2013

Unrealistischer Optimismus der Cloud Computing Anbieter bezüglich IT Sicherheitsrisiken – Eine Bedrohung für die Nutzer?

André Loske
CASED - Center for Advanced Security Research Darmstadt, Darmstadt, Germany, andre.loske@cased.de

Thomas Widjaja
CASED - Center for Advanced Security Research Darmstadt, Darmstadt, Germany, thomas.widjaja@cased.de

Peter Buxmann
CASED - Center for Advanced Security Research Darmstadt, Darmstadt, Germany, peter.buxmann@cased.de

Unrealistischer Optimismus der Cloud Computing Anbieter bezüglich IT Sicherheitsrisiken – Eine Bedrohung für die Nutzer?

André Loske, Thomas Widjaja, und Peter Buxmann

CASED - Center for Advanced Security Research Darmstadt, Darmstadt, Germany
{andre.loske,thomas.widjaja,peter.buxmann}@cased.de

Abstract. Anbieter von Cloud Computing (CC) Lösungen versprechen zahlreiche technische und ökonomische Vorteile gegenüber klassischen IT Outsourcing Konzepten. Der Paradigmenwechsel hin zu CC induziert jedoch auch neuartige IT Sicherheitsrisiken, die zu erheblichen Bedenken seitens potenzieller Anwender führen. Anbieter von CC Lösungen betonen hingegen stetig die hohen Standards der IT Sicherheit ihrer eigenen Angebote. Auf Grundlage der kognitionspsychologischen Theorie des „unrealistischen Optimismus" und einer empirischen Untersuchung unter deutschen CC Anbietern zeigen wir, dass Anbieter die IT Sicherheitsrisiken ihrer eigenen CC Angebote in vielen Fällen systematisch unterschätzen. Das Verständnis der systematischen Verzerrungen bei der Risikowahrnehmung ermöglicht Wissenschaftlern, Anbietern und Nutzern das tatsächliche Risiko besser zu bewerten und so gezielter Strategien zur Verbesserung der IT Sicherheit im CC zu entwickeln.

Keywords: Cloud Computing, Unrealistischer Optimismus, IT Sicherheit, psychologische Faktoren, Risikomanagement

1 Einleitung

Outsourcing der Informationstechnologie (IT) an externe Anbieter ist heute Bestandteil der IT Strategie vieler Unternehmen. Cloud Computing (CC) stellt eine Weiterentwicklung klassischer IT Outsourcing (ITO) Konzept unter Verwendung moderner Kommunikationstechnologien dar, das auf zunehmendes Interesse stößt, aber derzeit auch Gegenstand kontroverser öffentlicher und wissenschaftlicher Diskussionen ist. CC ist ein Modell *„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"* [1]. Obwohl CC gegenüber klassischen ITO Konzepten eine Vielzahl technischer und ökonomischer Vorteile verspricht, bleibt die Akzeptanz bei den Nutzern weit hinter den Erwartungen zurück [2]. Insbesondere das wiederholte Auftreten aufsehenerregender Zwischenfälle hat potentielle Nutzer in den letzten Jahren hinsichtlich der IT Sicherheitsrisiken (ITSR) von

11th International Conference on Wirtschaftsinformatik,
27th February – 01st March 2013, Leipzig, Germany

CC stark sensibilisiert und in vielen Fällen langfristig von der Nutzung abgeschreckt [3]. Im April 2011 haben bspw. hunderte Kunden einen Großteil ihrer gespeichert Daten durch einen fatalen Systemabsturz der Amazon EC2 Dienste verloren. Wenige Monate später verursachte ein Blitzschlag einen über 48 stündigen Ausfall von Microsofts CC Dienst "Business Productivity Online Suite". Während des gesamten Zeitraums hatten die Nutzer weder Zugriff auf Ihre E-Mails, Kalender und Kontakte noch auf Ihre Dokumente im Managementsystem [4]. Sicherheitsexperten betonen allerdings das Vorhandensein geeigneter Konzepte und Maßnahmen, die einen umfassenden Schutz der CC Angebote hinsichtlich der ITSR gewährleisten können [5]. Angesichts der Häufung sicherheitsrelevanter Zwischenfälle in der Cloud stellt sich die Frage, ob die Anbieter die ITSR erheblich unterschätzen und in Folge erforderliche Sicherheitsmaßnahmen und -konzepte nicht hinreichend umsetzen?

Eine mögliche systematische Unterschätzung der ITSR durch die CC Anbieter beruht im Wesentlichen auf dem Umstand, dass nicht das tatsächliche Risiko, sondern das seitens einer Person wahrgenommene Risiko, bspw. durch den Sicherheitsbeauftragten oder CIO, die Risikobewertung für ein Unternehmen bestimmt. Die Höhe des wahrgenommenen Risikos weicht allerdings oftmals signifikant vom tatsächlichen Risiko ab, da z. B. erforderliche Informationen fehlen und kognitive Abläufe die Einschätzung unbewusst in bestimmte Richtungen verzerren können [6]. Insbesondere im Bereich der IT existieren i. d. R. keine vergangenheitsbezogenen Daten bzgl. des Schadens und der Auftrittswahrscheinlichkeit bestimmter ITSR, die eine objektive Quantifizierung des tatsächlichen Risikos ermöglichen würden. Das Fehlen quantitativer Daten ist im Wesentlichen darauf zurückzuführen, dass die IT im Allgemeinen einem schnellen technologischen Wandel mit kurzen Produktlebenszyklen unterliegt und außerdem Sicherheitsvorfälle in vielen Fällen nicht entdeckt oder nicht systematisch dokumentiert werden [7]. Das wahrgenommene Risiko eines Entscheidungsträgers basiert dann häufig auf sozialen Vergleichen mit anderen Personen bzw. Unternehmen [8-9]. Menschen tendieren allerdings im Allgemeinen dazu, ihr persönliches Risiko erheblich geringer einzuschätzen als das Risiko der Vergleichsperson. Diese systematische Unterschätzung des Risikos basiert hauptsächlich auf einem abstrakten Gefühl der persönlichen Unverwundbarkeit und wird in der Literatur als „unrealistischer Optimismus" (UO) bezeichnet [10]. UO in der Risikowahrnehmung konnte bereits von Wissenschaftlern in unterschiedlichen Disziplinen, z. B. bzgl. gesundheitlicher Probleme, Autounfällen oder Kriminalität, nachgewiesen werden [11-13].

