweiligen Servicearten (IaaS, PaaS, SaaS) zur zeitlich begrenzten Nutzung durch unterschiedliche Dienstleister zur Verfügung gestellt. Während die direkten Vertragsverhältnisse zwischen Anbieter und Kunden offensichtlich sind, werden Kooperationen zwischen den Cloud-Diensten oftmals nicht dargelegt. Für Unternehmen kommt es aufgrund von dieser Form von Informationsasymmetrie zu einer starken Intransparenz und erschwert das Risikomanagement bei der Auswahl geeigneter Cloud-Anbieter. *Abbildung 4* stellt die Möglichkeiten der Vertragsverhältnisse zwischen den Cloud-Akteuren dar.

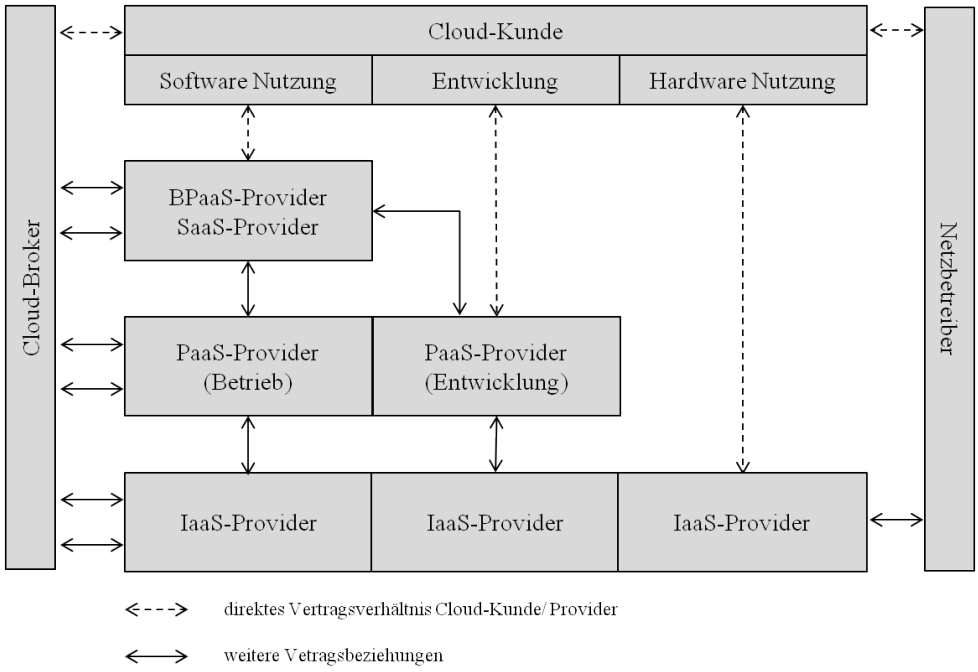

Abbildung 4: Mögliche Konstellation von Vertragsverhältnissen im Cloud-Computing[18]

[18] Eigene Darstellung in Anlehnung an *Bitkom* (2010), S. 36.

3 Analyse der Risikosituation und Versicherbarkeit von Cloud-Computing

3.1 Cloud-Risiken im Kontext von IT-/ Cyber-Risiken

Risiken, die im Zusammenhang mit der Verarbeitung von digitalen Informationen stehen, werden allgemein als *IT- oder Cyber-Risiken*[19] bezeichnet und zählen zu den *operationellen Unternehmensrisiken*. Cyber-Risiken unterliegen aufgrund der Weiterentwicklung von Technologie, Geschäftsmodellen und (internationaler) Gesetzgebung einem stetigen Änderungsprozess. Für die Versicherungswirtschaft stellen derartige instabile Risikoursachensysteme eine besondere Herausforderung bei der Kalkulation und der Ausgestaltung geeigneter Versicherungsprodukte dar. Neben diesem Änderungsrisiko, müssen spezifische Merkmale von Cyber-Risiken, wie bspw. starke Interdependenzen zwischen den Einzelrisiken in einem Schadenfall und deren Auswirkung auf das Gesamtschadenpotential, berücksichtigt werden.[20] Diese Abhängigkeiten können zu weltweiten, aber auch regional begrenzten Kumulproblemen führen und sind bei einem versicherungstechnischen Risikotransfer entsprechend relevant.

Die Versicherungswirtschaft hat für das besondere Schadenspektrum, das durch den Einsatz von Informationssystemen bzw. elektronischer Datenverarbeitung hervorgerufen wird, spezielle Cyberversicherungsprodukte vorgesehen. Es können Risiken aus Datenverlust und –diebstahl, Verstößen gegen (Daten-)Schutzgesetze, Ausfallschäden und Betriebsunterberechnungen, entgangenem Gewinn, Reputationsverlusten oder auch Hackerattacken auf ein Versicherungsunternehmen übertragen werden. Für Unternehmen bieten sich diese Versicherungsprodukte ergänzend zu klassischen Deckungsvarianten der Industriesach-, Unternehmenshaftplicht- oder Vertrauensschadenversicherung an.[21]

Grundsätzlich sind die *Risiken aus der Nutzung von Cloud-Computing-Dienstleistungen* auch der Kategorie der Cyber-Risiken zuzuordnen. Jedoch sind aufgrund der bisher nicht ausreichend analysierten Risikosituation und geringen Erfahrungen mit Schadenpotentialen Cloud-Computing-Dienstleistungen von den heute verfügbaren Cyberversicherungspolicen überwiegend ausgeschlossen.[22] Für den versicherungstechnischen Risikotransfer ist daher eine Anpas-

[19] Die Abgrenzung von IT- und Cyber-Risiken ist in der Literatur nicht immer eindeutig. IT-Risiken beziehen sich in der Regel auf die physischen IT-Ressourcen wie Hardware, Cyber-Risiken betreffen die digitale Datenverarbeitung. Im Folgenden wird in Einklang mit der englischsprachigen Literatur der Begriff Cyber-Risiken allgemein für Risiken im Zusammenhang mit Informationstechnologien verwendet.

[20] Zur Bedeutung von Korrelation und Interdependenz von Einzelrisiken im Bereich Cyber-Risiko vgl. *Böhme/ Kataria* (2006); *Hofmann/Ramaj* (2011).

[21] Vgl. *Koch* (2005), S. 126.

[22] Eine Analyse der Cyber-Policen erfolgte im Zeitraum Dezember 2012 bis Februar 2012. In den hierbei vorliegenden Cyber-Policen war nur bei einer Cyberrisk-Police „Cloud-Computing“ als optionaler Bestandteil erwähnt. Eine weitere Differenzierung bestimmter Cloud-Kriterien in den Versicherungsbedingungen erfolgte jedoch nicht.

sung existierender Cyber-Policen auf die Risikosituation von Cloud-Computing unter Berücksichtigung der verschiedenen Cloud-Modelle[23] vorzunehmen. Im Folgenden wird ein Überblick über die Risikolandschaft des Cloud-Computing gegeben, um Ansatzpunkte einer möglichen versicherungstechnischen Überprüfung cloudspezifischer Risiken aufzuzeigen.

3.2 Die Cloud-Computing-Risikosituation

Zur Analyse der Risikosituation des Cloud-Computing werden Cyber-Risiken in drei Kategorien untergliedert, um von den bereits versicherbaren Cyber-Risiken cloudspezifische Risiken abzugrenzen und die weitere Betrachtung auf diese einzugrenzen. *„Allgemeine Cyber-Risiken"* treten beim Einsatz von Informationstechnologien, digitaler Datenverarbeitung und klassischem IT-Outsourcing auf und können (weitgehend) unverändert auf Cloud-Computing übertragen werden. Die Kategorie der *„veränderten Cyber-Risiken"* umfasst Risiken, deren Bedeutung sich im Kontext des Cloud-Computing wandelt – bspw. hinsichtlich des Schadenpotentials oder der Schadenwahrscheinlichkeit. Als dritte Kategorie treten *„cloudspezifische Cyber-Risiken"* als neuartige oder technologiebezogene Risiken des Cloud-Computing hervor. Die folgende Aufarbeitung konzentriert sich auf die veränderten und cloudspezifischen Cyber-Risiken.

3.2.1 Abhängigkeit von den Cloud-Service-Providern unter starken Informationsasymmetrien

Mit der Nutzung von Cloud-Services wird die physische Kontrolle über IT-Ressourcen und die Verantwortung für die Datenhaltung, -verarbeitung und -bereitstellung vollständig an einen oder mehrere Cloud-Service-Provider übertragen. Unternehmen müssen dabei besonders auf die Umsetzung ausreichender Sicherheitsmaßnahmen seitens des Anbieters vertrauen. Informationen darüber werden jedoch insbesondere bei Public-Clouds i.d.R. nicht offengelegt. Verstärkt wird dieses Problem durch die Vielzahl der Beteiligten an der Bereitstellung von cloudbasierten Leistungen wie Software-as-a-Service. Alle angreifbaren Ebenen – von der Infrastruktur bis hin zum Softwareangebot und deren Schnittstellen – müssen ein verlässliches Sicherheitsniveau gewährleisten.[24] Durch die fehlende Transparenz und die Wertschöpfungsstruktur bestehen seitens der Nutzer erhebliche Informationsasymmetrien hinsichtlich der Sicherheitsbemühungen und zugrundeliegenden Kooperationen.

