Georg-August-Universität
Göttingen

Wirtschaftswissenschaftliche Fakultät
Professur für Informationsmanagement
Prof. Dr. Lutz. M. Kolbe

Diplomarbeit

Entwicklung einer Methode zur Bewertung der Informationssicherheit im Cloud Computing

18. Oktober 2011

Atman
Sense
20422852

Inhaltsverzeichnis

Abkürzungsverzeichnis

BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
GoF	Goodness of Fit
IaaS	Infrastructure as a Service
ISM	Informationssicherheitsmanagement
ISMS	Informationssicherheitsmanagementsystem
PaaS	Platform as a Service
PCA	Principal Components Analysis
PDCA	Plan-Do-Check-Act
PLS	Partial Least Squares
PLSPM	Partial Least Squares Path Modeling
SaaS	Software as a Service
SEM	Structural Equation Modeling
SLA	Service Level Agreement
VPN	Virtual Private Network

Abbildungsverzeichnis

1 Einleitung

Cloud-Computing war das „Top-Thema“ der CeBIT 2011 (vgl. Deutsche Messe AG 2011, 1) und ist laut Umfrage des Branchenverbands BITKOM (2011, 1) wichtigster IT-Trend 2011. Die Nutzung von Cloud-Computing kann Vorteile bieten, birgt aber auch Gefahren. In dieser Arbeit wird ein Ansatz entwickelt, der helfen soll auf die neuen Bedrohungen angemessen zu reagieren.

Bisher betreiben viele Unternehmen ihre IT selbst oder lassen sie durch einen Outsourcingpartner bereitstellen. Outsourcing bringt unter anderem Vorteile indem Fixkosten, die durch den Betrieb eines eigenes Rechenzentrum entstünden, in variable Kosten umgewandelt werden(vgl. Amberg/Wiener 2006, 41). Der Outsourcing-Ansatz lässt sich durch tiefergehende Modularisierung weiter optimieren. Beim Cloud-Computing werden virtuelle Rechen- und Speichereinheiten bzw. Dienste und Anwendungen nachfragegerecht dynamisch bereitgestellt (vgl. Baun et al. 2010, 2). Dadurch werden stets nur so viele Ressourcen gebunden wie auch benötigt werden. Unternehmen müssen nicht mehr dedizierte Server für bestimmte Funktionen bereitstellen, sondern nutzen für ihre Dienste beliebig skalierbare Einheiten über definierte Schnittstellen. Auf der Seite des Cloud-Dienstleisters sind diese virtuellen Einheiten ebenfalls von Vorteil, da sie auf jeder physischen Einheit der Cloud betrieben und auch im laufenden Betrieb verschoben werden können (vgl. Baun et al. 2010, 9). Vorhandene Ressourcen können auf diese Weise optimal ausgelastet werden, während nicht genutzte physische Einheiten deaktiviert werden. Dadurch wird eine Effizienzsteigerung erreicht (vgl. Pichler 2009, 7; Baun et al. 2010, 8).

Für den Dienstleistungsnehmer verspricht Cloud-Computing sowohl Zeit- und Kosteneinsparungen als auch die Reduktion von Risiken (vgl. Baun et al. 2010, 87). Während es in einer traditionellen IT-Abteilung Wochen dauern kann bis neue Hardware angeschafft und eingerichtet ist, sind hingegen beim Cloud-Computing Ressourcen in der Regel innerhalb von Minuten bereitgestellt (vgl. Baun et al. 2010, 90). Zudem müssen keine eigenen Rechenzentren betrieben werden, die möglicherweise bedingt durch seltene Lastspitzen überdimensioniert sind und dadurch Kapital binden (vgl. Armbrust et al. 2009, 2; Foster et al. 2008, 65; Baun et al. 2010, 8).

Das Anwendungsgebiet von Cloud-Computing erstreckt sich über die Bandbreite von Infrastruktur über Plattformen bis zu Anwendungen (vgl. Stanoevska-Slabeva/Wozniak 2010, 51f.). Werden Plattformen oder Anwendungen von einem Cloud-Dienstleister bezogen, ergeben sich weitere Vorteile in Form von entfallendem Lizenzmanagement und reduzierten Administrationsaufgaben. Die Unternehmen können sich auf ihre Kernkompetenzen und neuen Geschäftsideen konzentrieren und dabei die Kosten und Managementaufgaben der nötigen IT minimieren und transparent halten.

Eine zentrale Frage ist die Sicherheit im Cloud-Computing. Im Endnutzerbereich berei-

tet diese, zumindest für ausländische Anbieter, weniger Probleme. Praktisch jeder benutzt täglich Dienste aus der Cloud, wie z.B. „Google Maps“ oder Microsofts „Office 365“, aber auch die großen E-Mail-Anbieter arbeiten in der Regel mit der Cloud. In Deutschland hat es Cloud-Computing aus datenschutzrechtlichen Gründen schwer. Personenbezogene Daten dürfen nur mit Zustimmung der Betroffenen an einen externen Dienstleister übergeben werden (vgl. BITKOM 2009, 51ff.). Es gibt aber auch generelle Sicherheitsbedenken gegenüber Cloud-Computing (vgl. Herrmann 2010, 1). Wenn hohe Sicherheitsanforderungen nötig sind, besteht allerdings die Möglichkeit eine Cloud innerhalb der Organisation zu betreiben; dies nennt sich „Private Cloud“. Dadurch können zwar Effizienzgewinne durch dynamische Skalierung ausgenutzt werden, allerdings müssen die restlichen Lasten wie Hardware- und Lizenzmanagement wieder selbst bewältigt werden. Ein Mittelweg ist das Betreiben der IT durch einen Outsourcingpartner, wobei die IT des Auftraggebers technisch abgeschottet von fremden Teilen ist. Wenn Lastspitzen von der „Private Cloud“ nicht mehr abgefangen werden können, müssen Kapazitäten aus der „Public Cloud“ hinzugenommen werden (vgl. BITKOM 2009, 43). Es entsteht eine „Hybrid Cloud“. Spätestens an diesem Punkt kommt die Frage auf, ob durch den parallelen Betrieb fremder Inhalte Datenschutzanforderungen eingehalten werden können (vgl. BITKOM 2009, 11).

Technisch gesehen ist es fast unerheblich, ob sich die Cloud in geographischer Nähe befindet oder im Ausland bzw. auf anderen Kontinenten. Die Unabhängigkeit verspricht weitere Einsparmöglichkeiten, allerdings auch neue Gefahren. Die Integrität der Anbieter und die Sicherheit der Daten können bei großer geographischer und politischer Entfernung schlechter kontrolliert werden. Zwar ist das Lagern von verschlüsselten Daten in der Cloud meist sicherer als unverschlüsseltes Lagern auf lokalen Rechnern (vgl. Baun et al. 2010, 68), wenn allerdings die Verarbeitung von Daten deren Entschlüsselung verlangt, entstehen neue Risiken (vgl. BITKOM 2009, 11).

Die vorliegende Arbeit will klären, welche Gefahren durch Cloud-Computing entstehen und in wie weit bestehende Sicherheitsframeworks auf Cloud-Computing anwendbar sind.

Anfangs wird auf die Grundlagen des Cloud-Computing eingegangen. Es werden verschiedene Einsatzmöglichkeiten und Geschäftsmodelle sowie Vor- und Nachteile vorgestellt. Es folgen Grundlagen der IT-Sicherheit, insbesondere wird auf Fragen und neue Bedrohungen im Zusammenhang mit Cloud-Computing eingegangen. Anschließend werden Sicherheits-Frameworks und „Best Practices“ wie z.B. ISO/IEC 27001 oder ITIL vorgestellt. Diese werden von Standardisierungsorganisationen, privaten Organisationen oder Regierungen herausgegeben. Es wird darauf eingegangen, welche Ziele diese verfolgen und wie sie verwendet werden.

Anschließend wird ein Modell entwickelt, wie die Sicherheit im Cloud-Computing gewährleistet werden kann. Dieses Modell soll die Besonderheiten im Cloud-Computing integrieren und die (geänderten) Zusammenhänge erfassen. Im Anschluss wird eine

empirische Studie vorgestellt, mit der die im Modell erarbeiteten Hypothesen überprüft werden. Durch die Auswertung von Fragebögen soll ermittelt werden welchen Stellenwert IT-Sicherheit im Cloud-Computing in Unternehmen hat und wie dazu IT-Sicherheitsframeworks genutzt werden. Die Auswertung soll zeigen, wie weit deutsche Unternehmen die Chancen des Cloud-Computing nutzen und wie sie mit den neuen Risiken umgehen. Die darauffolgenden Teile der Arbeit orientieren sich an den folgenden Fragestellungen:

1. Welche Methoden zur Bewertung und Gewährleistung der IT-Sicherheit in Bezug auf Cloud-Computing sind im Einsatz?
2. Welche Bedeutung hat Effizienz der Informationssicherheitsmanagements für die Unternehmen und findet ein Controlling der IT-Sicherheit statt?
3. Wie beurteilen die Unternehmen ihre Ansätze hinsichtlich einer allgemeinen Praxistauglichkeit?

Abschließend verdeutlicht das verfeinerte Modell die aktuellen „Best Practices“ in Bezug auf IT-Sicherheit im Cloud-Computing.