Systematische Unterschätzungen eines Risikos sind dabei insbesondere hinsichtlich der reduzierten Motivation zur Umsetzung erforderlicher Präventions- oder Schutzmaßnahmen als überaus kritisch zu betrachten [14-15]. Raucher kennen z. B. im Allgemeinen die, mit dem Rauchen verbunden, Gesundheitsrisiken, wie Lungenkrebs oder Herzinfarkt. Jedoch erst mit dem Bewusstsein, um die persönliche Verwundbarkeit durch, bspw. in Folge des Auftretens erster Symptome, leiten Personen entsprechende Maßnahmen ein [16]. Gleichermaßen benötigen die Verantwortlichen seitens der CC Anbieter zunächst ein Bewusstsein für die Verwundbarkeit ihrer Dienste durch bestimmte ITSR, bevor Entscheidungen für die Umsetzung notwendige und ggf. kostenintensive Sicherheitsmaßnahmen getroffen werden. Das Wissen um

die Existenz eines IT Sicherheitsrisikos allein ist demnach im Allgemeinen nicht ausreichend. Es ergeben sich die folgenden Forschungsfragen für den UO im CC:

1. *Sind die CC Anbieter unrealistisch optimistisch bzgl. der ITSR?*
2. *Hat UO negative Folgen für die Awareness der CC Anbieter bzgl. der ITSR?*
3. *Variiert der Grad des UO der CC Anbieter in Abhängigkeit der Charakteristika einzelner ITSR?*

In der vorliegenden Studie zeigen wir anhand der spezifischen ITSR von CC [4], dass der UO sowohl relativ zu anderen Wettbewerbern als auch insgesamt [10] eine systematische Unterschätzung der relevanten ITSR seitens der Anbieter bedingt. Grundlage der Untersuchung des UO ist eine quantitative empirische Studie unter den CC Anbietern im deutschen Markt, wobei die Entscheidungsträger gebeten wurden die ITSR jeweils für das eigene Unternehmen sowie den durchschnittlichen Wettbewerber im Markt zu bewerten. Der Vergleich der Durchschnittswerte aus der Einschätzung des ITSR des eigenen Unternehmens und der des durchschnittlichen Wettbewerbs erlaubt dabei eine differenzierte Analyse systematischer Verzerrungen bzw. des UO [11]. Darüber hinaus weisen wir nach, dass der UO bei den einzelnen Anbietern zu einem signifikant reduzierten Bewusstsein (Awareness) bzw. Auseinandersetzung der Verantwortlichen mit den ITSR und –maßnahmen [17] im Bereich des CC führt.

Mit der Schaffung eines besseren Verständnisses der kognitiven Abläufe und insbesondere der s. g. „systematischen kognitiven Fehlleistungen“ bei der Wahrnehmung von Risiken, können die Ergebnisse den Anbietern in erster Linie eine Verbesserung ihrer Strategien zur Risikobewertung, auch bei zukünftigen Technologieinnovationen, ermöglichen. Eine korrekte Bewertung der ITSR seitens der Anbieter stellt eine Grundvoraussetzung dar, um mögliche Bedrohungen rechtzeitig zu identifizieren und Sicherheitsmaßnahmen in erforderlichem Umfang zu implementieren. Durch die Implementierung der objektiv erforderlichen Sicherheitsmaßnahmen kann sowohl der Schutz der CC Angebote gesteigert als auch der finanzielle Aufwand für die Sicherheit optimiert werden. Mit einer Steigerung der IT Sicherheit kann außerdem eine langfristige Verbesserung der Akzeptanz von CC erwartet werden.

Auch wenn insbesondere die Marketingabteilungen der CC Anbieter angesichts der zögerlichen Nachfrage unablässig den umfassenden Schutz der Dienste betonen, sollten die Nutzer den Stand der IT Sicherheit anhand unserer Ergebnisse kritisch hinterfragen und für Risiken mit typischerweise hohen Verzerrungen ggf. eigene Sicherheitsüberprüfungen vor Vertragsabschluss durchführen.

2 Grundlagen: ITSR im CC und Unrealistischer Optimismus

2.1 Wahrgenommene ITSR von CC

Auf Basis von Cunningham (1967) wird wahrgenommenes Risiko in der Literatur oftmals als “*the felt uncertainty regarding the possible negative consequences of adopting a product or service*” verstanden [18]. Die Analyse von (insb. wahrgenommenen) Risiken hat im Kontext von ITO eine lange Tradition – mit der Entwicklung

des ITO-Konzepts hat sich jedoch der Fokus der betrachteten Risikodimensionen verschoben: Während bei der Forschung zu traditionellem ITO eher strategische und finanzielle Risiken im Vordergrund standen [19-20], änderte sich der Betrachtungsgenstand mit dem Aufkommen von Application Service Providing (ASP) und CC in Richtung eher technisch bedingter Risiken [21-22]. Aktuelle Studien zeigen, dass gerade die IT sicherheitsbezogenen Risiken den größten Einfluss auf die Adoptionsentscheidung im CC Kontext haben [21].

Wir definieren das wahrgenommene ITSR im CC Kontext als *das vom Entscheider wahrgenommen Risiko für die Sicherheit der IT des Unternehmens wenn CC als Bezugsmodell verwendet wird*. Damit bauen wir auf Forschungsergebnissen zur Konzeptualisierung der wahrgenommenen ITSR im Kontext von CC aus einer vorangegangenen Studie auf [4]. Hierbei wurde auf Basis einer umfangreichen Literaturrecherche, eines anschließenden Q-Sorts (6 IS Experten), strukturierten Interviews mit 24 IT Sicherheitsexperten und einer empirischen Untersuchung unter 356 Unternehmen eine umfassende Konzeptualisierung von wahrgenommenen ITSR für den CC Kontext entwickelt und validiert (in der Studie als PITSR - Perceived IT Security Risk) bezeichnet. Dabei konnten wir „*Verfügbarkeit*“, „*Vertraulichkeit*“, „*Integrität*“, „*Leistung*“, „*Anpassbarkeit und Wartung*“ und „*Zurechenbarkeit*“ als die sechs Risikodimensionen wahrgenommener ITSR identifizieren. Die Risikodimension Verfügbarkeit bezieht sich dabei darauf, dass der Zugriff auf das Angebot und die Daten zu jedem vom Kunden gewünschten Zeitpunkt möglich ist. Unter Vertraulichkeit verstehen wir, dass Daten ausschließlich von autorisierten Benutzern gelesen werden. Die Dimension Integrität umfasst Risiken bezüglich der Veränderung von Daten durch Unbefugte. Leistungsrisiken betreffen Vorfälle, durch die eine Nutzung des CC Angebots und der Daten nicht in der Geschwindigkeit erfolgen kann, die den Anforderungen der Kunden entspricht. Unter Anpassbarkeit und Wartung verstehen wir, dass die Anpassungen des Angebots an eigene bzw. geänderte Anforderungen möglich und Wartung sowie Support gewährleistet sind. Zurechenbarkeitsrisiken treten auf, wenn Authentifizierungsmechanismen umgangen werden können und Aktionen im Rahmen der Nutzung des Angebots nicht eindeutig identifizierbaren Benutzern zugeordnet werden können. Zu den sechs Dimensionen wurden zudem 31 IT-Sicherheitsrisiken von CC identifiziert (vgl. Tabelle 3 in Kap. 3.3).