Dies ist insbesondere deshalb von besonderer Bedeutung, da sich bei Nicht-Erfüllung der zugesagten Dienstverfügbarkeit oder bei Datenverlusten die Entschädigungsleistung seitens

[23] Es sollte sowohl zwischen Deployment- als auch zwischen Service-Modellen unterschieden werden.
[24] Vgl. *CSA* (2010), S.9; vgl. *ENISA* (2009), S.33-43.

eines Public-Cloud-Providers auf die Höhe des monatlichen Nutzungsentgeltes beschränkt oder sogar vertraglich ganz ausgeschlossen ist. Dem möglichen Risiko eines Unternehmens, das Cloud-Computing nutzt, wird im Schadenfall folglich nicht Rechnung getragen.[25] Kleine und mittlere Unternehmen beachten solche kritischen Aspekte bei Nutzung von Public-Cloud-Diensten häufig noch nicht in ausreichendem Maße. Gefördert wird dies u.a. auch durch fehlende Hinweise auf mögliche Risiken seitens der Anbieter. Darüber hinaus ist auch die Beurteilung der rechtlichen Situation für vorgenannte Nutzer schwierig, da große Datencenter häufig in den USA liegen mit dem dort anwendbaren Recht. Es fehlt bislang eine entsprechende deutsche Rechtsprechung, die insbesondere den Ausschluss von Haftung im Cloud-Kontext über AGBs näher bestimmen würde. All dies muss jedoch in einem wirksamen (unternehmensinternen) Risikomanagement berücksichtigt werden.

3.2.2 Aspekte des Datenschutzes

Von dem unautorisierten Zugriff Dritter[26] auf Daten, der Datenmanipulation oder dem Datenverlust, kann ein erhebliches wirtschaftliches Risiko für Unternehmen ausgehen. Insbesondere bei der Verarbeitung sensibler Kundendaten sind die Maßnahmen des Cloud-Providers zur Einhaltung von (weltweit differierenden) Datenschutzvorschriften und Datensicherheit von erheblicher Bedeutung. U.a. bei personenbezogenen Daten muss der Cloud-Anbieter rechtsverbindlich und nachweisbar zusichern können, dass die überlassenen Daten innerhalb eines Landes oder am vereinbarten Ort verbleiben. Dies ist insbesondere im Hinblick auf die Konformität der jeweiligen Datenschutzvorschriften notwendig. Public-Cloud-Infrastrukturen sind in der Regel auf eine weltweite Datenverarbeitung ausgelegt. Softwarenagebote die darauf aufbauen sind somit ggf. den Schutzanforderungen nicht gewachsen. Auch schließen die fehlenden Verhandlungsmöglichkeiten bei Public-Cloud-Angeboten vertragsrechtliche Anpassungen aus.

Es bieten sich der Übergabe kritischer Daten an einen Provider Verschlüsselungsmechanismen an, allerdings ist eine Verarbeitung der Daten bei Verschlüsselung ausgeschlossen bzw. eingeschränkt. Kommt es trotz Sicherheitsmaßnahmen zur Offenlegung sensibler Kunden- oder Geschäftsdaten, kann dies ein existenzbedrohendes Risiko für ein Unternehmen darstellen. Die Konsequenzen reichen von Reputationsschäden bis hin zum Verlust von unternehmensspezifischem Know-how und Wettbewerbsvorteilen.

Cloud-Kunden sind zudem auf eine zuverlässige und schnelle Informationspolitik des Cloud-Providers im Schadenfall angewiesen, da Datenschutzbestimmungen, ggf. die zeitnahe

[25] Vgl. *Bradshaw et al.* (2011), S. 202.
[26] Es sind sowohl Hackerangriffe als auch Zugriffe eigener Mitarbeiter möglich.

Meldung einer Datenschutzverletzung vorsehen und eine Missachtung sanktionieren. Letztlich können Fragen der Datensicherheit auch nach Beendigung der Vertragsbeziehung relevant sein, bspw. wenn die genutzten Cloud-Provider kein ausreichend sicheres Verfahren zur Datenvernichtung anbieten. Hierbei ist auch schwierig zu beurteilen, welche Unternehmen an der Service-Bereitstellung beteiligt waren und in welchen Ländern die Daten verarbeitet wurden. Beides ist in Public-Clouds nicht offensichtlich und erschwert die Bewertung dieser Aspekte im Rahmen des Risikomanagements.

3.2.3 Eingeschränkte Möglichkeiten des Schadenrisikomanagements

Im Schadenfall können IT-Infrastrukturen auf Hinweise zur Schadenursache untersucht werden. Diese sog. forensischen Maßnahmen dienen zur Aufklärung eines digitalen Schadenereignisses und zur Bestimmung des tatsächlichen Schadenausmaßes, u.a. um die Schadenfolgekosten (wie bspw. Kundenbenachrichtigungen) zu reduzieren. Die Durchführung einer forensischen Maßnahme ist im Interesse des Versicherungsnehmers, obliegt jedoch den Cloud-Providern als Inhaber der Rechenzentren. Diese werden aufgrund der haftungsrechtlichen Relevanz, fehlender Standards sowie fehlender rechtlicher Verpflichtung von den Anbietern oftmals nicht durchgeführt. Außerdem stellen dabei die Speicherstrukturen[27] der Cloud-Infrastrukturen ein spezifisches Problem dar. Bei einer forensischen Untersuchung könnten auch Daten nichtbetroffener Unternehmen, die sich auf demselben Datenträger befinden, offengelegt werden.[28] Ist die Möglichkeit forensischer Maßnahmen eingeschränkt, kann dies Auswirkungen auf den Leistungsumfang entsprechender Versicherungsprodukte haben bzw. die Versicherungsprämie erhöhen.

3.2.4 Cloud-Computing und Supply-Chain-Risiken

Im Cloud-Computing greifen Anbieter von Softwarelösungen auf die Infrastruktur von Drittunternehmen zurück. Hierdurch entstehen *Providerketten*, in denen mehrere Leistungserbringer an der Bereitstellung eines Cloud-Dienstes beteiligt sind. Wie in klassischen Lieferketten kann die verzögerte oder ausbleibende Produktionsleistung bzw. Datenbereitstellung ein finanzielles unternehmerisches Risiko bei den beteiligten Akteuren darstellen.[29] Ursachen wie technische Defekte, Programmierfehler, Hackerangriffe, aber auch Unternehmensinsolvenzen und -

[27] Ein wesentliches Merkmal von Cloud-Computing sind multi-tenant Strukturen. Dies bedeutet, dass die Daten verschiedener Kunden auf einer physischen Festplatte direkt nebeneinander abgelegt und mithilfe von Softwaremechanismen voneinander getrennt werden.
[28] Vgl. *Hansen* (2012), S. 409.
[29] Vgl. *Jüttner et al.* (2003), S. 130; vgl. *Tang* (2006), S. 452.

übernahmen, Naturkatastrophen oder Terrorakte an einer Stelle der Providerkette können zur temporären oder dauerhaften Beeinträchtigung der Dienstverfügbarkeit bei nachfolgenden Wertschöpfungsstufen führen.

Insbesondere die Betriebsunterbrechung infolge eines fehlerhaften oder nicht-verfügbaren Dienstes birgt ein hohes Schadenpotential aus entgangenem Gewinn oder ungedeckten fortlaufenden Betriebskosten. Heutige Cyberrisk-Policen ersetzen Schäden der Betriebsunterbrechung oftmals nur im Rahmen einer Sachversicherung (z.B. Elektronikversicherung) und schließen somit Cloud-Dienste implizit als Schadenursache aus. Die Haftung der Anbieter ist, wie in Abschnitt 3.2.1 dargestellt, in Public-Clouds nicht risikogerecht.

3.2.5 Oligopole Cloud-Strukturen erhöhen das Schadenpotenzial

Das Angebot von großen und bedeutenden Cloud-Infrastrukturen ist auf wenige Anbieter, wie bspw. Amazon, Microsoft oder Google begrenzt. Cloud-Anwendungen und Unternehmen nutzen diese Infrastrukturen, da diese trotz günstiger Nutzungs- und Transaktionskosten technologisch führend sind. Solche große Infrastrukturprovider bieten jedoch eine attraktive Angriffsfläche für schädigende Maßnahmen, da sich dort aufgrund des hohen Marktanteils sensible Unternehmensdaten konzentrieren können. Mit der zunehmenden Nutzung von Cloud-Dienstleistungen durch Unternehmen steigt folglich die allgemeine Risikoexposition der Anbieter und Nachfrager. Dies führt zugleich zu einem steigenden Gesamtschadenpotenzial bei jedem Cloud-Provider.

3.2.6 Doppelte Schadenkosten in Cloud-Wertschöpfungsstrukturen

Die Abhängigkeitsstrukturen in der Cloud-Computing-Wertschöpfung führen zu einer sich duplizierenden Schadendimension bei den einzelnen Cloud-Akteuren. Die Trennung von IT-Infrastruktur, Entwicklungsumgebung und Softwareangebot sowie die Kombinations- und Kooperationsmöglichkeiten zwischen den Anbietern können im Schadenfall bei allen beteiligten Akteuren Eigen- und Drittschäden auslösen. Diese Risikoperspektive ist primär für Erstversicherungsunternehmen von Interesse die mehrere Akteure eines Cloud-Wertschöpfungsnetzwerkes gleichzeitig versichern, sowie für den Rückversicherungsmarkt.