2 Grundlagen

Im folgenden Kapitel werden Begriffe definiert und grundlegende Sachverhalte erläutert, die zum Verständnis dieser Arbeit nötig sind.

2.1 Informationssicherheit

Informationssicherheit wird in dieser Arbeit wie folgt verwendet: Sie beschreibt einen Zustand, in dem sich Informationen befinden, wenn sie frei von unvertretbaren Risiken sind (vgl. Krcmar 2010, 567f.). Es geht um Informationen, die von Informationssystemen verarbeitet oder gespeichert werden.

2.1.1 Grundbegriffe

Im folgenden werden die Grundbegriffe der Informationssicherheit vorgestellt und näher erläutert.

Information
Information ist nach Definition von Kuhlen (1995, 35ff.) ein Bestandteil der Komponenten Wissen, Daten und Zeichen. Wissen kann in Information transformiert werden und wird erst kommunizierbar, wenn es eine Repräsentation in einem Zeichensystem gibt. Aus dieser Repräsentation entsteht erst wieder Wissen, wenn jemand versucht die

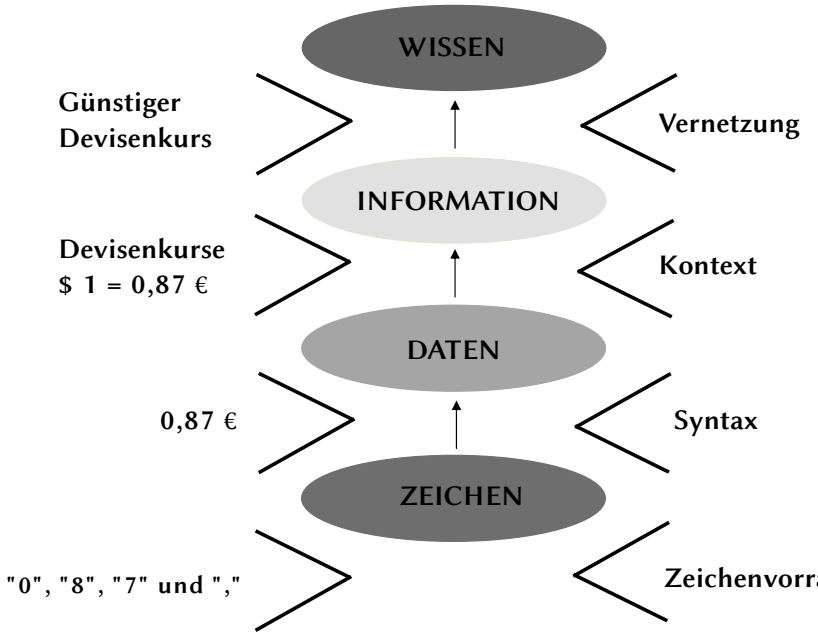


Abbildung 2-1: Zusammenhang zwischen Wissen, Information, Daten und Zeichen (Quellen: vgl. Krcmar 2005, 14; zitiert nach Kolbe 2008, 40)

Daten, die sich aus Zeichen zusammensetzen, zu verstehen. In dieser Arbeit wird beim Informationsbegriff in erster Linie von digitalen Informationen ausgegangen.

Holthaus (2000, 21ff.) definiert die Komponenten, die im Zusammenhang mit Information und Wissen stehen wie folgt:

Wissen umfasst den Bestand an Kenntnissen in einem bestimmten Sachgebiet.

Information ist die Verwendung von Wissen für einen speziellen Zweck, für ein sich dem Individuum stellendes Problem.

Daten sind die Repräsentation von Wissen mit Zeichen aus einem Zeichensatz.

Nachrichten sind Daten, welche von einem Individuum an ein anderes übertragen werden.

Der Zusammenhang zwischen diesen Komponenten ist in Abbildung 2-1 verdeutlicht. In diesem Beispiel ist das „Wissen“ in Form von „Günstiger Devisenkurs“ ausgeprägt. Die dazugehörige Information ist der Devisenkurs an sich, wobei die Daten die strukturierte Darstellung der monetären Größe sind. Diese Daten bestehen aus einem bestimmten Satz an „Zeichen“.

Informationssystem

Ein Informationssystem besteht aus allen Komponenten, die im Zusammenhang mit der Informationsverarbeitung stehen (vgl. Holthaus 2000, 75). Dies sind nach Heinrich (1993, 14) die drei Elemente „Mensch“, „Technik“ und „Aufgabe“ inklusive deren Beziehungen

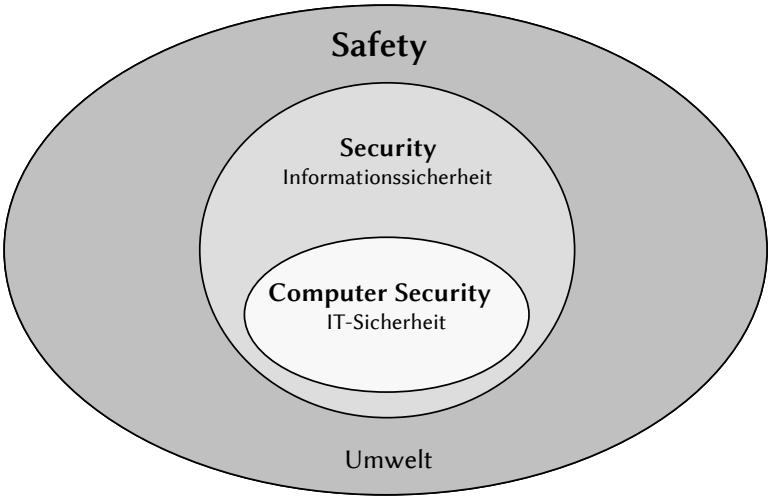


Abbildung 2-2: Zusammenhang zwischen Safety, Security, Informationssicherheit und IT-Sicherheit (Quellen: vgl. Pohl 2004, 679; zitiert nach Klempt et al. 2007, 5)

zueinander. Sie sind voneinander abhängig bzw. greifen ineinander. Im Mittelpunkt steht die Unterstützung bei der Erfüllung betrieblicher Aufgaben. Die Informationsinfrastruktur umfasst „die Einrichtungen, Mittel und Maßnahmen, welche die Voraussetzung für die Produktion von Information und Kommunikation in einem Unternehmen schaffen (z.B. Hardware, Software, Personal)“ (Heinrich 1993, 330).

Sicherheit und Risiko, Security und Safety

Sicherheit bezeichnet „den Zustand des Sicherseins vor Gefahr oder Schaden bzw. einen Zustand, in dem Schutz vor Gefährdungen besteht“ (vgl. Hoppe/Prieß 2003, 23). Im Zustand der Sicherheit sind das Verhalten von Objekten und die damit verbundenen Auswirkungen klar definiert (vgl. Holthaus 2000, 26). Sie entsprechen immer den Erwartungen. Risiko dagegen ist der Zustand, in dem das Verhalten von der Erwartung abweicht. Diese beiden Begriffe sind subjektive Beurteilungen, die nicht beweisbar sind (vgl. Holthaus 2000, 26). So gibt es beispielsweise keine vollständige Sicherheit (vgl. Gronau/Lindemann 2010, 209).

Des Weiteren wird zwischen Security und Safety unterschieden. Security ist der Schutz vor beabsichtigten Angriffen. Safety bezieht sich auf die Gesamtzuverlässigkeit eines Systems, speziell in Bezug auf Ablauf- und Ausfallsicherheit (z.B. redundante Datenhaltung). Safety ist dabei der Oberbegriff, der auch Security mit einbezieht (vgl. Sikora 2003, 1). Dieser Zusammenhang ist in Abbildung 2-2 dargestellt. IT-Sicherheit ist ein Teilgebiet der Informationssicherheit, speziell mit dem Bezug auf IT-Systeme. Der umfassendere Begriff „Informationssicherheit“ bezieht sich allgemein auf Informationen (vgl. BSI 2008a, 8).

2.1.2 Schutzziele

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (2003, 14) nennt drei grundsätzliche Schutzziele für Informationen — Vertraulichkeit, Integrität und Verfügbarkeit — und unter anderem weitere Ziele — Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit. Klempt et al. (2007, 5) definieren diese Ziele wie folgt:

Vertraulichkeit Informationen werden vor unberechtigter Kenntnisnahme geschützt. Das System muss so aufgebaut sein, dass ein Zugriff nur für befugte Personen oder Dienste möglich ist.

Integrität Informationen, Systeme und Netze können nicht unbemerkt verändert werden. Das System muss so beschaffen sein, dass eine Veränderung offensichtlich wird. Die Sicherstellung der Integrität beinhaltet die Komponenten Übereinstimmung, Genauigkeit, Korrektheit und Vollständigkeit.

Verfügbarkeit Informationen, Systeme und Netze müssen verfügbar sein. Das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen ausführen. Zum Schutzziel der Verfügbarkeit werden die Komponenten Fehlertoleranz, Zuverlässigkeit, Robustheit und Wiederherstellbarkeit gezählt.

Verbindlichkeit Die Nachweisbarkeit des Sendens und Empfangens von Informationen in Verbindung mit dem Identitätsnachweis des Kommunikationspartners schafft eine Verbindlichkeit von Informationen, die z.B. für elektronische Vertragsabschlüsse erforderlich ist. Die Verbindlichkeit beinhaltet die Authentizität und die Beherrschbarkeit.