2.2 Unrealistischer Optimismus

Menschen tendieren in vielen Fällen dazu, sich anderen überlegen zu fühlen. Obwohl wissenschaftliche Studien [23] zeigen, dass dieses Phänomen nicht zwangsläufig mit negativen Konsequenzen verbunden sein muss und für das Selbstwertgefühl bzw. das psychische Wohlbefinden einer Person sogar unabdingbar sein kann [24], verdeutlichen resultierende Verzerrungen in der Bewertung von Risiken gleichzeitig eine mögliche Gefahr. Individuen schreiben sich selbst vielfach wünschenswerte Attribute zu und interpretieren vorhandene Informationen oder unbekannte Sachverhalte in für sich positiver Weise [16]. Aufgrund dieser kognitiven Prozesse unterschätzen Personen typischerweise besonders die eigene Wahrscheinlichkeit für das Auftreten negativer Ereignisses im Vergleich zu anderen erheblich und lassen auch im Hinblick auf

bekannte Risiken nicht die notwendige Vorsicht walten [11]. Diese s. g. „systematische kognitive Fehlleistung“ wird in der Literatur als „unrealistischer Optimismus“, „optimistische Verzerrung“ oder „optimistischer Fehlschluss“ bezeichnet [10].

Frühere Studien über die Verzerrung der Risikowahrnehmung konnten nachweisen, dass Personen im Allgemeinen besonders UO bei der Einschätzung ihrer Verwundbarkeit durch verschiedene negative Ereignisse zeigen. So schätzt bspw. Menschen das eigene Risiko für das Auftreten gesundheitlicher Probleme, wie z. B. Herzinfarkt, chronische Krankheiten oder auch AIDS, signifikant geringer ein als das Risiko einer anderen Person mit gleichem Geschlechts, Alter und Bildungsstand [11]. Neben den gesundheitlichen Risiken konnte UO von Wissenschaftlern in einer Vielzahl anderer Bereichen, z. B. hinsichtlich Risiken des Autofahrens, Rauchens oder Kriminalität, gezeigt werden [12-13], [16]. Auch in unserer Disziplin konnte in Bezug auf Risiken der Internetnutzung sowie der IT Sicherheit im Allgemeinen bereits UO bei den Entscheidungsträger in Unternehmen nachgewiesen werden [25-26].

Das Vorhandensein von UO bei einem Individuum kann grundsätzlich bewertet werden, wenn die Risikoeinschätzung der Person mit dem tatsächlichen Risiko verglichen werden kann. Allerdings sind in vielen Bereichen, wie bspw. der IT, keine geeigneten quantitativen Daten verfügbar, um das tatsächliche Risiko bestimmen zu können. Die Bewertung des UO ist dann für eine einzelne Person im Allgemeinen nicht möglich, da die Einschätzung der befragten Person, dass sie einem geringeren Risiko ausgesetzt sei, durchaus korrekt sein könnte [27]. Die UO Forschung bedient sich in diesem Fall einem Vergleich der Risikobewertungen einer bestimmten Personengruppe, wobei die Teilnehmer aufgefordert werden ihr Risiko im Vergleich zu einer Referenz (direkte Methode) oder ihr eigenes Risiko und das Risiko der Referenz separat (indirekte Methode) zu bewerten [15]. Die Referenz des Vergleichs hängt dabei vom Gegenstand der Untersuchung ab und kann sowohl eine andere Person mit bestimmten Merkmalen als auch ein Wettbewerber bzw. ein anderes Unternehmen sein. Anhand eines Vergleichs der Mittelwerte der Selbsteinschätzungen und des Durchschnitts der Bewertungen der anderen Personen kann untersucht werden, ob eine Person bzw. ein Personenkreis ein Risiko systematisch verzerrt wahrnimmt [11]. Ist bspw. die Risikowahrnehmung einer repräsentativen Stichprobe von Rauchern nicht systematisch durch UO verzerrt, sollte die Differenz zwischen dem Durchschnitt der Einschätzungen des eigenen Risikos und der Bewertung des durchschnittlichen Rauchers gleich Null sein. Andernfalls würden sich alle Raucher im Durchschnitt einem anderen Risiko ausgesetzt sehen als der durchschnittliche Raucher und eine Verzerrung der Risikobewertung dieser Personengruppe wäre offenkundig.

Grundlage dieser Vorgehensweise bildet die Theorie des sozialen Vergleichs nach Festinger (1954) [9]. Personen streben zwar grundsätzlich zunächst eine Bewertung ihres Risikos mit objektiven Maßnahmen an, bedienen sich allerdings beim Fehlen entsprechender Mittel einem Vergleich mit anderen Personen, denen sie ähnliche Eigenschaften zurechnen [28]. Auch wenn der kognitive Mechanismus in erster Linie einer objektiven Einschätzung eines Risikos dienen soll, zeigen Studien in diesem Bereich, dass unterschiedliche Einflussfaktoren, wie bspw. Selbstüberschätzung oder Wünsche, den Vergleich beeinflussen können [29]. So neigen Personen bspw. unbewusst dazu, sich mit anderen zu vergleichen, von denen sie wissen, dass sie hinsicht-

lich bestimmter Eigenschaften benachteiligt sind. Auf diese Weise werden Bedrohungen negativer Ereignisse relativiert und das persönliche Wohlbefinden gesteigert [30]. Analog würde eine solche optimistische Verzerrung bspw. die Zufriedenheit des Entscheidungsträgers im CC hinsichtlich seines beruflichen Erfolges steigern und gleichzeitig die Wahrnehmung der Verwundbarkeit der Dienste durch die ITSR reduzieren [26].

Als wesentliche Einflussfaktoren auf den UO wurden von den Wissenschaftlern in früheren Studien die wahrgenommene Kontrolle und die s. g. „soziale Distanz" zur Vergleichsperson identifiziert [31]. Die wahrgenommene Kontrolle beschreibt dabei die Erwartung einer Person, inwieweit sie den Ausgang eines bestimmten Ereignisses in ihrem Sinne beeinflussen kann. Außerdem bestimmt die Charakteristik des Vergleichsziels als soziale und psychologische Distanz den Grad des UO einer Person. Die Befragten zeigen im Allgemeinen einen höheren UO, wenn sie sich mit einer durchschnittlichen anderen Person statt einer bestimmten Person, wie bspw. einem Freund, vergleichen sollen, da ersteren eher schlechtere Eigenschaften zugerechnet werden [13].