Betrachtet man zusammenfassend die Risikosituation von Cloud-Computing-Dienstleistungen so wird deutlich, dass insbesondere die im Vergleich zum klassischen IT-Outsourcing weniger präzisen vertraglichen Regelungen, cloudspezifische Eigenschaften wie geteilte IT-Ressourcen, die hohe organisatorische Abhängigkeit aufgrund der extern genutzten IT-Ressourcen, rechtliche Aspekte und die Intransparenz eines Cloud-

Wertschöpfungsnetzwerkes eine Herausforderung für das Risikomanagement von Unternehmen darstellen. Zudem fehlen häufig Informationen zur Bewertung der Risikosituation von (Public)-Cloud-Angeboten.[30] Die interdependenten Risikostrukturen von Public-Cloud-Diensten mit der Konzentration einer Vielzahl an Einzelrisiken bei wenigen großen Anbietern, die sich duplizierenden Schadenkosten und die Neuartigkeit von Cloud-Risiken verändern sowohl das Schadenshöhenpotenzial als auch das mögliche Gesamtschadenausmaß. Diese Aspekte bedingen eine Betrachtung der Versicherbarkeit von Cloud-Computing-Risiken.[31]

3.3 Versicherungstechnische Aspekte und Management von Risiken aus Cloud-Computing Dienstleistungen

Die Absicherung möglicher Schäden aus der Nutzung von Cloud-Computing-Dienstleistungen kann durch ein Versicherungsunternehmen erfolgen, wenn entsprechende Versicherungslösungen umsetzbar sind und angeboten werden. Um den Risikotransfer auf ein Versicherungsunternehmen gegen eine Risikoprämie zu gewährleisten, wird untersucht, ob die Risiken aus der Nutzung von Cloud-Computing-Dienstleistungen einer Versicherbarkeitsprüfung standhalten und somit im engeren Sinne versicherbar sind. In der Versicherungswirtschaft gelten Risiken als versicherbar, wenn eine Einschätzung hinsichtlich der Eintrittswahrscheinlichkeit und der Schadenhöhe möglich ist. Außerdem muss die Schadenursache definierbar und die Schadenwirkung eingrenzbar sein. Eine Prüfung der Versicherbarkeit bezieht sich nach Karten (1972) auf den Grad der Erfüllbarkeit elementarer Kriterien wie Zufälligkeit, Eindeutigkeit, Schätzbarkeit, Unabhängigkeit und Größe.[32] Neben diesen versicherungsmathematischen Kriterien müssen aber auch marktbedingte Aspekte wie die Zahlungsbereitschaft für Versicherungsprämien, die Grenzen der Risikodeckung und ggfs. die Kapazität der Versicherungsbranche berücksichtigt werden.[33] Auch wenn für Cyber-Risiken bereits grundsätzlich (unvollständige) Versicherungsansätze existieren, sind die in Kapitel 3.2 gezeigten Veränderungen durch Cloud-Computing eine zusätzliche Herausforderung für die Versicherungsbranche.[34] Dabei ist nicht direkt offensichtlich, ob die genannten Kriterien zur Versicherbarkeit auch bei Cloud-Computing erfüllt sind. Diese werden daher im Folgenden genauer analysiert.

[30] Vgl. *CSA* (2011), S.33-34.
[31] Vgl. *Mather et al.* (2009), S. 39-41.
[32] Vgl. *Benzin* (2005), S. 211-212; *vgl. Karten* (1972), S. 287.
[33] Vgl. *Berliner* (1982).
[34] Vgl. *Brand/Schauer* (2007), S. 324.

Das Kriterium der *Zufälligkeit* verlangt, dass ein zu versicherndes Ereignis (bspw. Datendiebstahl oder Ausfall einer Cloud-Infrastruktur) von den Versicherungsparteien zum Zeitpunkt der Vertragsunterzeichnung nicht vorhersehbar und nicht beeinflussbar sein darf.[35] Im Cloud-Computing hängt die Beurteilung dieses Kriteriums von der Risikoperspektive ab. Während der Cloud-Nutzer keinen Einfluss auf die individuelle Schadenneigung eines Cloud-Dienstes hat, so können Cloud-Provider direkten Einfluss auf die gewählten Sicherheitsmaßnahmen und Kooperationspartner nehmen. Die Zufälligkeit wird zudem direkt durch die Popularität eines Cloud-Dienstes beeinflusst: Werden besonders sensible oder unternehmenskritische Daten verarbeitet, sind diese Anbieter einem erhöhten Risiko schädlicher Attacken ausgesetzt, da ein größeres „Erfolgspotential" in Form der Werthaltigkeit relevanter Kundendaten besteht.

Ein wichtiger Aspekt im Zusammenhang mit der Auslagerung von unternehmensrelevanten Prozessen und Daten ist das *moralische Risiko*.[36] Jeder Risikotransfer ist mit einer Verzerrung der Anreize zur Schadenminderung verbunden. Dabei sinkt der Anreiz mit der zunehmenden Zession des Gesamtrisikos. Im Cloud-Computing kann der Datentransfer mit einem Transfer des datenbezogenen Risikos vom Kunden hin zum Cloud-Anbieter gleichgesetzt werden. Da die derzeitigen Nutzungsbedingungen die Haftung eines Public-Cloud-Providers für Datensicherheit und Verfügbarkeit jedoch weitestgehend ausschließen, existieren hierbei vorgenannte Moral Harzard Probleme nicht.[37] Erst mit dem Angebot spezieller Versicherungslösungen werden für den Kunden Anreize geschaffen, bei der Wahl des Cloud-Modells weniger auf das Sicherheitsniveau als wesentliches Selektionskriterium zu achten. Teurere Private-Cloud-Lösungen mit einem höheren realisierten Sicherheitsniveau wären bei dieser Konstellation aus Kostengründen benachteiligt, der Kunde könnte einen Public-Cloud-Dienst vorziehen. Dieses Argument wird dadurch gestützt, dass selbst die Schadenfälle der Public-Cloud-Dienste in den letzten Jahren nicht dazu geführt haben, dass betroffene Unternehmen wie bspw. Netflix auf eine Private-Cloud wechseln. Allerdings können geeignete Selbstbehalte in den Versicherungspolicen einem zu sorglosem Handeln entgegenwirken.

Das Angebot von speziellen Versicherungsprodukten zur Absicherung der Schäden auf Kundenseite bei der Nutzung von Cloud-Diensten kann zudem auch mit einem erheblichen ex ante moralischen Risiko beim Cloud-Anbieter verbunden sein. Dies ist vor allem dann der Fall, wenn die Kosten für Sicherheitsmaßnahmen stark ansteigen und somit die Präventionsanstren-

[35] Vgl. *Karten* (1972), S. 287-288.
[36] Vgl. *Eisen/Nell* (1994), S. 221.
[37] Im Schadenfall werden bei Public-Cloud-Diensten i.d.R. nur die monatlichen Nutzungsgebühren erstattet.

gungen der Anbieter tendenziell sinken. Versicherungsprodukte können zwar an den Nachweis von entsprechenden Sicherheitszertifikaten sowie die Einhaltung von relevanten Standards gekoppelt sein, aber gerade darüber hinausgehende Maßnahmen erscheinen wichtig, um ein hohes Sicherheitsniveau für den Kunden zu gewährleisten. Diese zusätzlichen Schadenverhütungsmaßnahmen könnten dann bspw. aus Kostengründen unterlassen werden.

Das Kriterium der Zufälligkeit kann weiterhin aufgrund der Konzentration der Einzelrisiken bei wenigen großen und stark exponierten Cloud-Service-Providern beeinträchtigt sein.[38] Eine solche „räumliche" Begrenzung der Exponierung führt zu einer Beschränkung der Risikogemeinschaft, die vergleichbar mit der Situation von Naturkatastrophen ist, bei denen i.d.R. nur regional beschränkte Gebiete betroffen sind. Dies würde zwar die Versicherbarkeit hinsichtlich des Kriteriums Zufälligkeit nicht ausschließen, es kann jedoch aufgrund der Ansammlung von schlechten Risiken zu Kumul- und Selektionseffekten kommen. Diese kommen dann zustande, wenn sich Kunden wiederum versicherungsinduziert mit der Wahl einer Public-Cloud-Form bewusst einem höheren Nutzungsrisiko gegenüber einer Private-Cloud-Form aussetzen. Eine Folge des eingeschränkten Risikoausgleichs im Kollektiv sind Kumulprobleme und als Konsequenz vergleichsweise hohe Versicherungsprämien. Ähnlich wie bei Elementarrisiken könnte an dieser Stelle der Lösungsansatz einer Pflichtversicherung für Public-Cloud-Kunden diskutiert werden.[39]

Eine weitere Überlegung bezüglich der Versicherbarkeit von Cloud-Risiken bezieht sich auf die gezielte und böswillige Angriffsabsicht auf eine Cloud-Computing-Infrastruktur, bspw. durch einen Hackerangriff oder die physische Zerstörung des Datenzentrums – ggfs. mit einem terroristischen Hintergrund. In diesen Fällen ist das Kriterium der Zufälligkeit ebenfalls nicht uneingeschränkt gegeben. Zwar sind böswillige Angriffe aus Sicht der Versicherungsnehmer nicht vorhersehbar, aber Anbieter können durchaus wie gezeigt Einfluss auf die Zufälligkeit nehmen. Versicherungsprodukte müssen zwischen Public- und Private-Cloud-Angeboten aufgrund unterschiedlicher grundsätzlicher Sicherheitsniveaus differenzieren und die Prämie an diesem Kriterium und anderen Sicherheitsnachweisen ausrichten.