Authentizität Es muss beweisbar sein, dass Informationen von der angegebenen Quelle stammen und deren Identität korrekt ist. Die Echtheit der Identität von Kommunikationspartnern und deren Informationen muss nachweisbar sein.

Zurechenbarkeit Aktionen und Informationen können einer auslösenden Instanz (Personen oder Systeme) zugerechnet werden. Die Zurechenbarkeit folgt ggf. aus der Authentizität.

Rechtssicherheit und Revisionsfähigkeit Alle für den Rechtsverkehr in Systemen und Netzen verwendeten Informationen und Vorgänge gegenüber Dritten sind nachweisbar.

2.1.3 Bedrohungsszenarien und Angriffspunkte

Bedrohungen bestehen aus verschiedenen Komponenten (vgl. Holthaus 2000, 38-43). Diese sind

ein betroffenes Objekt („was“) Bezieht sich auf ein Objekt innerhalb eines Informationssystems. Dies können technische oder personelle Komponenten sein.

eine Aktivität („wie“) Beschreibt, welche Handlungen vorgenommen wurden, die zu einem Vorfall geführt haben. Im Fall von Böswilligkeit ist die Ausnutzung von Schwachstellen gemeint.

ein Urheber der Bedrohung („wer“) Die Urheberschaft kann in „Umwelt“ oder „Personen“ unterteilt werden. Umweltereignisse können Höhere Gewalt oder Infrastrukturversagen sein. Personen als Urheber können interne und externe Personen aber auch Mittler sein.

eine Motivation („warum“) Ist nur im Fall von Personen relevant. Sie teilt sich in beabsichtigte und unbeabsichtigte Motivation.

Wird die Betrachtung des Risikos mit einbezogen, kommen folgende Komponenten hinzu:

Häufigkeit („wie oft“) Betrachtet die Häufigkeit des Auftretens von Bedrohungen. Die Konzentration auf bestimmten Zeiten (z.B. nachts) oder die Abhängigkeit von Ereignissen (z.B. Veröffentlichung eines neuen Produkts oder Stimmungslage der Bevölkerung) ist ebenfalls relevant. Weiterhin wird ein stoßweises bzw. punktuelles Auftreten betrachtet.

Höhe des entstehenden Schadens („wieviel“) Betrachtet die qualitative und quantitative Ermittlung des Schadens. Quantitativ lassen sich Schäden mit betriebswirtschaftlichen Bewertungsgrundsätzen bestimmten. Qualitative Schäden sind immaterielle Schäden wie z.B. Imageverlust.

2.1.4 Maßnahmen zur Durchsetzung von Informationssicherheit

Im folgenden Abschnitt wird Bezug auf technische und organisatorische Sicherheitsmaßnahmen genommen, die insbesondere im Cloud-Computing eine wichtige Rolle spielen.

Organisatorische Maßnahmen

Audits Audits sind Untersuchungsverfahren, die die Einhaltung der operationellen, finanziellen und vom Management vorgegebenen Regeln überprüfen (vgl. Peltier 2004, 9). Auch die Effektivität der organisatorischen Einheiten wird dabei überprüft. Ein Informationssystem-Auditor prüft die Einhaltung von Sicherheitsrichtlinien, Prozeduren, Standards, Architekturen und anderen Anforderungen. Er berichtet dem Management, ob die Sicherheitsvorgaben umgesetzt und effektiv sind (vgl.

Fitzgerald 2007, 31). Im Rahmen solcher Audits werden beispielsweise Gesetzesanpassungen bemerkt, die etwa eine Anpassung der vereinbarten Leistungen eines Dienstleistungsverhältnisses erforderlich machen. Die von beiden Seiten getroffenen Annahmen und daraus abgeleiteten Leistungen können so aktuell gehalten werden. Dienstleister haben oft Probleme die Sicherheit ihrer Systeme zu beweisen und zu demonstrieren (vgl. Misrahi 2007, 126). Externe Audits können diese Funktion erfüllen. Solche Audits können auch anhand von Standards durchgeführt werden. Bekannte Beispiele sind der „Statement on Auditing Standards No. 70“ (SAS 70) des Wirtschaftsprüferverbands „American Institute of Certified Public Accountants“ und der britische Standard BS 7799-2.

Service Level Agreements Ein SLA ist eine ausgehandelte Vereinbarung zwischen einem IT-Dienstleister und einem Kunden, bei der die Verantwortlichkeiten jeder Partei bzgl. der Diensterbringung geregelt sind (vgl. Long 2008, 19). SLAs sollten alle wichtigen Aspekte zum Betrieb der Services umfassen (vgl. Schürmann 2010, 68). Diese sind u.a. Verfügbarkeit, Qualität, Preise und die in diesem Abschnitt genannten Aspekte. Dazu gehören auch Vertragslaufzeiten und Vereinbarungen wie bei Übernahme oder Liquidierung des Anbieters zu verfahren ist.

Reporting Ein zügiges Reporting von Sicherheitsvorfällen hilft, rechtzeitig Maßnahmen zu ergreifen und Schäden zu begrenzen (vgl. BSI 2009, 80). Es ist Pflicht laut § 42a Bundesdatenschutzgesetz die Betroffenen eines Vorfalls zu informieren.

physikalischer Aufbewahrungsort Der physikalische Aufbewahrungsort von Daten spielt bei solchen Daten eine Rolle, für die gesetzliche Bestimmungen in dieser Hinsicht gelten. Dies sind insbesondere personenbezogene Daten. Im nichteuropäischen Ausland ist im Fall von externen IT-Dienstleistern, was bei Cloud-Computing i.d.R. gegeben ist, die Kontrolle schwierig. Diese Daten dürfen laut § 4b Bundesdatenschutzgesetz den Bereich der EU bzw. des Europäischen Wirtschaftsraumes (EWR) i.d.R. nicht verlassen, wenn im Zielland kein angemessenes Datenschutzniveau herrscht (vgl. BITKOM 2008, 11). Ausnahmen gelten u.a. dann, wenn sich Anbieter aus den USA der „safe harbor“-Regelung unterworfen haben und sich damit verpflichten strengere Datenschutzbestimmungen einzuhalten (vgl. BITKOM 2008, 11).

Transparenz des Anbieters Zum einen erlaubt Transparenz zu sehen was und wie produziert wird (vgl. Hofstede 2003, 18). Zum anderen beinhaltet sie Aspekte wie Orientierung, Partizipierung und Kommunikation (vgl. Frentrup/Theuvsen 2006, 66). Transparenz hilft, schneller Vertrauen aufzubauen (vgl. BITKOM 2010, 27). In Bezug auf Cloud-Computing ergibt sich das Problem, dass eine Prüfung auf vertragsgemäße Verarbeitung der Daten vor Ort oft nicht möglich ist, da Daten und

Anwendungen zeitgleich über eine Vielzahl von geografisch getrennten Standorten verteilt sein können (vgl. Budszus et al. 2011, 20).

Zertifizierungen Die Einhaltung von Richtlinien und Standards kann von externen Stellen zertifiziert werden. Zertifikate eignen sich dazu, verschiedenen Interessengruppen zu zeigen, dass die angebotenen Services bestimmte Eigenschaften haben oder generell bestimmte Anforderungen erfüllen (vgl. Amberg et al. 2009, 37). Zertifizierungen können entweder gesetzlich vorgeschrieben sein oder als vertrauensbildende Maßnahme dienen (vgl. Schürmann 2010, 62f.).

Mitarbeiterschulung/-sensibilisierung Der sensible Umgang mit unternehmenskritischen Informationen ist wichtig (vgl. Schürmann 2010, 67). Ausgereifte Sicherheitsrichtlinien sind wertlos, wenn diese von den eigenen Mitarbeitern nicht beachtet werden. Es sollte eine risikobewusste Unternehmenskultur geschaffen werden, die drohende Gefahren für alle Mitarbeiter transparent macht (vgl. Schürmann 2010, 67).

Technische Maßnahmen

Firewalls Firewalls dienen dazu eine Zugriffspolitik zwischen zwei Netzwerken durchzusetzen (vgl. Pandya 2009, 158). In der Regel soll das Intranet vor nichtauthorisiertem Zugriff aus dem Internet geschützt werden. Oft wird der zentrale Virenschutz zu den Leistungen eines Firewall-Systems gerechnet (vgl. BITKOM 2003, 45). Jegliche Zugriffe sollten zusätzlich protokolliert werden.

Identitätsmanagement Im Bereich des Identitätsmanagements versteht man unter Identitäten Personen oder Dinge (vgl. Cameron 2005, 4) in einer Organisation oder einem anderem Gebilde, die einer eindeutigen Identifikation bedürfen. Das umfasst grundsätzlich alle Mitarbeiter und Kunden eines Unternehmens. Aber auch Geräte wie Drucker können hier eine Identität haben. Das Identitätsmanagement ist dabei die Verwaltungseinheit aller Identitäten. Ziel des Identitätsmanagements ist es, Datenredundanz zu vermeiden und die Möglichkeit zu schaffen, Daten nur einmal eingeben zu müssen. Die Reduzierung auf eine einzige Authentifizierungsschnittstelle kann eine Erhöhung der Sicherheit bedeuten, da nur eine Schnittstelle gewartet werden muss. Dadurch lässt sich zusätzlich eine einheitliche Authentifizierungsstruktur durchsetzen. Ein weiterer Grund für das Identitätsmanagement ist der Datenschutz. Durch eine einheitliche, sorgfältig geführte Verwaltung werden Parallelsysteme vermieden, die unter Umständen schlecht gewartet werden. Laut Williamson et al. (2009) ist das Identitätsmanagement ein wichtiger Bestandteil der Sicherheitsinfrastruktur eines Unternehmens. Das Identitätsmanagement soll die Sicherheit erhöhen und eine Vereinfachung ermöglichen.