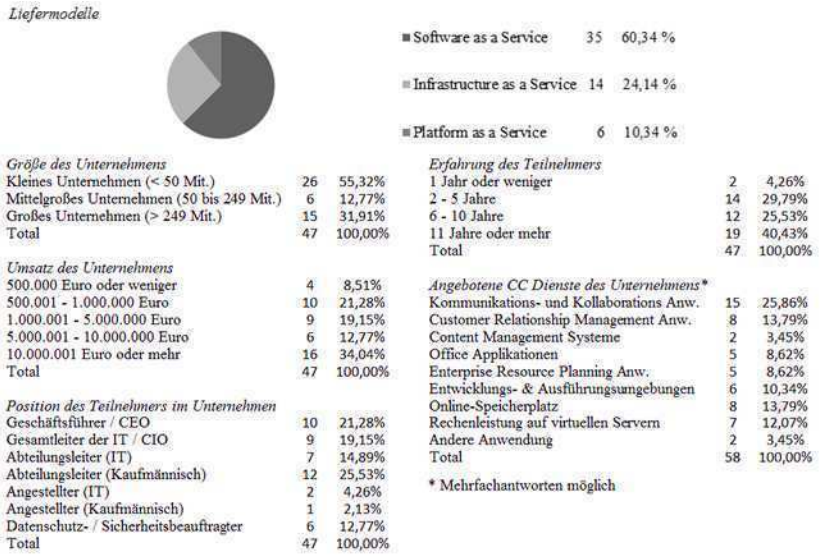
3 Empirische Studie – Unrealistischer Optimismus im CC

3.1 Datenerhebung und Analyse

Zur Identifikation und Bewertung des unrealistischen Optimismus in der Risikowahrnehmung der CC Anbieter wurde ein Fragebogen entwickelt und in einem mehrstufigen Prozess anhand kognitiver Interviews [32] mit 4 Wissenschaftlern und 7 Experten aus der Praxis getestet, wodurch einige Formulierungen geschärft werden konnten. Die finale Version des Fragebogens enthält Indikatoren zur empirischen Bewertung der (Gesamt-) ITSR, der (Einzel-) ITSR sowie Elemente zur Messung des Bewusstseins *(Awareness)* bzgl. ITSR von CC. Der Fragebogen wurde an 247 CC Anbieter im deutschen Markt (Stand: Dezember 2011) verteilt, die im Wesentlichen anhand entsprechender Publikationen [33] sowie Datenbanken, unterstützt von einer systematischen Recherche in einem sozialen Netzwerk im Internet (Xing), ermittelt werden konnten. Sofern entsprechende Informationen verfügbar waren, haben wir grundsätzlich zunächst den CIO oder IT Sicherheitsbeauftragten des Unternehmens kontaktiert. Bei vielen kleineren CC Anbietern konnte ausschließlich der Geschäftsführer bzw. CEO ermittelt werden. Die Fragebögen wurden anschließend oftmals innerhalb des Unternehmens an den Verantwortlichen weitergeleitet, der uns im Folgenden als Ansprechpartner für die Studie diente.

Die Datenerhebung fand im Zeitraum vom 10. Juni bis 20. Juli 2012 statt. Die Ansprechpartner wurden durch das Angebot eines detaillierten Ergebnisberichts mit einer Übersicht über die Risikobewertung der Wettbewerber sowie einer Erinnerung per E-Mail zur Teilnahme motiviert. Darüber hinaus wurden nach Ablauf des halben Datenerhebungszeitraums alle bekannten Ansprechpartner telefonisch kontaktiert und an die Studie erinnert. Nach Ablauf des Zeitraums haben wir insgesamt 58 ausgefüllte Fragebögen (23,5%) erhalten, wobei 11 aufgrund schlechter Datenqualität oder feh-

lender Angaben bei einzelnen Indikatoren aussortiert werden mussten. Insbesondere in Anbetracht der Schwierigkeiten bei der Erhebung von Daten bei IT Führungskräften stellt dies ein gutes Ergebnis dar, das auch auf Interesse der CC Anbieter an der Thematik schließen lässt [34].



Liefermodelle

Software as a Service	35	60,34 %
Infrastructure as a Service	14	24,14 %
Platform as a Service	6	10,34 %

Größe des Unternehmens		
Kleines Unternehmen (< 50 Mit.)	26	55,32%
Mittelgroßes Unternehmen (50 bis 249 Mit.)	6	12,77%
Großes Unternehmen (> 249 Mit.)	15	31,91%
Total	47	100,00%

Umsatz des Unternehmens		
500.000 Euro oder weniger	4	8,51%
500.001 - 1.000.000 Euro	10	21,28%
1.000.001 - 5.000.000 Euro	9	19,15%
5.000.001 - 10.000.000 Euro	6	12,77%
10.000.001 Euro oder mehr	16	34,04%
Total	47	100,00%

Position des Teilnehmers im Unternehmen		
Geschäftsführer / CEO	10	21,28%
Gesamtleiter der IT / CIO	9	19,15%
Abteilungsleiter (IT)	7	14,89%
Abteilungsleiter (Kaufmännisch)	12	25,53%
Angestellter (IT)	2	4,26%
Angestellter (Kaufmännisch)	1	2,13%
Datenschutz- / Sicherheitsbeauftragter	6	12,77%
Total	47	100,00%

Erfahrung des Teilnehmers		
1 Jahr oder weniger	2	4,26%
2 - 5 Jahre	14	29,79%
6 - 10 Jahre	12	25,53%
11 Jahre oder mehr	19	40,43%
Total	47	100,00%

*Angebotene CC Dienste des Unternehmens**		
Kommunikations- und Kollaborations Anw.	15	25,86%
Customer Relationship Management Anw.	8	13,79%
Content Management Systeme	2	3,45%
Office Applikationen	5	8,62%
Enterprise Resource Planning Anw.	5	8,62%
Entwicklungs- & Ausführungsumgebungen	6	10,34%
Online-Speicherplatz	8	13,79%
Rechenleistung auf virtuellen Servern	7	12,07%
Andere Anwendung	2	3,45%
Total	58	100,00%

* Mehrfachantworten möglich

Abb. 1. Deskriptive Teilnehmerdaten der empirischen Untersuchung

Eine Analyse der Charakteristik der deskriptiven Teilnehmerdaten (s. Abbildung 1) lässt auf eine gute Repräsentativität der Stichprobe schließen [35]. Sowohl im Hinblick auf die angebotenen Dienste (60,3 % Software-as-a-Service; 25,9 % Infrastructure-a-Service; 10,3 % Platform-as-a-Service) als auch auf die Liefermodelle sowie die Unternehmensgröße bilden die Teilnehmer ungefähr den Durchschnitt des CC Markts ab [33]. In Anbetracht der Kritikalität systematischer Antwortausfälle bei der Bewertung des unrealistischen Optimismus, bspw. könnten sich die teilnehmenden Anbieter intensiver mit der IT Sicherheit im CC befassen und in Folge objektiv einem geringeren Risiko ausgesetzt sein, haben wir weitere Untersuchungen der Stichprobe durchgeführt. Nach Armstrong und Overton (1977) haben wir die frühsten 25% mit den 25% letzten (alle nach der schriftlichen und telefonischen Erinnerung) der eingegangenen Antworten verglichen [36]. Die Vorgehensweise prüft die Auswirkungen der Höhe des Interesses der Befragten auf das Antwortverhalten unter der Annahme, dass Teilnehmer mit hohem Interesse sich frühzeitiger an der Studie beteiligen. Wir konnten in der Stichprobe mit t-Tests keine signifikanten Unterschiede zwischen den Antworten in den betrachteten Variablen identifizieren. Im Rahmen der Telefonanrufe bzw. der Kontaktaufnahme in sozialen Netzwerken haben wir die Ansprechpartner außerdem nach dem Grund für die ggf. fehlende Bereitschaft zur Teilnahme befragt. In den meisten dieser Fälle haben unternehmensinterne Richtlinien grundsätzlich eine

Beteiligung an Umfragen jeglicher Art verboten oder fehlende Zeit haben es den Ansprechpartner nicht erlaubt sich an der Studie zu beteiligen.