Das Kriterium der *Eindeutigkeit* erfordert, dass der Versicherungsfall, der versicherte Schaden und die zugehörige Versicherungsleistung im Versicherungsvertrag eindeutig und intersubjektiv überprüfbar deklariert sind.[40] Bei Cyber-Risiken kann es, aufgrund der vielfälti-

[38] Siehe Abschnitt 3.2.5.
[39] Vgl. *Albrecht et al.* (2004), S. 428-429.
[40] Vgl. *Karten* (1972), S. 289.

gen Schadenursachen und des hohen Änderungsrisikos auf der Schadenseite, zu Spezifikationslücken in den Versicherungsverträgen kommen. Die Erfüllung dieses Kriteriums ist folglich auch beim Cloud-Computing nicht immer gegeben. Die Aufklärung und Analyse der Schadenursache ist, wie in Abschnitt 3.2.2 dargelegt, besonders in Public-Cloud-Netzwerken bei mangelnder Kooperation der Cloud-Provider schwierig oder nicht möglich. Private-Cloud-Provider bieten dagegen meist bessere Standards und ein höheres Interesse an der Aufklärung.[41] Eine ausreichende Informationsbasis zur Schadenursache ist zudem notwendig, um Cyberpolicen für Cloud-Computing-Dienstleistungen von anderen vorhandenen Versicherungsprodukten abzugrenzen – beispielsweise im Falle von Betriebsunterbrechungen. Das Kriterium Eindeutigkeit kann aber mittels einer entsprechenden Ausgestaltung des Versicherungsvertrages auch im Cloud-Computing erfüllt sein.

Gemäß dem Kriterium der *Schätzbarkeit* muss das zu versichernde Risiko bzw. die Wahrscheinlichkeitsverteilung eines Risikos und die voraussichtliche Schadenhöhe bekannt bzw. zumindest hinreichend genau schätzbar sein, um den Schadenerwartungswert für den Versicherer kalkulierbar zu machen.[42] Die Erfüllung der Schätzbarkeit stellt bei Cloud-Computing-Risikokollektiven hohe Anforderungen an einen Versicherer. Ein Grund dafür ist, dass Kundenstamm und Datenbestand insbesondere bei Public-Cloud-Infrastrukturen einem hohen Änderungsprozess unterliegen. Die niedrigen Eintrittsbarrieren bei Public-Cloud-Diensten implizieren stetige Schwankungen des Kundenbestands und damit auch Informationsasymmetrien hinsichtlich der wirtschaftlichen Relevanz des Datenbestands. Darüber hinaus können sich die Lieferkettenbeziehungen zu vorgelagerten Cloud-Providern ändern. Eine möglichst genaue Schätzung erscheint zudem problematisch, da kaum verlässliche Vergleichs- bzw. Erfahrungswerte für Cloud-Infrastrukturen vorliegen. Der Wert ausgelagerter Daten und Geschäftsprozesse erreicht mit zunehmender Akzeptanz von Cloud-Computing-Dienstleistungen eine neue wirtschaftliche Dimension.

Versicherungslösungen für neue Risiken werden trotz eines Informationsmangels unter Zugrundlegung von subjektiven Einschätzungen entwickelt – auch wenn keine hinreichend statistisch gesicherte Risikoprognose besteht. Um einer bestehenden Informationsasymmetrie entgegenzuwirken, können Versicherer ihre Einschätzung im Bezug auf die Fehleranfälligkeit einer Cloud-Infrastruktur oder -Dienstleistung mithilfe von geeigneten Zertifizierungen und der Überprüfung gängiger Standards unterstützen sowie auf Ausfalldaten klassischer Datenzentren

[41] Vgl. *Rowe* (2008), S. 6.
[42] Vgl. *Karten* (1972), S. 290.

zurückgreifen. Aus versicherungstechnischer Perspektive ist zudem ein ausreichend hoher Sicherheitszuschlag auf die Versicherungsprämie zu erheben – eine Limitierung der Haftungsobergrenzen kann dem Schätzbarkeitsproblem entgegenwirken. Somit ist die eingeschränkte Schätzbarkeit keine grundsätzliche Einschränkung für die Versicherbarkeit von Cloud-Computing-Dienstleistungen, zumindest solange die Unabhängigkeit zwischen den Einzelrisiken gewährleistet ist.

Die einzelnen Risiken innerhalb eines versicherten Kollektivs sollen nach Möglichkeit stochastisch unabhängig voneinander sein.[43] Das Kriterium der *Unabhängigkeit* ist bei Cloud-Computing-Kollektiven problematisch, denn aufgrund der interdependenten Netzwerkstruktur ist das Ansteckungsrisiko nicht nur innerhalb einer, sondern auch zwischen Cloud-Architekturen gegeben. Eine Dienstunterbrechung oder ein gezielter schädlicher Angriff kann beim Cloud-Computing eine große Anzahl von Einzelrisiken gleichzeitig treffen. Aufgrund der Lieferkettenstrukturen kann der Ausfall einer Cloud-Infrastruktur auch andere Cloud-Provider und deren Kunden betreffen.[44] Relevant ist in diesem Zusammenhang die Größe des betrachteten Netzwerkes: Ist ein Angebot für Unternehmen oder Privatkunden von Interesse und wird zunehmend genutzt, dann wird das Cloud-Netzwerk ebenfalls wachsen. Der Netzwerkeffekt ist somit indirekt gegeben und entscheidend für die Kalkulierbarkeit des zu versichernden Schadenereignisses. Ansteckungsrisiken bzw. interdependente Risikostrukturen sind somit ein Problem für die Versicherbarkeit.

Aufgrund des Zusammenschlusses zahlreicher Einzelrisiken in einer interdependenten Netzwerkstruktur entsteht ein *Externalitätenproblem*: die Anzahl der Kunden mit hohem Vermögensschadenpotenzial kann die Wahrscheinlichkeit eines (Hacker-)Angriffs auf die Cloud-Infrastruktur beeinflussen. Im Fall von Cloud-Dienstleistungen sind nun aber nicht die Nutzer die aktive Partei im Schadenverhütungsmanagement, sondern die Cloud-Provider.

Im Zusammenhang mit der interdependenten Netzwerkstruktur wirken Schadenverhütungsmaßnahmen der Anbieter aber nicht immer in der gewünschten Weise. So können Sicherheitsmaßnahmen bzw. Investitionen in die Sicherheit eines Cloud-Computing-Dienstes *Substitutionseffekte* hervorrufen. Solche Substitutionseffekte sind als kritische Herausforderung im Management von Risiken aus interdependenten Netzwerken zu sehen.[45] Dies gilt auch insbesondere für Risiken aus Cloud-Computing-Diensten. Der Grund liegt in der Krux dieser Effek-

[43] Vgl. *Karten* (1972), S. 292.
[44] Vgl. Abschnitt 3.2.3.
[45] Vgl. *Enders/Sandler* (2002).

te: verstärkt beispielsweise ein Cloud-Provider die Sicherheit an einer Stelle des Netzwerks und macht damit einen Hackerangriff an dieser Stelle schwieriger bzw. aufwendiger, so hat dies zu Folge, dass die Hacker sich tendenziell eine andere Schwachstelle suchen, die weniger aufwendig angreifbar ist. Es wäre somit aus Sicht der Unabhängigkeit empfehlenswert, weitgehend gleichmäßig verteilte Sicherheitsstrategien über die identifizierten möglichen Angriffspunkte zu entwickeln. Neben Ansteckungsrisiken besteht im Zusammenhang mit der Unabhängigkeit insbesondere das Problem der *Kumulrisiken*.[46] Betrifft ein Schadenereignis viele Versicherte gleichzeitig, kann ein solcher Kumulschaden die Zahlungsfähigkeit des Versicherers im Extremfall gefährden. Die Abhängigkeit zahlreicher Nachfrager von einem Provider ist insbesondere bei Public-Cloud-Services gegeben.

Das Kriterium der *Größe* bezieht sich auf den möglichen Maximalschaden.[47] Das Kriterium kann ebenfalls als problematisch angesehen werden, da die Größe des Einzelrisikos schwierig zu bewerten ist. Public-Cloud-Infrastrukturen werden dem Kunden auf Abruf automatisiert zur Verfügung gestellt. Somit befindet sich eine theoretisch „unbegrenzte“ und vorher nicht definierbare Anzahl von Unternehmen in der Cloud-Infrastruktur eines Providers. Dies und fehlende Quantifizierungsvorschriften bei IT-Risiken erschweren die Einschätzung der maximalen Aggregation des Risikopotentials. Insbesondere im Fall von Unternehmenskunden ist das Risiko nicht auf den Datenverlust oder die temporär fehlende Verfügbarkeit der Cloud-Dienste allein begrenzt, sondern beinhaltet zudem mögliche Folgeschäden. Je sensibler die in der Cloud gespeicherten Informationen, desto höher ist ein möglicher Reputationsschaden. Aktuelle Cyberversicherungslösungen lösen diese Probleme jedoch mit entsprechenden Haftungsbegrenzungen.