Verschlüsselung Im Internet werden Daten oft über das unverschlüsselte Protokoll HTTP übertragen. Die Daten werden in diesem Fall im Klartext übertragen und können von jedem Transportknoten eingesehen werden. Da gerade im Cloud-Computing Browser und damit HTTP zum Einsatz kommen, sollte zur Wahrung der Vertraulichkeit auf eine verschlüsselte Übertragung zwischen Browser und Webserver geachtet werden (vgl. Schürmann 2010, 61). Als Standard hat sich hier die HTTP-Erweiterung HTTPS etabliert, welche TLS als Verschlüsselungsprotokoll einsetzt. Hierbei wird ein sicherer Kanal zwischen den kommunizierenden Objekten aufgebaut, über den die Daten anschließend verschlüsselt übertragen werden (vgl. Eckert 2008, 729).

Virtual Private Networks Mit Hilfe von VPNs werden entfernte Komponenten über ein öffentliches Netz in das interne Netzwerk eingebunden (vgl. Eckert 2008, 697). Meist werden zwei von einander getrennte private Netzwerke über ein öffentliches Netz so verbunden, dass sie wie eines erscheinen.

physikalische Sicherheit Diese umfasst die physische Zutrittskontrolle, den Einbruchschutz, bauliche Schutzmaßnahmen vor Wasser, Feuer und Blitzschlag (vgl. Schürmann 2010, 64). Redundante Datenleitungen, Stromversorgungen und Klimatisierungen fallen auch darunter.

mehrstufige Authentifizierungen (oder Mehrfaktorauthentifizierungen) Authentifizierung, also die Zugangskontrolle, ist ein Bestandteil des Identitätsmanagements. Eine Authentifzierung kann durch bestimmte Faktoren erfolgen. Über etwas, das nur die zu authentifzierende Identität hat, etwas, das nur die zu authentifzierende Identität weiß, und etwas, das die Identität ist (vgl. Windley 2005, 51). Im nicht-digitalen Umfeld kann dies z.B. ein Schlüssel sein. Im digitalen Umfeld müssen den nicht-digitalen entsprechende, digitale Faktoren gewählt werden, wie z.B. Schlüsselkarten oder Passwörter. Die Sicherheit kann durch Kombination mehrerer Identifikationsfaktoren erhöht werden (vgl. Eckert 2008, 431).

Klassifikation von Daten Görtz/Stolp (1999, 25) empfehlen eine Einteilung von Informationen in verschiedene Kategorien. Diese könnten beispielsweise „öffentliche Daten“, „unternehmensinterne Daten (nur für den Dienstgebrauch)“ und „vertrauliche Daten“ sein. Eine tiefergehende Klassifizierung kann erreicht werden, wenn die Festlegung für verschiedene Sicherheitsziele (z.B. Vertraulichkeit, Integrität, Nachvollziehbarkeit, Verfügbarkeit) in Stufen erfolgt. Daraus können die jeweiligen sicherheitstechnischen Anforderungen abgeleitet werden. Durch diese Bestandsaufnahme kann festgestellt werden, was wie geschützt werden muss.

Browsersicherheit Durch die Bedeutung des Browsers im Cloud-Computing (vgl. Schürmann 2010, 65) kommt der Browsersicherheit eine besondere Bedeutung zu.

Es sollte darauf geachtet werden, dass die jeweils neuesten Versionen installiert sind und insbesondere sollten die Gefahren, die von Erweiterungen wie „Flash Player“ von Adobe und „Java“ von Oracle ausgehen, berücksichtigt werden.

Backups Es sollten regelmäßige Backups außerhalb des Clouddienstleisters angefertigt werden (vgl. Schürmann 2010, 66). Je generischer und unabhängiger das Datenformat des Backups ist, desto einfacher gestaltet sich die Wiederaufnahme des Betriebs nach einem Schadensfall. Einfache Image-Kopien von virtuellen Maschinen sind daher meist nicht ausreichend (vgl. Schürmann 2010, 67)

Alarm-/Eskalationssystem Dieses System regelt die Verfahren, die ablaufen, wenn ein Sicherheitsvorfall eingetreten ist. Die IT-Grundschutzkataloge empfehlen, dass eine „Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen“ und eine „Festlegung von Meldewegen für Sicherheitsvorfälle“ erfolgen sollte (vgl. BSI 2009, 3888). Nach einer anschließenden Untersuchung und Bewertung eines Sicherheitsvorfalls werden weitere Maßnahmen in Gang gesetzt. Dies sollte in einer Eskalationsstrategie festgelegt werden, um eine weitere Bearbeitung zu gewährleisten (vgl. BSI 2009, 3888). Dies meint beispielsweise die Festlegung, wer bei welcher Art von Vorfall unterrichtet werden muss.

Intrusion Detection/Prevention Ein „Intrusion Detection System“ überwacht Netzwerkverkehr oder Systemprotokolle (Logs) auf Hinweise für eine Verletzung der Sicherheitspolitik (vgl. Krutz/Vines 2010, 236). Intrusion meint den Versuch oder die Vollendung des nichtauthorisierten Zugangs zu einem IT-System (vgl. Deograt-Lumy/Naldo 2007, 993). Ein solches System kann Einbrüche erkennen, die durch eine Firewall hinweg im Unternehmensnetzwerk erfolgt sind. Die Umsetzung erfolgt meist durch die Erkennung von statistisch ungewöhnlichem Verhalten oder durch Mustererkennung (vgl. Krutz/Vines 2010, 237). Ein „Intrusion Prevention System“ kann autonome Entscheidungen fällen wie bei einem Angriff zu verfahren ist (vgl. West 2009, 47). Dies kann beispielsweise die automatische Aussortierung von Netzwerkpaketen eines Angreifers sein.

Elektronische Signaturen Elektronische Signaturen (auch Digitale Signaturen) stellen in Informationssystemen sicher, dass Daten nicht unbefugt verändert werden können (vgl. BITKOM 2003, 43). Sie beweisen, dass die Daten authentisch und integer und somit verbindlich sind. Damit können beispielsweise Verträge, die ansonsten der Schriftform bedürfen, digital angefertigt und signiert werden. Diese Verträge sind, wenn entsprechende Gesetzesanforderungen eingehalten werden, genauso rechtskräftig, wie der entsprechende Vertrag auf Papier (vgl. BITKOM 2003, 43).

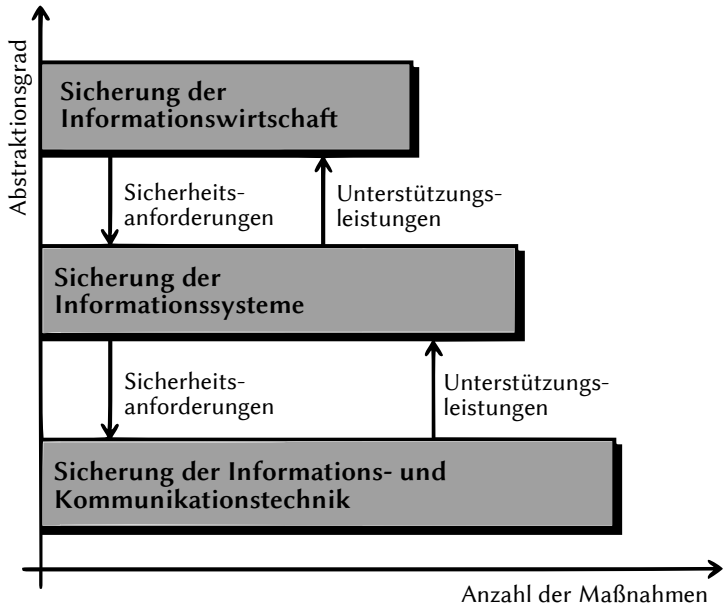


Abbildung 2-3: ISM-Top-Down-Ansatz (Quelle: in Anlehnung an Krcmar 2010, 564)

Compliance Compliance bedeutet „Einhaltung“ oder „Befolgung“. Bezogen auf regulatorische Vorgaben, etwa gesetzliche Regelungen, Richtlinien und Standards, ist damit ein konformes Verhalten gemeint (vgl. Amberg et al. 2009, 15). Im Unternehmen stellt Compliance eine Managementaufgabe dar, deren Zweck die Einhaltung aller branchenübergreifenden oder branchenspezifischen Gesetze und Vorschriften ist (vgl. Annuscheit 2006, 1).