3.2 Verwendete Skalen

Zur Sicherstellung der Konstrukts- und Inhaltsvalidität des Messmodells haben wir Skalen und Elemente aus vorhergehenden wissenschaftlichen Studien mit geringfügigen Anpassungen der ursprünglichen Formulierungen adaptiert (siehe Tabelle 1).

Tabelle 1. Verwendete Skalen der empirischen Untersuchung

Konstrukt	**Indikator**	**Quelle**
Wahrgenommen (Einzel-) ITSR für die CC Dienste	Wie bewertet Ihr Unternehmen das Risiko für (potenzielle) Nutzer des Cloud Computing-Angebots *(Ihres Unternehmens / Ihrer Wettbewerber)*, dass *(IT Sicherheitsrisiko, siehe Tabelle 3 in Kap. 3.3)* • überhaupt nicht riskant - überaus riskant	Indikatoren basieren auf Ackermann et al. (2012)
Wahrgenommenes (Gesamt-) ITSR für die CC Dienste	Zusammenfassend und unter Berücksichtigung aller Faktoren, die die Sicherheit der IT (potentieller) Nutzer betreffen, wäre es für die allgemeine IT Sicherheit der Nutzer … das Cloud Computing Angebot *(unseres Unternehmens / unserer Wettbewerber)* zu nutzen. • überhaupt nicht riskant – überaus riskant	Indikatoren basieren auf Featherman und Pavlou (2003)
Bewusstsein *(Awareness)* bzgl. ITSR von CC	• Unser Unternehmen hat einen guten Überblick über die Bedrohungen der IT Sicherheit von Cloud Computing *(Wissen)* • Unser Unternehmen hat sich sehr intensiv mit dem Thema Sicherheit im Cloud Computing auseinandergesetzt *(Verhalten)* • Cloud Computing setzt die Nutzer aus unserer Sicht keinen besonderen ITSR aus *(Einstellung)*	Indikatoren basieren auf Kruger und Kearney (2006); Featherman und Pavlou (2003)

Zur empirischen Bewertung der Wahrnehmung der einzelnen ITSR und des aggregierten Gesamtrisikos für das CC Angebot wurden die Indikatoren von Ackermann et al. (2012) [4] bzw. Featherman und Pavlou (2003) [37] verwendet. Jeder dieser Indikatoren wurden jeweils für die CC Angebote des eigenen Unternehmens und des durchschnittlichen Wettbewerbs getrennt abgefragt. Zur Messung des Bewusstseins (*Awareness*) für die IT Sicherheit der CC Anbieter wurden die Indikatoren von Kruger und Kearney (2006) auf den CC Kontext angepasst [17]. Die Auswahl der Referenz bzw. des Bezugsobjekts der Risikobewertung ist insbesondere hinsichtlich der sozialen Distanz, welche die Höhe des UO beeinflusst [8], sowie der Vergleichbarkeit der Ergebnisse relevant. Als Vergleichsobjekt zum eigenen Unternehmen wurde der durchschnittliche Wettbewerber ausgewählt, definiert als Anbieter mit Diensten ähnlicher Spezifikation im selben Marktsegment. Auf diese Weise kann die soziale Distanz fixiert und die Risikobewertungen auf äquivalente Vergleichsobjekte bezogen

werden, so dass auch verschiedenartigen Angeboten in absoluter Hinsicht verglichen werden können [38]. Die Teilnehmer sollten die ITSR anhand der Auswahl Ihrer Risikowahrnehmung auf einer 7er Skala zwischen zwei vorgegebenen Adjektiven bewerten. Die Auseinandersetzung mit der IT-Sicherheit wurde mit einer 7er Likert-Skala gemessen, wobei 1 die geringste und 7 die höchste Zustimmung des Befragten zu einer Behauptung repräsentieren.

3.3 Ergebnisse der empirischen Untersuchung

Forschungsfrage 1 (UO bei CC Anbietern). Wenn die Risikowahrnehmung der CC Anbieter im deutschen Markt nicht systematisch aufgrund UO verzerrt ist, müsste mathematisch für die Differenz des Durchschnitts der Risikowahrnehmungen für das eigenen Unternehmen und der Bewertungen des durchschnittlichen Wettbewerbers $\bar{D} = 0$ gelten, wobei R_{ijk} die Bewertung des ITSR Indikators i ($i = 0$: Gesamt-ITSR) in Bezug auf die Referenz j ($j = 1$: eigenes Unternehmen; $j = 2$: durchschnittlicher Wettbewerber) durch den CC Anbieter $k \in K$ ist.

$$\bar{M}_{ij} = \sum_k \frac{R_{ijk}}{|K|} \tag{1}$$

$$\bar{D}_i = \bar{M}_{i1} \tag{2}$$

Die Anwendung eines zweiseitigen t-Tests zeigt, dass sich die Mittelwerte der Risikobewertungen zwischen den eigenen Unternehmen und den durchschnittlichen Wettbewerbern hochsignifikant ($t(46) = -8{,}84$; $ps < 0{,}001$) mit $\bar{D}_0 = -1{,}66$ unterscheiden. Die CC Anbieter schätzen folglich im Durchschnitt das ITSR der eigenen Dienste signifikant geringer ein als das des durchschnittlichen Anbieters, so dass auf eine systematische Verzerrung der Risikowahrnehmung der CC Anbieter im deutschen Markt aufgrund von UO geschlossen werden [11]. Die Ergebnisse zeigen darüber hinaus, dass die CC Anbieter insgesamt das Risiko für die CC Dienste des eigenen Angebots als sehr gering ($\bar{M}_{01} = 1{,}55$) sowie des durchschnittlichen Angebots als eher gering ($\bar{M}_{01} = 3{,}21$) einschätzen. Ein einzelner Anbieter k kann genau dann als unrealistisch optimistisch betrachtet werden, wenn seine Wahrnehmung des ITSRs für das eigene Unternehmen signifikant vom Durchschnitt (über alle befragten Anbieter) der Bewertungen des ITSRs des durchschnittlichen Anbieters abweicht [11].

$$UO_{ik} = R_{i1k} - \bar{M}_{i2} \tag{3}$$

35 CC Anbieter (74,5%) aus unserer Stichprobe weisen eine negative Differenz zwischen der Wahrnehmung des ITSR der eigenen Dienste und der durchschnittlichen Risikobewertung aller Anbieter auf ($UO_{0k} < 0$) und können folglich als unrealistisch Optimistisch betrachtet werden.

Forschungsfrage 2 (UO und *Awareness* der CC Anbieter für ITSR). Alle Anbieter im Markt haben angegeben, einen guten Überblick über die IT Sicherheitsbedrohungen von CC (M = 6,49) zu haben und sich sehr intensiv mit dem Thema Sicherheit im CC auseinanderzusetzen (M = 6,27). Eine besondere Bedrohung der CC Dienste durch ITSR sehen die Anbieter im Allgemeinen eher nicht (M = 5,21).