Zusammenfassend kann festgehalten werden, dass Risiken aus Cloud-Computing-Dienstleistungen zumindest theoretisch als grundsätzlich versicherbar angesehen werden können. Hervorzuheben sind hier die besonderen Risikointerdependenzen und die Kumulproblematik. Dies lässt darauf schließen, dass das Kriterium der Unabhängigkeit als besonders problematisch bezüglich der Versicherbarkeit zu werten ist. Weiterhin ist das Kriterium der Größe kritisch zu betrachten. Letztlich besteht ein Problem in der Festlegung und Feststellung der Schäden und deren Verursacher. Dies erscheint allerdings weniger als ein Problem der versicherungstechnischen Machbarkeit als einer vertragsrechtlichen Umsetzung. Cyber-Policen müssen Haftungslimits an den Cloud-Anbietern sowie den genutzten Cloud-Diensten ausrichten und

[46] Vgl. *Gründer/Schrey* (2007), S. 332.
[47] Vgl. *Karten* (1972), S. 292.

danach auch die Versicherungsprämie differenzieren. Heutige Cyber-Policen sind für Cloud-Computing-Dienstleistungen noch nicht ausreichend konzipiert.

Während die Veränderung der Risikosituation durch Cloud-Computing primär die Vertragsgestaltung des Erstversicherers betrifft, ist die aufgezeigte Kumulproblematik und die mangelnde Unabhängigkeit von großer Bedeutung für den Rückversicherungsmarkt.

3.3.2 Risikoperspektive und Versicherungsnachfrage im Cloud-Computing

Die Risikoperspektive ist ein wesentlicher Aspekt bei der Einschätzung der Cloud-Einzelrisiken und wird auch bei der Frage nach einem *geeigneten Ansprechpartner für mögliche Versicherungslösungen* relevant. Die Haftungs- und Risikosituation im Cloud-Computing resultiert aus den jeweils erbrachten bzw. in Anspruch genommenen Cloud-Dienstleistungen. So determinieren Cloud-Schadenursachen bei den Risikoträgern divergente Schadenwirkungen und -höhen. Jeder Akteur im Cloud-Computing hat folglich eine eigene Risikoperspektive, so dass Risiken aus Sicht von *Cloud-Geschäfts- oder -Endkunden* (Eigenschaden-Perspektive), *Cloud-Providern* (Eigen- und Fremdschaden-Perspektive), *Netzanbietern* (Eigen- und Fremdschaden-Perspektive), sowie aus Sicht von *Versicherungsunternehmen* (doppelte Schadenlast[48]) berücksichtigt werden müssen. Daraus stellt sich die Frage, welcher Cloud-Akteur Versicherungsprodukte nachfragen sollte und welche ökonomischen Anreize dazu bestehen. Aus Versicherungsperspektive können die Cloud-Anbieter geeignete Versicherungsnehmer darstellen, da diese implizit das Risiko der Datenhaltung und Dienstbereitstellung übernehmen und im Schadenfall u.a. Ansprüchen aufgrund Vermögensschäden bei Dritten ausgesetzt sind. Zudem wäre ein spezielles Cloud-Versicherungsprodukt für die Anbieter ein interessantes Differenzierungsmerkmal, um die eigene Cloud-Dienstleistung von anderen Marktangeboten abzugrenzen. Der Versicherer hat hier die Möglichkeit einer individuelle Risikoprüfung seiner Vertragspartner und kann Haftungslimits und Selbstbehalte im Einzelfall definieren. Alternativ können auch Cloud-Kunden individuell Versicherungsprodukte nachfragen und diese bspw. gegen Aufpreis bei Nutzung eines Cloud-Services erwerben. Die Prämienhöhe hängt hierbei vom genutzten Cloud-Modell ab. Der Abschluss von entsprechenden Versicherungslösungen kann auch die Nutzung ausgewählter (und somit vom Versicherungsunternehmen überprüfbarer) Cloud-Provider bedingen. Die Anpassung von Cyberversicherungspolicen oder das Angebot spezieller Cloud-Versicherungen ist notwendig, da bspw. Schäden durch eine Betriebsunterbre-

[48] Versicherungsunternehmen müssten bei Angebot von Cloud-Versicherungen – im Rahmen der vereinbarten Deckung und abgeschlossenen Policen – ggfs. für die Schäden mehrerer beteiligter Akteure aufkommen.

chung aufgrund des Ausfalls eines genutzten Cloud-Services von den heutigen Cyberversicherungspolicen in Deutschland weitestgehend ausgeschlossen sind. Im Januar 2012 hat die EU-Kommission eine Datenschutzreform vorgeschlagen, die u.a. deutlich höhere Bußgelder bei Verstößen gegen Datenschutzvorschriften vorsieht. Mit dieser geplanten Verschärfung des Datenschutzrechts in Europa dürfte sich außerdem zukünftig die Nachfrage nach speziellen Cloud- bzw. Cyberversicherungsprodukten signifikant erhöhen und Unternehmen für die Risikosituation im Cloud-Computing stärker sensibilisieren.[49]

3.4 Alternative Möglichkeiten der Absicherung von Risiken aus Cloud-Computing-Dienstleistungen

Neben Versicherungslösungen sind alternative Möglichkeiten der Absicherung von Risiken aus Cloud-Computing-Dienstleistungen denkbar. Risiken aus Cloud-Computing können zunächst durch technische Schadenverhütungsmaßnahmen der beteiligten Parteien begrenzt werden. Ex ante eignen sich Verschlüsselungsverfahren zur Erhöhung der Datensicherheit beim Transfer von sensiblen Kundendaten. Diese können in Kombination mit Firewall- und weiteren Sicherheitssystemen auch das Schnittstellenrisiko senken.[50] Die unterschiedlichen Sicherheitsmaßnahmen stellen ein wesentliches Unterscheidungskriterium zwischen den Cloud-Providern dar. Wird ein hohes Sicherheitsniveau angestrebt, sollte der Nachfrager in eine Private-Cloud wechseln, um einige der oben gelisteten Risiken zumindest zu reduzieren. Das höhere Sicherheitsniveau spiegelt sich allerdings in höheren Nutzungs- und Transaktionskosten der Private-Cloud ggü. einer Public-Cloud wider.

Eine mögliche, allerdings aufwendige, Strategie der Absicherung von Risiken aus Cloud-Computing-Dienstleistungen stellt die Diversifikation über mehrere Cloud-Provider ggf. unter Zuhilfenahme eines aggregierenden Brokers dar. Cloud-Computing-Infrastrukturen weisen bei einem Anbieter bereits charakteristische Redundanzen bei der Datenhaltung auf. Allerdings zeigen die jüngsten Schadenfälle von Public-Cloud-Infrastrukturen, dass allein hierdurch Dienstausfall und Datenverlust nicht vermieden werden konnten. Analog zur Portfoliotheorie aus dem Finanzbereich ließe sich eine Risikoreduktion mittels Diversifikation über mehrere Cloud-Provider erreichen. Aus praktischer Sicht sprechen allerdings einige Gründe derzeit noch gegen diesen Risikomanagementansatz: Proprietäre Cloud-Anwendungen, das Fehlen einheitlicher Standards und die daraus resultierende fehlende Interoperabilität und Portabilität zwischen

[49] Hierzu siehe die aktuelle Diskussion zur Weiterentwicklung der EU Richtlinie 95/46/EG.
[50] Vgl. *Lesch* (2002), S. 189.

den Cloud-Angeboten führt zu einer langfristigen Bindung an einen Cloud-Provider. Hierdurch reduzieren sich die Möglichkeiten zur Diversifikation über mehrere Cloud-Provider hinweg. Alternative Diversifikationsmöglichkeiten, wie bspw. eine zusätzliche selbstverantwortliche Datensicherung, sind im Cloud-Computing nicht grundsätzlich möglich. Die zusätzlichen Kosten für diese ex ante Strategien würden zudem die Frage nach der ökonomischen Sinnhaftigkeit einer Cloud-Lösung aufwerfen. Als eine ex post Risikostrategie kann das Nutzungsrisiko auch über interne Finanzierungsinstrumente selbst getragen werden. So ist ein alternativer Risikotransfer am Kapitalmarkt über Derivate oder Insurance-Linked-Securities an die Kapitalmärkte denkbar, wobei allerdings die objektiv kalkulierbare Risikobestimmung problematisch sein kann. Eine weitere Möglichkeit ist die bedingte Finanzierung: Für den Fall des Eintritts eines existenzbedrohenden Schadenfalls sichert sich das Unternehmen bedingtes Risikokapital und kann hierdurch das Risiko im Vergleich zur Versicherungslösung ggf. kostengünstiger tragen.[51] Im Kontext der Risikobewertung ist Cloud-Computing aber auch eine Chance, um bekannte Cyber-Risiken zu minimieren. Die technologischen Strukturen cloudbasierter Infrastrukturen bieten mit der redundanten Datenspeicherung von weltweit verteilten Datenzentren Vorteile, die bspw. das Risiko einer Betriebsunterbrechung minimieren können. Auch übertreffen die Sicherheitsmaßnahmen der hochspezialisierten Cloud-Provider, die technischen und finanziellen Möglichkeiten der meisten kleinen und mittelständischen Unternehmen und stellen somit eine sicherere Lösung der IT-Versorgung dar.[52] Sollten sich im Cloud-Computing zudem stärkere Standards durchsetzen, dann könnten einige der derzeitigen Probleme abgeschwächt werden. Außerdem wäre dann die Aggregation diverser Cloud-Infrastrukturen unterschiedlicher Cloud-Provider mithilfe von Cloud-Brokern eine geeignete Möglichkeit der Risikodiversifizierung innerhalb von Cloud-Computing-Lieferketten.