2.1.5 Informationssicherheitsmanagement

Es gibt, wie bereits beschrieben, aufgrund der ausschließlich subjektiven Beurteilungsmöglichkeiten keine vollständige Sicherheit. Jedoch gilt es ein akzeptables Sicherheitsniveau zu erreichen und zu halten. Dies gelingt nicht durch einmalige Maßnahmen, sondern muss vielmehr in einem kontinuierlichen Managementprozess erfolgen (vgl. BSI 2008b, 10). Daher kann der Begriff des Informationssicherheitsmanagements (ISM) als Planungs- und Lenkungsaufgabe verstanden werden, die Aufbau, Umsetzung und Effektivität eines Sicherheitsprozesses gewährleistet (vgl. BSI 2008a, 17).

Nach Krcmar (2010, 564) kann das ISM in ein Top-Down-Ansatz mit drei Ebenen gegliedert werden (Abbildung 2-3).

Oberste Managementaufgabe ist die Sicherung der Informationswirtschaft und beinhaltet das Festlegen von Sicherheitszielen und -rahmenbedingungen. Dazu gehört beispielsweise die Festlegung von Verantwortlichkeiten und die Entwicklung eines Sicherheitsbewussteins bei den Mitarbeitern (vgl. Hoppe/Prieß 2003, 272). Aus diesen strategischen Zielen werden technische Anforderungen abgeleitet, die bei der Sicherung der Informati-

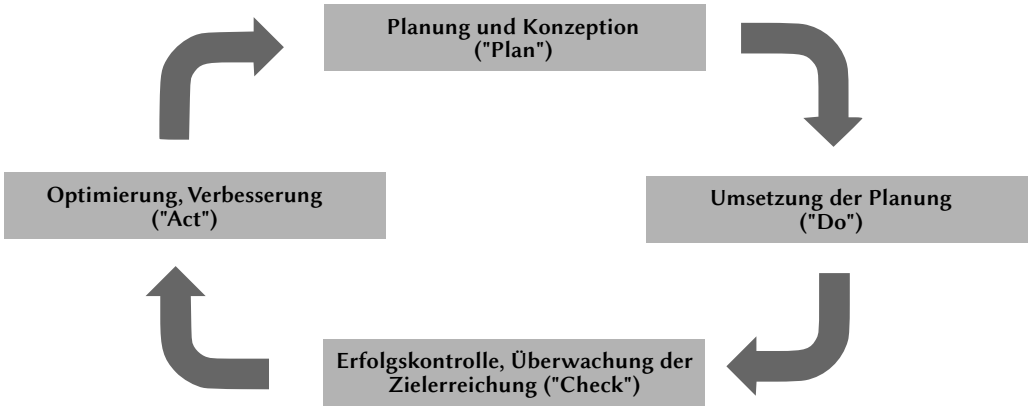


Abbildung 2-4: „Plan-Do-Check-Act"-Zyklus (Quelle:BSI 2008a, 16)

onssysteme eine Rolle spielen. Auf der untersten Ebene, der Sicherung der Informations- und Kommunikationstechnik ist eine technische Sichtweise von Belang; hier werden z.B. Authentifizierungsmethoden festgelegt.

Informationssicherheitsmanagementsystem Um ein strukturiertes und prozessorientiertes Vorgehen zu gewährleisten, ist der Einsatz eines Informationssicherheitsmanagementsystems (ISMS) sinnvoll. „Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert)" (BSI 2008a, 13). Ein üblicher Ansatz bei ISMS ist der „Plan-Do-Check-Act"-Zyklus (PDCA-Zyklus). Er stellt wiederkehrende Handlungen in einem Kreislauf dar (Abbildung 2-4).

Im ersten Schritt („Plan") wird eine ISMS-Politik festgelegt und Maßnahmen beschlossen, die anschließend im zweiten Schritt („Do") umgesetzt werden. Beim dritten Schritt („Check") wird die Wirksamkeit der festgelegten Maßnahmen, vor allem hinsichtlich der Effektivität und der Effizienz, überprüft und bewertet. Die aus dem dritten Schritt gewonnen Erkenntnisse dienen im vierten Schritt („Act") dazu Maßnahmen zu beschließen, um die entdeckten Schwächen zu beseitigen. Es handelt sich um einen iterativen Prozess, bei dem das ISMS kontinuierlich verbessert und an neue Sicherheitsanforderungen angepasst wird (vgl. Krcmar 2010, 580-582).

Risikomanagement Eine wesentliche Aufgabe des ISM ist das IT-Risikomanagement (vgl. Heinrich/Lehner 2005, 260). Da es keine vollständige Sicherheit gibt, wird immer ein gewisses Risiko bestehen. Es gibt aber Möglichkeiten, festzustellen, welches Risiko getragen werden kann. Um das angestrebte Sicherheitsniveau zu erreichen, muss ein gewisser Aufwand betrieben werden. Die Kosten steigen mit wachsendem Sicherheitsniveau exponentiell an, während das Risiko bzw. die Schadenssummen exponentiell

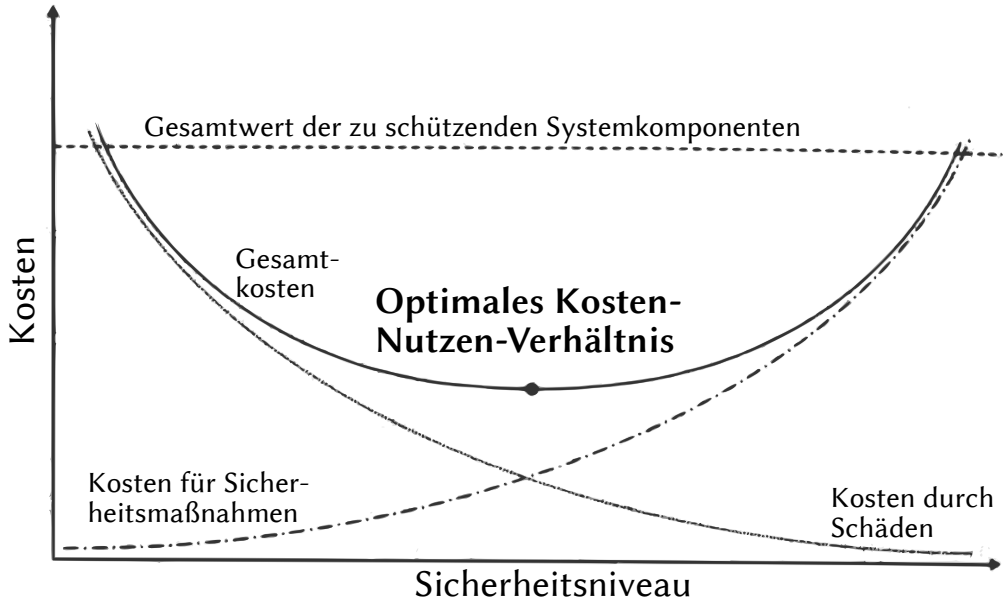


Abbildung 2-5: Optimales Kosten-Nutzen-Verhältnis von Sicherheitsmaßnahmen (Quelle: vgl. Hoppe/Prieß 2003, 280)

abnehmen. Wie hier eine Balance zwischen Sicherheitsniveau und Kosten gefunden werden kann, verdeutlicht Abbildung 2-5. Im Schnittpunkt Kosten und Risikofunktion besteht das optimale Kosten-Nutzen-Verhältnis. In diesem Punkt ist das Verhältnis zwischen Aufwand für Sicherheitsmaßnahmen und möglichen Kosten durch Schäden optimal.

Ein wesentlicher Bestandteil des IT-Risikomanagements ist die Risikoanalyse. Diese besteht in erster Linie aus einer Gefahren- bzw. Bedrohungsanalyse und einer Schwachstellenanalyse (vgl. Hoppe/Prieß 2003, 285f.). Gefahren wirken sich auf die in Kapitel 2.1.2 definierten Grundwerte aus. Dabei ist zu beachten, dass diese nicht nur von externen Quellen, z.B. durch Hackerangriffe oder Naturkatastrophen ausgehen, sondern auch intern entstehen können (vgl. Heinrich/Lehner 2005, 260). Dies geschieht z.B. durch den unverantwortlichen Umgang mit unternehmenssensiblen Daten der eigenen Mitarbeiter. Zusätzlich werden Schwachstellen des ISMS identifiziert. Das Ziel der Risikoanalyse besteht darin, das Risiko dieser Gefahren in Verbindung mit den Schwachstellen qualitativ oder quantitativ zu bewerten (vgl. Krcmar 2010, 576). Dabei besteht das Risiko meist aus der Eintrittswahrscheinlichkeit einer Gefahr und der sich ergebenden Schadenshöhe im Falle eines Eintritts (vgl. Hoppe/Prieß 2003, 285). Diese Vorgehensweise bildet die Grundlage, um das Sicherheitsniveau des Unternehmens bewerten und verbessern zu können. Die in der Risikoanalyse gewonnen Erkenntnisse dienen dazu Maßnahmen einzuleiten, um das Risiko zu steuern. Diese sollten sich an den Sicherheitszielen, die beim ISM festgelegt werden, orientieren (vgl. Krcmar 2010, 574). Eine vollständige Risikovermeidung, z.B. durch die Abschaffung eines gefährdeten Systems, ist selten möglich. Stattdessen muss versucht werden risikomindernde Maßnahmen einzuführen. Möglich

ist auch eine Übertragung des Risikos an Dritte (vgl. Krcmar 2010, 577), was im Fall von Cloud-Computing teilweise geschieht. Analog zum PDCA-Zyklus handelt es sich beim IT-Risikomanagement um keinen einmaligen Prozess. Risikoanalysen müssen regelmäßig wiederholt werden, um neue Gefahrenquellen und Schwachstellen zu entdecken (vgl. Heinrich/Lehner 2005, 260). Zusätzlich kann so die Wirksamkeit der eingeleiteten Maßnahmen überprüft werden.