Ein Vergleich der Mittelwerte zwischen Anbietern die UO ($UO_{0k} < 0$) und Anbietern die keinen UO ($UO_{0k} \geq 0$) in der Auseinandersetzung mit ITSR gezeigt haben, verdeutlicht hochsignifikante (D = 0,65; $t(33)$ = 5,12; $ps < 0{,}001$) bzw. signifikante (D = 0,82; $t(19)$ = 3,67; $ps < 0{,}05$) Abweichungen (zweiseitiger t-Test), wobei positive Differenzen eine höhere Zustimmung der Anbieter ohne UO repräsentieren (s. Tabelle 2). Anbieter deren Risikowahrnehmung nicht durch UO verzerrt ist, haben sich folglich intensiver mit der IT Sicherheit im CC auseinandergesetzt und haben einen besseren Überblick. Demgegenüber sind Anbieter, bei denen kein UO nachgewiesen werden konnte, erheblich kritischer gegenüber der IT Sicherheit von CC ($D = -0{,}86$; $t(14) = -2{,}07$; $ps < 0{,}01$) eingestellt. Eine negative Differenz zeigt in diesem Fall eine geringere Zustimmung dieser Anbieter zur Aussage, dass CC im Allgemeinen mit keinen besonderen ITSR verbunden ist. Insgesamt zeigen Anbieter, denen keine Verzerrung der Risikowahrnehmung aufgrund UO festgestellt werden konnte, tendenziell ein höheres Bewusstsein gegenüber den ITSR im CC [17]. Die Resultate bestätigen die Befunde in anderen Forschungsgebieten im Bereich der ITSR von CC, wonach der UO signifikant negative Auswirkungen auf das Bewusstsein für Risiken und damit die umgesetzte, Sicherheitsmaßnahmen hat [14-15].

Tabelle 2. Mittelwerte der *Awareness* bzgl. ITSR von CC (N=47)

***Awareness* bzgl. ITSR im CC**	**UO[a]**	**M[b]**	**SD[c]**	**D[d]**	**SE[e]**
Wissen	kein UO (≥ 0)	6,92	0,15	0,65***	0,31
	UO (< 0)	6,21	0,80		
Verhalten	kein UO (≥ 0)	6,71	0,49	0,82*	0,22
	UO (< 0)	5,90	0,78		
Einstellung	kein UO (≥ 0)	4,85	1,90	-0,86**	0,75
	UO (< 0)	5,71	1,25		

[a] UO ≥ 0: kein UO empirisch nachgewiesen; UO < 0: UO empirisch nachgewiesen.

[b] Mittelwert (M) der Indikatoren auf 7er Likert-Skala gemessen mit 1 (stimme überhaupt nicht zu) und 7 (stimme voll und ganz zu).

[c] Standardabweichung (SD)

[d] Differenz (D) der Mittelwerte, wobei ein positiver Wert eine höhere Zustimmung und eine negative Differenz eine geringere Zustimmung der Anbieter repräsentiert, denen kein UO empirisch nachgewiesen werden konnte. Signifikanzen mit zweiseitigem t-Test: *** $ps < 0{,}001$; ** $ps < 0{,}01$; * $ps < 0{,}05$.

[e] Standardfehler (SE)

Das Bewusstsein *(Awareness)* für ITSR hat im Allgemeinen starke Auswirkungen auf die konsequente Umsetzung von IT Sicherheitsmaßnahmen in Unternehmen [39]. Empirische Studien in diesem Bereich zeigen, dass die Unternehmen, deren Mitarbeiter über ein hohes Bewusstsein für die Relevanz von ITSR verfügen, objektiv erheb-

lich besser geschützt sind. Neben höheren Investitionen im Bereich der IT Sicherheit wurden die Maßnahmen in diesen Unternehmen eher organisationsweit umgesetzt bzw. von den Mitarbeitern stetig mitgetragen [17]. Das reduzierte Bewusstsein für ITSR hat somit auch negative Folgen für die IT Sicherheit der CC Angebote [26].

Forschungsfrage 3 (UO und Charakteristika der ITSR von CC). Die Analyse der empirischen Bewertungen der untersuchten 31 Risikoelemente von CC durch die Anbieter für das eigene Angebot und das der durchschnittlichen Wettbewerber, zeigt eine signifikante, systematische Verzerrung der Risikowahrnehmung [11]. Aufgrund der überschneidungsfreien und vollständigen Abdeckung der Gesamtheit der ITSR von CC durch die 31 Risikoelemente liefern die empirischen Befunde eine starke Bestätigung für das Vorhandensein von UO im CC (Forschungsfrage 1) [4]. Die Untersuchung erfolgt mit einem zweiseitigen t-Test anhand der Annahme, dass die Risikoeinschätzung der Anbieter in den Einzelrisiken nicht durch UO verzerrt sind und folglich die Differenzen der Mittelwerte zwischen der Bewertung des eigenen Unternehmens und des durchschnittlichen Wettbewerbers gleich Null ist ($\sum_1^{31} \overline{D}_i = 0$; vgl. Forschungsfrage 1: Formel 2) [11]. Die Annahme kann in der Stichprobe allerdings mit $\sum_1^{31} \overline{D}_i = -0{,}90$ verworfen werden, wobei sich alle Einzelrisiken signifikante und negative Differenzen aufweisen (vgl. Tabelle 3). Die Anpassbarkeits- und Wartungsrisiken sind dabei im Mittel durch die höchste Verzerrung ($\sum_{i=1}^{7} \overline{D}_i = -1{,}02$) gekennzeichnet. Die übrigen Risikofacetten weisen im Durchschnitt eine ähnliche negative Differenz der Mittelwerte auf (Integritätsrisiken: $\sum_{i=8}^{12} \overline{D}_i = -0{,}89$; Leistungsrisiken: $\sum_{i=13}^{16} \overline{D}_i = -0{,}87$; Verfügbarkeitsrisiken: $\sum_{i=17}^{22} \overline{D}_i = -0{,}86$; Vertraulichkeitsrisiken: $\sum_{i=23}^{26} \overline{D}_i = -0{,}85$; Zurechenbarkeitsrisiken: $\sum_{i=27}^{31} \overline{D}_i = -0{,}81$).