4 Schlussbemerkung

Dieser Artikel befasst sich mit zentralen Fragen des Managements von Risiken aus Cloud-Computing-Dienstleistungen. Die neuartige Risikosituation bei dieser Form des IT-Outsourcings stellt für die Versicherungswirtschaft zwar eine Herausforderung, aber auch eine erhebliche Geschäftschance dar. Insbesondere sollten bestehende Cyberversicherungsprodukte an die wachsenden Bedürfnisse der Kunden angepasst und Deckungslücken in Bezug auf Cloud-Computing-Dienstleistungen geschlossen werden. Ein Verständnis für die Risikosituati-

[51] Vgl. *Doherty* (2000), S. 460-464.
[52] Vgl. *Schlayer* (2011), S. 118; vgl. *Jansen/Grance* (2011), S. 9f.

on ist die Voraussetzung für den richtigen Umgang mit Cloud-Computing im Unternehmenseinsatz. Sicherheitsrisiken des Cloud-Computing müssen identifiziert und quantifiziert werden. Der Umgang mit potentiellen Risiken bspw. über Maßnahmen zur Schadenminderung oder die Möglichkeiten zum Risikotransfer sollten in der strategischen Unternehmensplanung berücksichtigt werden. Wenn Cloud-Computing-Services im Rahmen eines Risikomanagements bewertet und Restrisiken an ein Versicherungsunternehmen transferiert werden können, werden Unternehmen vermehrt die Adaption von Cloud-Diensten in Erwägung ziehen.[53] Die Analyse schließt deshalb auch die Sichtweise der Versicherungsunternehmen mit ein, um das Potential heutiger Versicherungsprodukte und die Anforderungen an zukünftige Lösungen für Cloud-Computing-Risiken zu erfassen. Das entscheidende Problem bei der Versicherbarkeit von Risiken aus Cloud-Computing-Dienstleistungen ist die fehlende Unabhängigkeit der Einzelrisiken untereinander, sowie die Kumulproblematik aufgrund der interdependenten Netzwerkstruktur. Versicherungskonzepte müssen durch innovative Lösungen unterstützt werden, beispielsweise durch die Einbindung spezieller Cloud-Broker. Im Rahmen des Risikomanagements sollten sich Unternehmen dabei über die Risikosituation der genutzten Cloud-Services und die möglichen operationellen Risiken bewusst werden. Dies erfordert die monetäre Bewertung der gespeicherten bzw. verarbeiteten (Kunden-)Daten sowie ausgelagerter Geschäftsprozesse, um das Schadenausmaß bei Datenverlust oder bei Nicht-Verfügbarkeit der Cloud-Dienste einschätzen zu können.[54]

Literaturverzeichnis

Albrecht et al.: Risikoforschung und Versicherung: Festschrift für Elmar Helten. 1. Auflage, Verlag Versicherungswirtschaft Karlsruhe (2004)

Armburst et al.: A View of Cloud Computing. *Communication of the ACM.* Vol. 53, No. 4, 50-58 (2010)

Berliner, B.: Limits of Insurability of Risks, Englewood-Cliffs (1982)

Benzin, A.: Versicherungstechnische Bewertung unterschiedlicher Deckungskonzepte für Terrorismusrisiken, Karlsruher Reihe II, Risikoforschung und Versicherungsmanagement. 1. Auflage, Verlag Versicherungswirtschaft Karlsruhe (2005)

BITKOM: Cloud Computing – Was Entscheider müssen wissen (2010)

Böhm et al.: Cloud Computing: Outsourcing 2.0 oder ein neues GeschäftsmodelI zur Bereitstellung von IT-Ressourcen?, Informationsmanagement und Consulting, Band 24, Nr. 2, 6-14 (2009)

Böhme, R., Kataria, G.: Models and Measures for Correlation in Cyber-Insurance, *Workshop on the Economics of Information Security*. http://weis2006.econinfosec.org/docs/16.pdf (2006). Abgerufen am 10.2.2013

Bradshaw et al.: Contract for clouds: comparision and analysis of the Terms and Conditions of cloud computing services,

[53] Vgl. *ENISA* (2011), S. 19.
[54] Vgl. *Mell/Grance* (2011), S. 1-3.

International Journal of Law and Information Technology, Vol. 19, No. 3, 187-223 (2011)

Brand, C., Schauer, S.: IT-Risikomanagement durch Risikotransfer, in: Gründer T., Schrey, J. (Hrsg.): *Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht,* S. 309-336 (2007)

Cloud Security Alliance (CSA): Top Threats to Cloud Computing v1.0. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (2010). Abgerufen am 20.2.2013

Cloud Security Alliance (CSA): Security Guidance for Critical Areas in Cloud Computing v3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (2011). Abgerufen am 3.2.2013

Deloitte: Cloud Computing in Deutschland – Ergebnisse der Umfrage von Deloitte und Bitkom. http://www.deloitte.com/assets/Dcom-Germany/Local%20Assets/Documents/12_TMT/2011/Studie_CloudComputinginDeutschlandStudieFeb2011.pdf (2011). Abgerufen am 25.1.2013

Doherty, N.: Integrated Risk Management – Techniques and Strategies for Managing Corporate Risk. McGraw-Hill Verlag NewYork (2000).

Eisen, R., Nell, M.: Die Wirkung von Versicherungsschutz auf Drittmärkte: Das externe moralische Risiko. In: Hesberg et al. (Hrsg.) Risiko Versicherung Markt: Festschrift für Walter Karten. 1. Auflage, Verlag Versicherungswirtschaft Karlsruhe, S. 221-242 (1994)

Enders, W., Sandler, T.: What do we know about the substitution efffect in transnational terrorism?, Working Paper, The University of Texas at Dallas. http://www.utdallas.edu/ ~tms063000/website/substitution2ms.pdf (2002). Abgerufen am 5.2.2013

European Network and Information Security Agency (ENISA): Cloud Computing: Benefits, risks and recommendations for information security (2009)

Foster et al.: Cloud Computing and Grid Computing 360-Degree Compared, *Proceedings of the 2008 Grid Computing Enviroments Workshop* (2008)

Furht, B., Escalante, A.: Handbook of Cloud Computing. 1. Auflage, Springer New York (2010)

Garg et al.: Quantifying the financial impact of IT security breaches, *Information Management und Computer Security*, Vol. 11, No. 2, 74-83 (2003)

Gordon, L., Loeb, M.: The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, Vol. 5, No. 4, 438-457 (2002)

Gründer, T., Schrey, J.: Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht. 1.Auflage, Erich Schmidt Verlag Berlin (2007)

Han, L.: Market acceptance of cloud computing: An analysis of market structure, price models and service requirements, Bayreuther Arbeitspapiere zur Wirtschaftsinformatik, No. 42 (2009)

Hachmann, M.: Microsoft signs up 1 Million Office 365 home subscribers. http://www.pcworld.com/article/2040088/microsoft-signs-up-1-million-office-365-home-subscribers.html (2013), Abgerufen am 30.05.2013

Hansen, M.: Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter, *DuD – Datenschutz und Datensicherheit*, Vol. 36, No. 6, pp. 407-412 (2012)

Jansen, W., Grance T.: Guidelines on Security and Privacy in Public Cloud Computing, *NIST Special Publication 800-144* (2011)

Jüttner, U.: Supply chain risk management: Understanding the business requirements from a practioner perspective, *The International Journal of Logistics Management*, Vol. 16, No. 1, 120-141 (2005)

Kakade et al.: Economic Properties of Social Networks, In: Advances in Neural Information Processing 17, Saul, L. , Weiss, Y., und Bottou, L. (eds.). Cambridge, Mass.: MIT Press (2005)

Karten, W.: Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsunternehmens – betriebswirtschaftliche Aspekte, *Zeitschrift für die gesamte Versicherungswissenschaft*, 61. Jahrgang, 279-299 (1972)

Kearns, M.: Economics, Computer Science, und Policy, *Issues in Science und Technology*, Vol. 21, 37-47 (2005)

Koch, R.: Versicherbarkeit von IT-Risiken: in der Sach-, Vertrauensschaden- und Haftpflichtversicherung. 1. Auflage, Erich

Schmidt Verlag Berlin (2005)

Kotulic, A., Clark, G.: Why there aren't more information security research studies. *Information und Management,* 41, 597-607 (2004)

KPMG: Cloud-Monitor 2012: Cloud-Computing in Deutschland – Status quo und Perspektiven. http://www.kpmg.de/docs/cloud-monitor-20120529.pdf (2012). Abgerufen am 5.2.2013

Kumar et al.: Optimally securing interconnected information systems and assets. *Proceedings of the Sixth Workshop on the Economics of Information Security,* Carnegie Mellon University, June 7-8, 2007 (2007)

Leimeister et al.: The business perspective of cloud computing. *Proceedings of the 18th European Conference on Information Systems, ECIS2010*. June 7-9 (2010)

Lesch, T.: Risk-Management von Risiken aus Nutzung des Internets – Eine ökonomische Analyse unter besonderer Berücksichtigung versicherungstechnischer Aspekte*,* Verlag Versicherungswirtschaft, Karlsruhe (2002)