Standards und Frameworks

ISO/IEC 27001 Die Standards ISO/IEC 27001 und ISO/IEC 27002 der „International Organization for Standardization“ und „International Electrotechnical Commission“ beschreiben im Wesentlichen den Aufbau und den Betrieb eines ISMS. Wobei ISO/IEC 27001 ein Standard ist, der zertifiziert werden kann und ISO/IEC 27002 ein „Code of Practise“ der nicht zertifiziert werden kann (vgl. Brotby 2009, 64).

CobiT ist ein Framework zur IT-Governance und wurde von der „Information Systems Audit and Control Association (ISACA) 1996 veröffentlicht (vgl. Jaquith 2007, 91). Aktuell wird es von dem „Information Technology Governance Institute“ (ITGI) herausgegeben. Aufgaben der IT werden in Prozesse und Kontrollziele gegliedert. Die Prozesse sind u.a. die Erstellung eines strategischen IT-Plans, einer Informationsarchitektur, des Configuration- und Facility-Management und die Sicherstellung der Systemsicherheit (vgl. Fitzgerald 2007, 17). Letztere ist in Kontrollziele heruntergebrochen, wie z.B. Security-Measures-Management, Authentifizierung und Identitätsmanagement, Datenklassifizierung, Firewallarchitektur. Die Prozesse sind in vier Bereiche geteilt: „Plan and Organize“, „Acquire and Implement“, „Deliver and Support“ und „Monitor and Evaluate“ (vgl. Brotby 2009, 59).

ITIL ist ein „Best Practices“-Framework für Prozesse, die beim Betrieb von IT-Services Anwendung finden (vgl. Fitzgerald 2007, 17). Diese sind u.a. das Change-, Release-, Incident-, Kapazitäts- und Verfügbarkeits-Management. ITIL beschreibt wie Kontrollen und Überwachungen dieser Prozesse zuverlässig gewährleistet werden können. Im Zentrum stehen bei der Version 3 des Frameworks die Bedürfnisse der Kunden der angebotenen Services (vgl. Long 2008, 16) und nicht mehr die technischen Rahmenbedingen.

Im Vergleich zwischen ISO 27001, COBIT und ITIL zielt ITIL eher auf die Service-Erbringung, ISO 27001 eher auf Technologie und CobiT eher auf Kontrollprozesse ab (vgl. Jaquith 2007, 92)

Richtlinien, Gesetze und Verordnungen

Bundesdatenschutzgesetz (BDSG) Das BDSG regelt die Übermittlung von personenbezogenen Daten und gilt für alle öffentlichen Stellen des Bundes und für die Privatwirtschaft (vgl. BITKOM 2008, 6). Das anzuwendende Recht bezieht sich auf den Sitz der verantwortlichen Stelle, nicht auf den Ort der Datenverarbeitung. Das gilt auch für ausländische Unternehmen, die in Deutschland eine Niederlassung haben und personenbezogene Daten erheben oder verarbeiten (vgl. BITKOM 2008, 6).

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) Die GDPdU sind eine Verwaltungsanweisung des Bundesministeriums für Finanzen. Sie verlangen die Bereithaltung von steuerlich relevanten Daten in auswertbarer Form (vgl. Kampffmeyer 2006, 2).

2.1.6 Controlling der Informationssicherheit

Messbarkeit der Informationssicherheit

Um ein System oder ein Risiko bewerten zu können, werden Informationen über den Ist-Zustand benötigt. Die Informationen werden durch Messungen, aus denen Kennzahlen hervorgehen, gewonnen. Die Bedeutung von Kennzahlen geht über die der reinen Messwerte hinaus. Es sind quantitativ erfassbare Sachverhalte in aggregierter Form, die den Bedürfnissen der Bewertung angepasst sind (vgl. Staats 2009, 33). Die Schwierigkeit der Messungen liegt in der schwierigen Zuordnung von Kosten. Beim Cloud-Computing sind diese aber transparenter, zumindest was Administrationsaufgaben angeht, die der Dienstleister durchführt.

ISO/IEC 27004 Die ISO/IEC-Standards 27001/27002 für Informationsmanagementsysteme haben kaum Ansätze, um Aussagen über die Güte und Performance eines ISMS zu treffen (vgl. Böhmer 2010, 2163). Aus diesem Grund ist der Standard ISO/IEC 27004 entwickelt worden, der beschreibt wie geeignete Messgrößen für ein ISMS erstellt und benutzt werden können, um dessen Effektivität zu beurteilen (vgl. ISO 2009, 18ff.).

NIST SP 800-55 Der „Performance Measurement Guide for Information Security“ (NIST SP 800-55) des U.S. „National Institute of Standards and Technology“ (NIST) ist ein Handbuch zur Entwicklung und Anwendung von Metriken der Informationssicherheit. Die im NIST SP 800-55 entwickelten Metriken sollen Indikatoren für die Umsetzung, Effektivität/Effizienz und Wirkung von Sicherheitsmaßnahmen des Unternehmens sein (vgl. NIST 2008, 10).

2.2 Cloud-Computing

Der folgende Abschnitt beschreibt den Begriff des Cloud-Computings und die Voraussetzungen für seine Nutzung sowie technische Grundlagen und Ausprägungen in der Praxis.

2.2.1 Grundlagen des Cloud-Computings

Cloud-Computing ist eine Weiterentwicklung der Service-Orientierung von IT-Leistungen. Dem Nutzer werden IT-Leistungen wie Hard- und Software nicht mehr als losgelöste Produkte angeboten, sondern als Dienstleistung (vgl. Buxmann et al. 2008, 500). Möglich wird dies durch abstrakte virtuelle Einheiten, die dynamisch skalierbar „on demand“ dem Nutzer über das Internet zur Verfügung gestellt werden (vgl. Foster et al. 2008, 60).

Virtualisierung
Virtualisierung ist eine Basistechnologie des Cloud-Computings (vgl. Baun et al. 2010, 7). Mehrere physische Komponenten (Prozessoren, Speicher) erhalten durch eine Abstraktionsschicht eine einzige logische Sicht. Diese ist wiederum in kleinere logische Einheiten unterteilt, welche gemeinsam verwaltet werden. Werden nun mehrere logische Einheiten beansprucht, spielt es keine Rolle von wie vielen physischen Komponenten diese stammen. Abbildung 2-6 zeigt den Vergleich zwischen traditionellen Rechenzen-

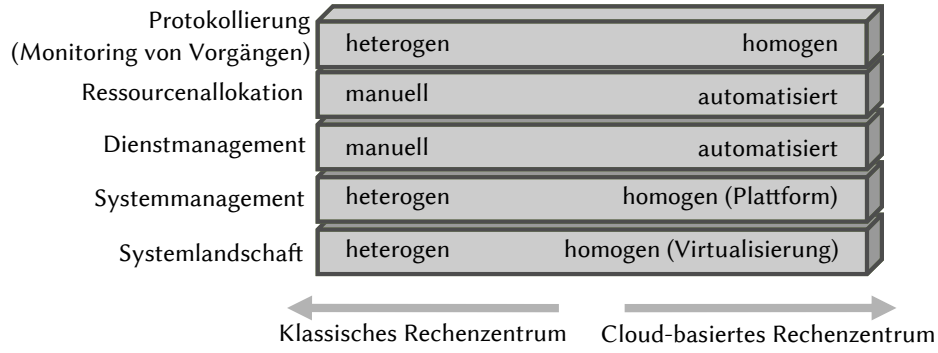
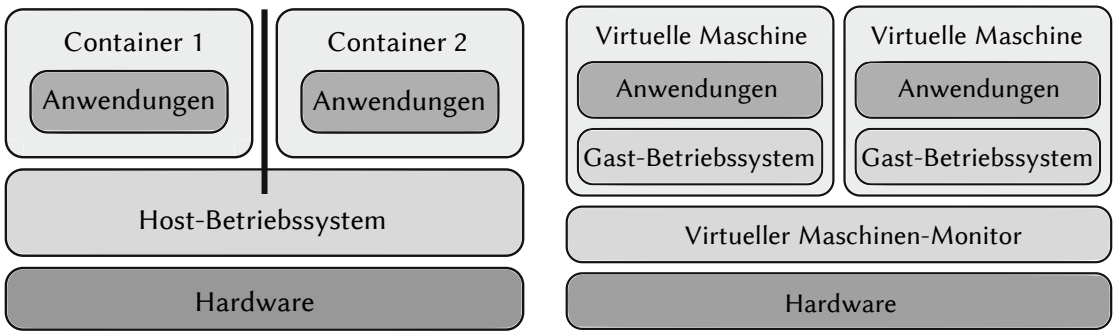


Abbildung 2-6: Klassische Rechenzentren im Vergleich zu cloud-basierten Rechenzentren (Quelle: vgl. Deussen et al. 2010, 24)

tren und Cloud-basierten Rechenzentren. Die Systemlandschaft in einem klassischen Rechenzentrum ist heterogen, jeder Server ist seinen spezifischen Aufgaben angepasst; in einem Cloud-Rechenzentrum sind die Server durch die Abstraktionsschicht homogen. Daraus leitet sich ab, dass in einem klassischen Rechenzentrum die Server individuell verwaltet werden müssen, während bei der Cloud-Infrastruktur durch die Homogenität eine gemeinsame Verwaltung stattfinden kann. Dies lässt sich auch auf das Dienstemanagement und die Ressourcenallokation ableiten, da durch die Gleichheit der Komponenten eine Automatisierung möglich wird.