Eine differenzierte Betrachtung der Risikobewertungen der einzelnen ITSR verdeutlicht teilweise erhebliche Unterschiede zwischen den Abweichungen der jeweiligen Mittelwerte bzw. der relativen Höhe der Unterschätzung, die bereits erste Rückschlüsse auf die Ursachen des UO ermöglichen. So unterscheidet sich bspw. das IT Sicherheitsrisiko mit der höchsten Risikoverzerrung („Unzureichende Wartung“ (#1): $\overline{D}_1 = -1{,}42$; $t(46) = -5{,}46$; $ps < 0{,}001$) zu dem mit der geringsten Differenz („Identitätsdiebstahl“ (#31): $\overline{D}_{31} = -0{,}46$; $t(46) = -3{,}11$; $ps < 0{,}01$) durch die Kontrollmöglichkeiten seitens des Anbieters. Der Anbieter kann im Allgemeinen leichter die Wartung seiner CC Dienste kontrollieren als z. B. den Diebstahl der Anmeldedaten der Nutzer, da dieses Risiko zum großen Teil auch vom Verhalten der Kunden abhängig ist. Analog hat ein Anbieter bspw. direkten Einfluss auf die Bereitstellung der CC Angebote („Einstellung des Angebots“ (#2): $\overline{D}_{17} = -1{,}33$; $t(46) = -5{,}13$; $ps < 0{,}01$), aber weniger Kontrolle bzgl. einem möglichen Versagen interner IT Systeme („Nichtverfügbarkeit interner Systeme“ (#30): $\overline{D}_{22} = -0{,}51$; $t(46) = -2{,}26$; $ps < 0{,}01$). Die Ergebnisse weisen auf eine Bestätigung der Theorie hin, wonach die wahrgenommene Kontrolle [12] über ein negatives Ereignis bzw. ITSR signifikanten Einfluss auf die Höhe des UO und somit dem Grad der Unterschätzung eines Risikos haben [10], [26]. Forschungsfrage 3 kann als empirisch bestätigt betrachtet werden, da die Einzelrisiken nicht den gleichen Grad an UO aufweisen und sich hinsichtlich ihrer Charakteristika unterscheiden [4].

Tabelle 3. UO der Anbieter in den (Einzel-) PITSR von CC (N=47)

#	IT Sicherheitsrisiko[a]	D[b]	SD[c]
1	[1] Unzureichende Wartung (Wart.)	-1,42***	1,79
2	[17] Einstellung des Angebots (Verf..)	-1,33***	1,20
3	[2] Zeitlich ungünstige Updates (Wart.)	-1,25***	1,22
4	[13] Minderleistung nach Vertragsabschluss (Leist.)	-1,17***	1,24
5	[27] Aktionen unzureichend protokolliert (Zurech.)	-1,13***	1,26
6	[8] Datenmanipulation während Übertragung (Int.)	-1,08**	1,53
7	[3] Fehlender technologischer Fortschritt (Wart.)	-1,08***	1,35
8	[18] Verlust von Zugriff auf Daten (Verf.)	-1,04***	1,12
9	[14] Unzureichende Skalierbarkeit (Leist.)	-1,04**	1,43
10	[9] Datenmanipulation beim Anbieter (Int.)	-1,00***	1,14
11	[10] Ändern von Daten auf internen Systemen (Int.)	-1,00***	1,35
12	[23] Abhören der Übertragung (Vert.)	-1,00**	1,38
13	[24] Datenweitergabe durch Anbieter (Vert.)	-1,00**	1,50
14	[19] Datenverluste beim Anbieter (Verf.)	-0,96**	1,40
15	[28] Unzureichende Trennung von Kunden (Zurech.)	-0,96**	1,33
16	[4] Inkompatible Geschäftsprozesse oder Software (Wart.)	-0,92**	1,50
17	[5] Unzureichender Datenimport (Wart.)	-0,92***	1,21
18	[25] Einsehen von Daten beim Anbieter (Vert.)	-0,88**	1,33
19	[6] Unzureichende Anpassbarkeit (Wart.)	-0,83*	1,58
20	[29] Zugriff ohne Autorisation (Zurech.)	-0,83***	1,09
21	[7] Proprietäre Technologien (Wart.)	-0,75*	1,48
22	[11] Datenveränderung während Übertragung (Int.)	-0,75**	1,03
23	[20] Ungewollte Ausfälle (Verf.)	-0,71**	1,04
24	[21] Angriffe auf Verfügbarkeit (Verf.)	-0,71**	1,04
25	[15] Geschwindigkeitsprobleme (Leist.)	-0,71**	1,20
26	[30] Nichtzurechenbarkeit bei internen Aktionen (Zurech.)	-0,67*	1,31
27	[12] Datenveränderung beim Anbieter (Int.)	-0,63**	0,97
28	[16] Geschwindigkeitsprobleme interner Systeme (Leist.)	-0,58*	1,14
29	[26] Einsehen von Daten auf internen Systemen (Vert.)	-0,54*	1,18
30	[22] Nichtverfügbarkeit interner Systeme (Verf.)	-0,51**	0,78
31	[31] Identitätsdiebstahl (Zurech.)	-0,46**	0,72

[a] ITSR: [Elementnr.] Name (Risikofacette)

[b] Differenz (D) der Mittelwerte für die einzelnen ITSR gemessen auf einer 7er Skala mit 1 (überhaupt nicht riskant) und 7 (überaus riskant), wobei eine signifikant negative Differenz eine systematische Unterschätzung des jeweiligen IT Sicherheitsrisikos verdeutlicht. Signifikanzen mit zweiseitigem t-Test: *** $ps < 0{,}001$; ** $ps < 0{,}01$; * $ps < 0{,}05$.

[c] Standardabweichung (SD)

4 Zusammenfassung der Ergebnisse und Ausblick

Auf Grundlage der Theorie des UO konnten wir empirisch eine systematische Verzerrung in Form einer Unterschätzung der ITSR seitens der CC Anbieter im deutschen Markt nachweisen. Darüber hinaus konnten wir zeigen, dass die resultierende Unterschätzung der ITSR signifikant negative Auswirkungen auf die Auseinandersetzung der Entscheidungsträger mit IT Sicherheit bzw. die „*Awareness*“ für diese Risiken hat. Die Betrachtung der 31 Einzelrisiken des CC ermöglichte uns in diesem Zusammenhang sowohl die Risikowahrnehmung der Entscheider vollständig hinsichtlich des Vorhandenseins von UO zu analysieren als auch erste Rückschlüsse auf relevante Einflussfaktoren in unserem Forschungsgebiet zu ziehen. In allen Facetten des ITSRs konnte dabei eine systematische Unterschätzung der Risiken durch die Verantwortlichen gezeigt werden, wobei in Abhängigkeit der Charakteristika eines ITSR, bspw. der Kontrollierbarkeit durch den Anbieter, der Grad des UO variiert.

Insbesondere im Hinblick auf die Einflussfaktoren des UO im CC ist weitere Forschung erforderlich, um die Auswirkungen der bekannten Einflussgrößen im Bereich der IT zu analysieren und ggf. spezifische Faktoren zu identifizieren [29]. Darüber hinaus sollte die Untersuchung auf internationaler Ebene fortgeführt werden, um den Einfluss kultureller Faktoren auf die subjektive Risikowahrnehmung zu untersuchen.

Während die systematische Verzerrung der Risikowahrnehmung seitens der Anbieter im deutschen CC Markt im Durchschnitt eindeutig nachgewiesen werden konnte, unterliegt die Analyse einzelner Anbieter methodischen Einschränkungen. Obgleich die Methode nach Weinstein (1980) [11] eine gute Approximation des individuellen UO liefert, ist die Quantifizierung des tatsächlichen Risikos, dem eine Person ausgesetzt ist, notwendig, um Messfehler und falsche Klassifizierungen vollständig ausschließen zu können.