Lipsky, S.: Cloud Computing: Eine Abgrenzung zum IT-Outsoucring und Systematisierung möglicher Sourcingoptionen, *Arbeitspapiere d. Instituts für Genossenschaftswesen der Westfälischen Wilhelms-Universität Münster,* No. 119 (2011)

Mather et al.: Cloud Security and Privacy – An Enterprise Perspective on Risks and Compliance, Sebastopol (2009)

Marston et al.: Cloud Computing – The business perspective. *Decision Support Systems*, Vol. 51, 176-189 (2011)

Mell, P., Grance, T.: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, Gaithersburg (2011)

o.A.: Twenty-One Experts Define Cloud Computing, SYS-CON Media Inc. http://cloudcomputing.sys-con.com/node/612375/print (2008). Abgerufen am 15.2.2013

Rhoton, J.: Cloud Computing Explained, 2. Auflage (2011)

Rowe, B.R.: Will Outsourcing IT Security Lead to a Higher Social Level of Security? (2008)

Schlayer, A.: Management und Versicherung von Risiken in der Informationstechnologie. In: Picot, A., Hertz, U., Götz, T. (Hrsg.) Trust in IT – Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an, S. 113 – 124 (2011)

Sydow, J.: Strategische Netzwerke: Evolution und Organisation, Wiesbaden (1992)

Symantec: State of Cloud Survey: Global Findings. http://www.symantec.com/content/en/us/about/ media/pdfs/symc-state-of-cloud-report-global.pdf?om_ext_cid=biz_socmed_twitter_facebook_ marketwire_linkedin_2011Sep_worldwide_stateofcloudsurvey (2011). Abgerufen am 17.2.2013

Tang: Perspectives in supply chain risk management, *Internal Journal of Production Economic*, vol. 103, issue 2, pp. 451-488 (2006)

Vaquero et al.: A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, Vol. 39, No. 1, 50-55 (2009)

Wouter, B., Lambrette, U.: The Cloud Value Chain Exposed – Key Takesaways for Network Serivce Providers, *Cisco White Paper* (2012)

Youseff et al.: Toward a Unified Ontology of Cloud Computing, *Proceedings of the 2008 Grid Computing Environment Workshop* (2008)

FZID Discussion Papers

Competence Centers:

IK:	Innovation and Knowledge
ICT:	Information Systems and Communication Systems
CRFM:	Corporate Finance and Risk Management
HCM:	Health Care Management
CM:	Communication Management
MM:	Marketing Management
ECO:	Economics

Download FZID Discussion Papers from our homepage: https://fzid.uni-hohenheim.de/71978.html

Nr.	Autor	Titel	CC
01-2009	Julian P. Christ	NEW ECONOMIC GEOGRAPHY RELOADED: Localized Knowledge Spillovers and the Geography of Innovation	IK
02-2009	André P. Slowak	MARKET FIELD STRUCTURE & DYNAMICS IN INDUSTRIAL AUTOMATION	IK
03-2009	Pier Paolo Saviotti and Andreas Pyka	GENERALIZED BARRIERS TO ENTRY AND ECONOMIC DEVELOPMENT	IK
04-2009	Uwe Focht, Andreas Richter, and Jörg Schiller	INTERMEDIATION AND MATCHING IN INSURANCE MARKETS	HCM
05-2009	Julian P. Christ and André P. Slowak	WHY BLU-RAY VS. HD-DVD IS NOT VHS VS. BETAMAX: THE CO-EVOLUTION OF STANDARD-SETTING CONSORTIA	IK
06-2009	Gabriel Felbermayr, Mario Larch, and Wolfgang Lechthaler	UNEMPLOYMENT IN AN INTERDEPENDENT WORLD	ECO
07-2009	Steffen Otterbach	MISMATCHES BETWEEN ACTUAL AND PREFERRED WORK TIME: Empirical Evidence of Hours Constraints in 21 Countries	HCM
08-2009	Sven Wydra	PRODUCTION AND EMPLOYMENT IMPACTS OF NEW TECHNOLOGIES – ANALYSIS FOR BIOTECHNOLOGY	IK
09-2009	Ralf Richter and Jochen Streb	CATCHING-UP AND FALLING BEHIND KNOWLEDGE SPILLOVER FROM AMERICAN TO GERMAN MACHINE TOOL MAKERS	IK

Nr.	Autor	Titel	CC
10-2010	Rahel Aichele and Gabriel Felbermayr	KYOTO AND THE CARBON CONTENT OF TRADE	ECO
11-2010	David E. Bloom and Alfonso Sousa-Poza	ECONOMIC CONSEQUENCES OF LOW FERTILITY IN EUROPE	HCM
12-2010	Michael Ahlheim and Oliver Frör	DRINKING AND PROTECTING – A MARKET APPROACH TO THE PRESERVATION OF CORK OAK LANDSCAPES	ECO
13-2010	Michael Ahlheim, Oliver Frör, Antonia Heinke, Nguyen Minh Duc, and Pham Van Dinh	LABOUR AS A UTILITY MEASURE IN CONTINGENT VALUATION STUDIES – HOW GOOD IS IT REALLY?	ECO
14-2010	Julian P. Christ	THE GEOGRAPHY AND CO-LOCATION OF EUROPEAN TECHNOLOGY-SPECIFIC CO-INVENTORSHIP NETWORKS	IK
15-2010	Harald Degner	WINDOWS OF TECHNOLOGICAL OPPORTUNITY DO TECHNOLOGICAL BOOMS INFLUENCE THE RELATIONSHIP BETWEEN FIRM SIZE AND INNOVATIVENESS?	IK
16-2010	Tobias A. Jopp	THE WELFARE STATE EVOLVES: GERMAN KNAPPSCHAFTEN, 1854-1923	HCM
17-2010	Stefan Kirn (Ed.)	PROCESS OF CHANGE IN ORGANISATIONS THROUGH eHEALTH	ICT
18-2010	Jörg Schiller	ÖKONOMISCHE ASPEKTE DER ENTLOHNUNG UND REGULIERUNG UNABHÄNGIGER VERSICHERUNGSVERMITTLER	HCM
19-2010	Frauke Lammers and Jörg Schiller	CONTRACT DESIGN AND INSURANCE FRAUD: AN EXPERIMENTAL INVESTIGATION	HCM
20-2010	Martyna Marczak and Thomas Beissinger	REAL WAGES AND THE BUSINESS CYCLE IN GERMANY	ECO
21-2010	Harald Degner and Jochen Streb	FOREIGN PATENTING IN GERMANY, 1877-1932	IK
22-2010	Heiko Stüber and Thomas Beissinger	DOES DOWNWARD NOMINAL WAGE RIGIDITY DAMPEN WAGE INCREASES?	ECO
23-2010	Mark Spoerer and Jochen Streb	GUNS AND BUTTER – BUT NO MARGARINE: THE IMPACT OF NAZI ECONOMIC POLICIES ON GERMAN FOOD CONSUMPTION, 1933-38	ECO

Nr.	Autor	Titel	CC
24-2011	Dhammika Dharmapala and Nadine Riedel	EARNINGS SHOCKS AND TAX-MOTIVATED INCOME-SHIFTING: EVIDENCE FROM EUROPEAN MULTINATIONALS	ECO
25-2011	Michael Schuele and Stefan Kirn	QUALITATIVES, RÄUMLICHES SCHLIEßEN ZUR KOLLISIONSERKENNUNG UND KOLLISIONSVERMEIDUNG AUTONOMER BDI-AGENTEN	ICT
26-2011	Marcus Müller, Guillaume Stern, Ansger Jacob and Stefan Kirn	VERHALTENSMODELLE FÜR SOFTWAREAGENTEN IM PUBLIC GOODS GAME	ICT
27-2011	Monnet Benoit Patrick Gbakoua and Alfonso Sousa-Poza	ENGEL CURVES, SPATIAL VARIATION IN PRICES AND DEMAND FOR COMMODITIES IN CÔTE D'IVOIRE	ECO
28-2011	Nadine Riedel and Hannah Schildberg-Hörisch	ASYMMETRIC OBLIGATIONS	ECO
29-2011	Nicole Waidlein	CAUSES OF PERSISTENT PRODUCTIVITY DIFFERENCES IN THE WEST GERMAN STATES IN THE PERIOD FROM 1950 TO 1990	IK
30-2011	Dominik Hartmann and Atilio Arata	MEASURING SOCIAL CAPITAL AND INNOVATION IN POOR AGRICULTURAL COMMUNITIES. THE CASE OF CHÁPARRA - PERU	IK
31-2011	Peter Spahn	DIE WÄHRUNGSKRISENUNION DIE EURO-VERSCHULDUNG DER NATIONALSTAATEN ALS SCHWACHSTELLE DER EWU	ECO
32-2011	Fabian Wahl	DIE ENTWICKLUNG DES LEBENSSTANDARDS IM DRITTEN REICH – EINE GLÜCKSÖKONOMISCHE PERSPEKTIVE	ECO
33-2011	Giorgio Triulzi, Ramon Scholz and Andreas Pyka	R&D AND KNOWLEDGE DYNAMICS IN UNIVERSITY-INDUSTRY RELATIONSHIPS IN BIOTECH AND PHARMACEUTICALS: AN AGENT-BASED MODEL	IK
34-2011	Claus D. Müller-Hengstenberg and Stefan Kirn	ANWENDUNG DES ÖFFENTLICHEN VERGABERECHTS AUF MODERNE IT SOFTWAREENTWICKLUNGSVERFAHREN	ICT
35-2011	Andreas Pyka	AVOIDING EVOLUTIONARY INEFFICIENCIES IN INNOVATION NETWORKS	IK
36-2011	David Bell, Steffen Otterbach and Alfonso Sousa-Poza	WORK HOURS CONSTRAINTS AND HEALTH	HCM
37-2011	Lukas Scheffknecht and Felix Geiger	A BEHAVIORAL MACROECONOMIC MODEL WITH ENDOGENOUS BOOM-BUST CYCLES AND LEVERAGE DYNAMICS	ECO
38-2011	Yin Krogmann and Ulrich Schwalbe	INTER-FIRM R&D NETWORKS IN THE GLOBAL PHARMACEUTICAL BIOTECHNOLOGY INDUSTRY DURING 1985–1998: A CONCEPTUAL AND EMPIRICAL ANALYSIS	IK