(a) Betriebssystemvirtualisierung (b) Plattformvirtualisierung

Abbildung 2-7: Virtualisierung (Quelle: Baun et al. (vgl. 2010, 11))

Um die Virtualisierung vorzunehmen gibt es verschiedene Konzepte; die wichtigsten zwei werden im Folgenden dargestellt:

Betriebssystemvirtualisierung (Abbildung 2-7a) Auf einem Host-Betriebssystem laufen verschiedene Container mit seperaten Laufzeitumgebungen. Alle Container verwenden den gleichen Betriebsystemkern.

Plattformvirtualisierung (Abbildung 2-7b) Auf einem Host-System können vollständige Rechner virtualisiert werden, die beliebige Betriebssysteme als Gast erlauben.

Gründe für die Nutzung

Die Gründe für die Nutzung von Cloud-Computing sind auf Nutzerseite:

Flexibilität Durch die dynamische Skalierung der genutzten Ressourcen und das „pay-as-you-go“-Modell werden nur die Ressourcen beansprucht und bezahlt, die auch benötigt werden (vgl. Armbrust et al. 2009, 2; Foster et al. 2008, 65; Baun et al. 2010, 8). Zudem müssen keine eigenen Rechenzentren betrieben werden, die bedingt durch seltene Lastspitzen möglicherweise überdimensioniert sind und dadurch Kapital binden.

Verfügbarkeit Durch die flexible Austauschbarkeit der Hardware im Hintergrund und die Möglichkeit, den physikalischen Ort der Nutzung im laufenden Betrieb zu ändern, kann der Anbieter für eine hohe Verfügbarkeit sorgen.

Reduktion der Komplexität Die Komplexität der Informationstechnologie wird vor dem Nutzer verborgen; er muss nicht wissen wie der Dienst generiert wird (vgl. Baun et al. 2010, 7). Technische Einrichtungs- und Verwaltungsaufgaben entfallen für den Nutzer.

Zeit- und Kostenersparnis
Während es in einer traditionellen IT-Abteilung Wochen dauern kann bis neue Hardware angeschafft und eingerichtet ist, sind beim Cloud-Computing Ressourcen in der Regel innerhalb von Minuten bereitgestellt (vgl. Baun et al. 2010, 90). Es ergeben sich weitere Vorteile in Form von entfallendem Lizenzmanagement und reduzierten Administrationsaufgaben. Die Unternehmen können sich auf ihre Kernkompetenzen und neuen Geschäftsideen konzentrieren und dabei die Kosten und Managementaufgaben der nötigen IT auf ein Minimum reduzieren. Schutzmaßnahmen (Viren, Spam) für Server entfallen je nach Situation ebenfalls, da der Dienstleister dies übernimmt.

Auf Anbieterseite ergeben sich die Vorteile durch (vgl. Baun et al. 2010, 2):

Economies of scale Ein spezialisierte Anbieter kann mit großen Rechenzentren an strategisch günstigen Orten durch Skaleneffekte den Betrieb optimierten.

Virtualisierung Durch die Aufteilung der Hardware in flexible virtuelle Einheiten können Hardwarekomponenten optimal ausgelastet werden. In nicht virtualisierten Umgebungen übernehmen Rechner i.d.R. nur wenige Aufgaben und sind durch seltene Lastspitzen überdimensioiert ausgelegt, sie sind im Durchschnitt daher nur gering ausgelastet. Die Verwaltung kann wesentlich automatisierter stattfinden (siehe oben).

2.2.2 Erscheinungsformen

Es gibt verschiedene Erscheinungsformen des Cloud-Computings, die unterschiedliche Ansprüche bedienen und von unterschiedlichen Vorraussetzungen abhängen. Aus technischer Sicht sind dies in erster Linie Infrastrukturen, Plattformen und Software, die als Dienstleistung angeboten werden. An sich handelt es sich um bereits existierende Technologien, die im Cloud-Computing eine andere Nutzungsform erfahren (vgl. Mather et al. 2009, 11). Dieses neue System der Nutzung wird in Abbildung 2-8 dargestellt. Aus organisatorischer Sicht kann Cloud-Computing in Private, Hybrid und Public Cloud-Computing unterteilt werden.

Infrastructure as a Service IaaS bezeichnet die Bereitstellung von Infrastrukturen als Cloud-Service. Diese Infrastrukturen sind eine abstrahierte Sicht auf Hardware (vgl. Baun et al. 2010, 29). Typische Komponenten, die als IaaS bereitgestellt werden sind z.B. virtuelle Rechner, Massenspeicher und Datenbanken.

Platform as a Service PaaS stellt Entwicklungs- und Laufzeitumgebungen bereit. Dies können beispielsweise Programmierumgebungen mit passenden Laufzeitumgebungen sein (vgl. Baun et al. 2010, 33). Ein Beispiel ist die „Google App Engine“ (vgl. Google 2011, 1). Nutzer erhalten eine fertige und auf die gewünschte Sprache angepasste Programmierumgebung um „Google Apps“ zu erstellen. „Google Apps“

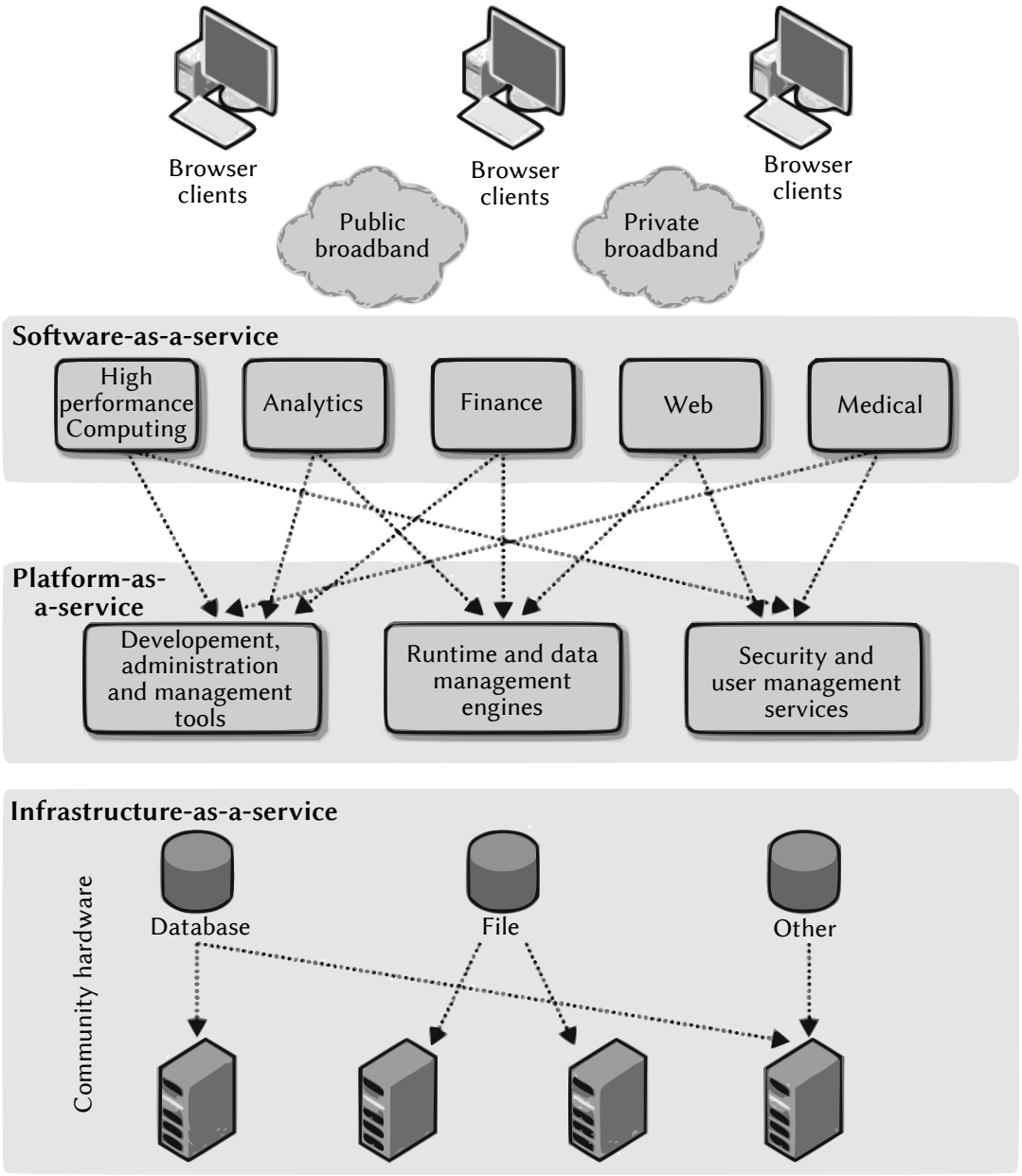


Abbildung 2-8: Verschiedene Cloud-Technologien (Quelle: vgl. Mather et al. 2009, 12)