Nach unserem Kenntnisstand haben wir mit der vorliegenden Studie erstmals die Theorie des UO auf ein ITO Konzept übertragen, wobei wir dieses vollständig hinsichtlich Verzerrungen in der Risikobewertung untersuchen konnten. Vor dem Hintergrund der Bedeutung der Risikowahrnehmung bzw. der „*Awareness*“ der Entscheidungsträger für die Umsetzung möglicher IT Sicherheitsmaßnahmen können die Ergebnisse wichtige Implikationen für zukünftige IT Sicherheitsforschungen und das Risikomanagement liefern. Das Verständnis der kognitiven Prozesse ermöglicht außerdem auch Anbietern und Nutzern gezielt Strategien zu entwickeln, um Verzerrungen in der Risikowahrnehmung zu adressieren und auf diese Weise langfristig sowohl die IT Sicherheit als auch den finanziellen Aufwand zu optimieren. Der Anwendungsfall des CC verdeutlicht dabei die zunehmende Bedeutung der IT Sicherheit für ITO Beziehungen [4], so dass in Zukunft vermehrt ganzheitliche Ansätze des IT Sicherheits- und Risikomanagements unter Berücksichtigung subjektiver Risikowahrnehmung sowie unbewussten „kognitiven Fehlleistungen“ aller Beteiligten erforderlich werden.

Literatur

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology (2011)
2. Vaquero, L.M., Rodero-Merino, L., Morán, D.: Locking the sky: a survey on IaaS cloud security. Computing 91 (1), 93-118 (2011)
3. Pring, B.: Cloud Computing: The Next Generation of Outsourcing. Gartner Group (2010)
4. Ackermann, T., Widjaja, T., Benlian, A., Buxmann, P.: Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development. In: Proceedings of the 33rd International Conference on Information Systems, Orlando (2012)
5. Hange, M.: Security Recommendations for Cloud Computing Providers. Federal Office for Information Security (2011)
6. Gigerenzer, G.: Dread Risk, September 11, and Fatal Traffic Accidents. Psychological Science 15 (4), 286-287 (2004)
7. Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., Wei, K.-K.: An integrative study of information systems security effectiveness. Int. Journal of Information Management 23, 139-154 (2003)
8. Klein, W.M.P.: Self-Prescriptive, Perceived, and Actual Attention to Comparative Risk Information. Psychology & Health 18, 625-643 (2003)
9. Festinger, L.: A Theory of Social Comparison Processes. Human Relations 7, 117-140 (1954)
10. Weinstein, N.D., Klein, W.M.: Unrealistic optimism: Present and future. Journal of Social and Clinical Psychology 15, 1-8 (1996)
11. Weinstein, N.D.: Unrealistic optimism about future life events. Journal of Personality and Social Psychology 39, 806-820 (1980)
12. McKenna, F.P.: It won't happen to me: Unrealistic optimism or illusion of control?. British Journal of Psychology 84, 39-50 (1993)
13. Perloff, L.S., Fetzer, B.K.: Self-Other Judgments and Perceived Vulnerability to Victimization. Journal of Personality and Social Psychology 50, 502-510 (1986)
14. Adams, J.: Cars, Cholera, and Cows: The Management of Risk and Uncertainty. Policy Analysis 335 (1999)
15. Helweg-Larsen, M., Shepperd, J.A.: Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature. Personality and Social Psychology Review 5, 74-95 (2001)
16. McKenna, F.P., Warburton, D.M., Winwood, M.: Exploring the limits of optimism: The case of smokers' decision making. British Journal of Psychology 84, 389-394 (1993)
17. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Computers & Security 25 (4), 289-296 (2006)
18. Cunningham, S.M.: The major dimensions of perceived risk. In: Cox, D.F.: Risk taking and information handling in consumer behavior. Harvard University Press (1967)
19. Quinn, J., Hilmer, F.: Strategic outsourcing. Sloan Management Review 35, 43-55 (1994)
20. Earl, M.J.: The risks of outsourcing IT. Sloan Management Review 37, 26-32 (1996)
21. Benlian, A., Hess, T.: Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems 52 (1), 232-246 (2011)
22. Ackermann, T., Miede, A., Buxmann, P., Steinmetz, R.: Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification. In: Proceedings of the 19th European Conference on Information Systems, Paper 240. AIS (2011)
23. Brown, J.D., Collins, R.L., Schmidt, G.W.: Self-Esteem and Direct versus Indirect Forms of Self-Enhancement. Journal of Personality and Social Psychology 55, 445-453 (1988)

24. Taylor, S.E., Brown, J.D.: Illusion and Well-Being: A Social Psychological Perspective on Mental Health. Psychological Bulletin 103, 193-210 (1988)
25. Campbell, J., Greenauer, N., Macaluso, K., End, C.: Unrealistic optimism in internet events. Computers in Human Behavior 23, 1273-1284 (2007)
26. Rhee, H.-S., Ryu, Y.U., Kim, C.-T.: Unrealistic optimism on information security management. Computers & Security 31, 221-232 (2012)
27. Rothman, A.J., Klein, W.M., Weinstein, N.D.: Absolute and Relative Biases in Estimations of Personal Risk. Journal of Applied Social Psychology 26, 1213-1236 (1996)
28. Wood, J.V.: Theory and Research Concerning Social Comparisons of Personal Attributes. Psychological Bulletin 106, 231-248 (1989)
29. Shepperd, J.A., Carroll, P., Grace, J., Terry, M.: Exploring the Causes of Comparative Optimism. Psychologica Belgica 42, 65-98 (2002)
30. Wills, T.A.: Downward comparison principles in social psychology. Psychological Bulletin 90, 245-271 (1981)
31. Klein, W.M., Weinstein, N.D.: Social comparison and unrealistic optimism about personal risk. In: Buunk, B.P., Gibbons, F.X. (eds.): Health, coping, and well-being: Perspectives from social comparison theory. Lawrence Erlbaum Associates Publishers, Mahwah, NJ (1997)
32. Bolton, R.N.: Pretesting Questionnaires: Content Analyses of Respondents' Concurrent Verbal Protocols. Marketing Science 12, 280-303 (1993)
33. Velten, C., Janata, S.: Cloud Vendor Benchmark 2011. Experton Group (2011)
34. Poppo, L., Zenger, T.: Do formal contracts and relational governance function as substitutes or complements?. Strategic Management Journal 23, 707-725 (2002)
35. Heberlein, T., Baumgartner, R.: Factors affecting response rates to mailed questionnaires: A quantitative analysis of the published literature. American Sociological Review 43, 447-462 (1978)
36. Armstrong, J.S., Overton, T.S.: Estimating Nonresponse Bias in Mail Surveys. Journal of Marketing Research 14, 396-402 (1977)
37. Featherman, M.S., Pavlou, P.A.: Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum.-Comput. Stud. 59, 451-474 (2003)
38. Karakayali, N.: Social Distance and Affective Orientations. Sociological Forum 24, 538-562 (2009)
39. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8, 31-41 (2000)