Nr.	Autor	Titel	CC
39-2011	Michael Ahlheim, Tobias Börger and Oliver Frör	RESPONDENT INCENTIVES IN CONTINGENT VALUATION: THE ROLE OF RECIPROCITY	ECO
40-2011	Tobias Börger	A DIRECT TEST OF SOCIALLY DESIRABLE RESPONDING IN CONTINGENT VALUATION INTERVIEWS	ECO
41-2011	Ralf Rukwid and Julian P. Christ	QUANTITATIVE CLUSTERIDENTIFIKATION AUF EBENE DER DEUTSCHEN STADT- UND LANDKREISE (1999-2008)	IK

Nr.	Autor	Titel	CC
42-2012	Benjamin Schön and Andreas Pyka	A TAXONOMY OF INNOVATION NETWORKS	IK
43-2012	Dirk Foremny and Nadine Riedel	BUSINESS TAXES AND THE ELECTORAL CYCLE	ECO
44-2012	Gisela Di Meglio, Andreas Pyka and Luis Rubalcaba	VARIETIES OF SERVICE ECONOMIES IN EUROPE	IK
45-2012	Ralf Rukwid and Julian P. Christ	INNOVATIONSPOTENTIALE IN BADEN-WÜRTTEMBERG: PRODUKTIONSCLUSTER IM BEREICH „METALL, ELEKTRO, IKT“ UND REGIONALE VERFÜGBARKEIT AKADEMISCHER FACHKRÄFTE IN DEN MINT-FÄCHERN	IK
46-2012	Julian P. Christ and Ralf Rukwid	INNOVATIONSPOTENTIALE IN BADEN-WÜRTTEMBERG: BRANCHENSPEZIFISCHE FORSCHUNGS- UND ENTWICKLUNGSAKTIVITÄT, REGIONALES PATENTAUFKOMMEN UND BESCHÄFTIGUNGSSTRUKTUR	IK
47-2012	Oliver Sauter	ASSESSING UNCERTAINTY IN EUROPE AND THE US - IS THERE A COMMON FACTOR?	ECO
48-2012	Dominik Hartmann	SEN MEETS SCHUMPETER. INTRODUCING STRUCTURAL AND DYNAMIC ELEMENTS INTO THE HUMAN CAPABILITY APPROACH	IK
49-2012	Harold Paredes-Frigolett and Andreas Pyka	DISTAL EMBEDDING AS A TECHNOLOGY INNOVATION NETWORK FORMATION STRATEGY	IK
50-2012	Martyna Marczak and Víctor Gómez	CYCLICALITY OF REAL WAGES IN THE USA AND GERMANY: NEW INSIGHTS FROM WAVELET ANALYSIS	ECO
51-2012	André P. Slowak	DIE DURCHSETZUNG VON SCHNITTSTELLEN IN DER STANDARDSETZUNG: FALLBEISPIEL LADESYSTEM ELEKTROMOBILITÄT	IK
52-2012	Fabian Wahl	WHY IT MATTERS WHAT PEOPLE THINK - BELIEFS, LEGAL ORIGINS AND THE DEEP ROOTS OF TRUST	ECO
53-2012	Dominik Hartmann und Micha Kaiser	STATISTISCHER ÜBERBLICK DER TÜRKISCHEN MIGRATION IN BADEN-WÜRTTEMBERG UND DEUTSCHLAND	IK
54-2012	Dominik Hartmann, Andreas Pyka, Seda Aydin, Lena Klauß, Fabian Stahl, Ali Santircioglu, Silvia Oberegelsbacher, Sheida Rashidi, Gaye Onan und Suna Erginkoç	IDENTIFIZIERUNG UND ANALYSE DEUTSCH-TÜRKISCHER INNOVATIONSNETZWERKE. ERSTE ERGEBNISSE DES TGIN-PROJEKTES	IK
55-2012	Michael Ahlheim, Tobias Börger and Oliver Frör	THE ECOLOGICAL PRICE OF GETTING RICH IN A GREEN DESERT: A CONTINGENT VALUATION STUDY IN RURAL SOUTHWEST CHINA	ECO

Nr.	Autor	Titel	CC
56-2012	Matthias Strifler Thomas Beissinger	FAIRNESS CONSIDERATIONS IN LABOR UNION WAGE SETTING – A THEORETICAL ANALYSIS	ECO
57-2012	Peter Spahn	INTEGRATION DURCH WÄHRUNGSUNION? DER FALL DER EURO-ZONE	ECO
58-2012	Sibylle H. Lehmann	TAKING FIRMS TO THE STOCK MARKET: IPOS AND THE IMPORTANCE OF LARGE BANKS IN IMPERIAL GERMANY 1896-1913	ECO
59-2012	Sibylle H. Lehmann, Philipp Hauber, Alexander Opitz	POLITICAL RIGHTS, TAXATION, AND FIRM VALUATION – EVIDENCE FROM SAXONY AROUND 1900	ECO
60-2012	Martyna Marczak and Víctor Gómez	SPECTRAN, A SET OF MATLAB PROGRAMS FOR SPECTRAL ANALYSIS	ECO
61-2012	Theresa Lohse and Nadine Riedel	THE IMPACT OF TRANSFER PRICING REGULATIONS ON PROFIT SHIFTING WITHIN EUROPEAN MULTINATIONALS	ECO

Nr.	Autor	Titel	CC
62-2013	Heiko Stüber	REAL WAGE CYCLICALITY OF NEWLY HIRED WORKERS	ECO
63-2013	David E. Bloom and Alfonso Sousa-Poza	AGEING AND PRODUCTIVITY	HCM
64-2013	Martyna Marczak and Víctor Gómez	MONTHLY US BUSINESS CYCLE INDICATORS: A NEW MULTIVARIATE APPROACH BASED ON A BAND-PASS FILTER	ECO
65-2013	Dominik Hartmann and Andreas Pyka	INNOVATION, ECONOMIC DIVERSIFICATION AND HUMAN DEVELOPMENT	IK
66-2013	Christof Ernst, Katharina Richter and Nadine Riedel	CORPORATE TAXATION AND THE QUALITY OF RESEARCH AND DEVELOPMENT	ECO
67-2013	Michael Ahlheim, Oliver Frör, Jiang Tong, Luo Jing and Sonna Pelz	NONUSE VALUES OF CLIMATE POLICY - AN EMPIRICAL STUDY IN XINJIANG AND BEIJING	ECO
68-2013	Michael Ahlheim and Friedrich Schneider	CONSIDERING HOUSEHOLD SIZE IN CONTINGENT VALUATION STUDIES	ECO
69-2013	Fabio Bertoni and Tereza Tykvová	WHICH FORM OF VENTURE CAPITAL IS MOST SUPPORTIVE OF INNOVATION? EVIDENCE FROM EUROPEAN BIOTECHNOLOGY COMPANIES	CFRM
70-2013	Tobias Buchmann and Andreas Pyka	THE EVOLUTION OF INNOVATION NETWORKS: THE CASE OF A GERMAN AUTOMOTIVE NETWORK	IK
71-2013	B. Vermeulen, A. Pyka, J. A. La Poutré, A. G. de Kok	CAPABILITY-BASED GOVERNANCE PATTERNS OVER THE PRODUCT LIFE-CYCLE	IK
72-2013	Beatriz Fabiola López Ulloa, Valerie Møller, Alfonso Sousa-Poza	HOW DOES SUBJECTIVE WELL-BEING EVOLVE WITH AGE? A LITERATURE REVIEW	HCM
73-2013	Wencke Gwozdz, Alfonso Sousa-Poza, Lucia A. Reisch, Wolfgang Ahrens, Stefaan De Henauw, Gabriele Eiben, Juan M. Fernández-Alvira, Charalampos Hadjigeorgiou, Eva Kovács, Fabio Lauria, Toomas Veidebaum, Garrath Williams, Karin Bammann	MATERNAL EMPLOYMENT AND CHILDHOOD OBESITY – A EUROPEAN PERSPECTIVE	HCM
74-2013	Andreas Haas, Annette Hofmann	RISIKEN AUS CLOUD-COMPUTING-SERVICES: FRAGEN DES RISIKOMANAGEMENTS UND ASPEKTE DER VERSICHERBARKEIT	HCM

FORSCHUNGSZENTRUM FZID

Universität Hohenheim
Forschungszentrum
Innovation und Dienstleistung
Fruwirthstr. 12
D-70593 Stuttgart
Phone +49 (0)711 / 459-22476
Fax +49 (0)711 / 459-23360
Internet www.fzid.uni-hohenheim.de