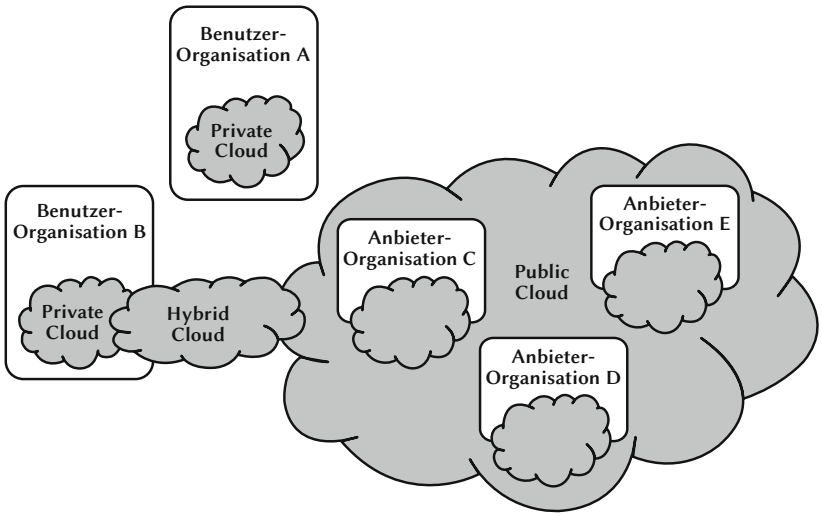


Abbildung 2-9: Private, Hybrid und Public Cloud (Quelle: vgl. Baun et al. 2010, 26)

ist eine Plattform der Firma Google Incorporated um Webanwendungen bereitzustellen. Mit der Laufzeitumgebung wird der Betrieb der Anwendung ermöglicht.

Software as a Service SaaS stellt Software als Service bereit. Die Installation und Bereitstellung von nötigen Ressourcen entfällt, sie kann sofort genutzt werden (vgl. Baun et al. 2010, 35). Beispiele für SaaS sind „Google Maps“, ein Kartendienst und „Microsoft Office Live“, eine Office-Suite (vgl. Baun et al. 2010, 35).

Die organisatorische Abgrenzung ist in Abbildung 2-9 dargestellt.

Private Cloud Bei der „Private“ oder auch „Internal Cloud“ gehören Anbieter und Nutzer der gleichen organisatorischen Einheit an (vgl. Baun et al. 2010, 26). Da die IT-Leistungen in diesem Fall unternehmensintern erbracht werden, haben Dritte keinen Zugang zur Cloud-Infrastruktur. Hauptgrund für die Nutzung einer „Private Cloud“ sind Sicherheitsaspekte oder Datenschutzvorgaben. Einige Vorteile, die Cloud-Computing bietet, werden durch eine Private Cloud wieder relativiert. Denn sie müssen intern erbracht werden. Effizienzgewinne lassen sich dank Virtualisierung zwar nutzen, allerdings müssen die restlichen Lasten wie Hardware- und Lizenzmanagement wieder selbst bewältigt werden.

Public Cloud Bei der „Public“ oder „External Cloud“ gehören Anbieter und Nutzer im Gegensatz zur „Private Cloud“ unterschiedlichen organisatorischen Einheiten an (vgl. Baun et al. 2010, 25). Hier kommen die oben angesprochenen Vorteile der Anbieter- und Nutzerseite voll zum Tragen.

Hybrid Cloud „Hybrid Clouds“ sind eine Mischform aus Private und Public Cloud. Es werden beide Varianten zusammen benutzt. Meist existiert eine Private Cloud und

	Private Cloud	Hybrid Cloud	Public Cloud
Vertraulichkeit	hoch, Daten bleiben im Unternehmen	gefährdet, Daten teilweise außerhalb des Unternehmens	gefährdet, Daten außerhalb des Unternehmens
Integrität	hoch, Daten auf eigenen Systemen	gefährdet, Daten teilweise auf Systemen Dritter	gefährdet, Daten auf Systemen Dritter
Verfügbarkeit	schwere Lokalisierung, hohe Verfügbarkeit	schwierigste Lokalisierung, teilweise Abhängigkeit von externer Verfügbarkeit	schwere Lokalisierung, Abhängigkeit von externer Verfügbarkeit

Abbildung 2-10: Grundwerte beim Cloud-Computing (Quelle: Schürmann 2010, 55 in Anlehnung an Hansen 2009, 10ff.)

bei Lastspitzen werden Ressourcen aus der Public Cloud hinzugenommen (vgl. Baun et al. 2010, 27).

Community Cloud Community-Clouds sind ebenfalls zwischen der Private-Cloud und der Public-Cloud einzuordnen. Es ist ein kooperatives Modell, bei dem Cloud-Dienste kolloborativ von mehreren Anbietern betrieben werden (vgl. Deussen et al. 2010, 20). Dabei kann es sein, dass die Dienste nur für einen definierten Kundenkreis bereitgestellt werden, was eher einer Private-Cloud entspräche. Es kann aber andererseits sein, dass die Dienste offen für andere sind, was eher einer Public-Cloud entspräche (vgl. Deussen et al. 2010, 20).

2.2.3 Sicherheitsaspekte des Cloud-Computings

Dieser Abschnitt versucht die veränderte Lage von Sicherheitsaspekten in Bezug auf das Cloud-Computing zu erörtern.

„It [Cloud-Computing] is a security nightmare and it can't be handled in traditional ways" (McMillan 2009, 2). Mit dieser Aussage stellte John Champers, CEO des Telekommunikationsanbieters Cisco klar, dass die bestehenden Ansätze zur Bewältigung der IT-Sicherheit im Fall von Cloud-Computing nicht mehr ausreichend sind. Abbildung 2-10 fasst die Sicherheitsaspekte der organisatorischen Cloud-Ebenen zusammen.

Durch die Virtualisierung und den netzwerkbasierten Zugang zu Diensten, werden die Besitz- und Berechtigungsstrukturen von Leistungserstellungsprozessen und Datenbeständen verändert (vgl. Deussen et al. 2010, 6). Daraus können Unsicherheiten bzgl. der jeweiligen Zuständigkeit entstehen und möglicherweise können traditionelle Verfahren nicht angewandt werden. Besonders zu prüfen ist, ob diese Schwierigkeiten im Rahmen

von Service Level Agreements hinreichend regelbar sind (vgl. Deussen et al. 2010, 6).

Browsersicherheit
Da Browser in Bezug auf Cloud-Computing häufig als Universalclient eingesetzt werden (vgl. Schwenk 2011, 75), kann es ein Problem darstellen, Browser mit fehlerhaft implementierten Sicherheitsmechanismen zu nutzen (z.B. wird bis heute von vielen Browsern das Protokoll TLS („Transport Layer Security“) in der Version 1.0 unterstützt, bei dem verschlüsselt übertragene Cookies ausgelesen werden können (vgl. Eikenberg 2011, 1)). Ein Lösungsweg besteht darin, verstärkt auf die Nutzung von VPNs auszuweichen, allerdings gibt es selbst in diesem Fall Gefahren. Es gibt grundsätzliche Probleme mit elektronischen Zertifikaten für das SSL-Protokoll (in der Vergangenheit wurden mehrfach Zertifikatsaussteller kompromittiert, sodass gefälschte, aber gültige Zertifikate missbräuchlich eingesetzt werden konnten) (vgl. Kuri 2011, 1). Zudem bieten Browser mit ihrer Universalität und Erweiterbarkeit einen enormen Funktionsumfang und damit viele Angriffspunkte (vgl. Schwenk 2011, 76).

Ausländische Dienstleister
Es gibt ein grundsätzliches Problem mit ausländischen Cloud-Dienstleistern, selbst wenn sie europäische Niederlassungen haben: Sowohl Microsoft als auch Google übergeben Daten an US-Behörden; dies gilt auch, wenn diese Daten in europäischen Rechenzentren liegen (vgl. Stölzel 2011, 1; Kirsch 2011b, 1). Die Herausgaben erfolgen u.U. sogar ohne Benachrichtigung der betroffenen Kunden (durch sog. „Gag orders“ im Rahmen des „National Security Letter“) (vgl. Kirsch 2011b, 1). D.h. dass kein Unternehmen aus den USA die erforderlichen Garantien geben kann, personenbezogene Daten nur innerhalb Europas zu halten. Im weiteren Sinne muss sogar die Frage gestellt werden, ob Unternehmen dies können, die eine Niederlassung in den USA haben, da sie dadurch unter Druck gesetzt werden könnten. Die Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben eine Orientierungshilfe (vgl. Budszus et al. 2011) veröffentlicht, die Handlungsempfehlungen für den Umgang mit ausländischen Cloud-Dienstleistern beinhalten. In dieser Orientierungshilfe wird die Nutzung von Cloud-Diensten aus den USA zwar nicht generell als unmöglich eingestuft, jedoch sind die Anforderungen hoch. So müssen die Dienstleister u.a. Garantien zum Schutz des allgemeinen Persönlichkeitsrechts vorlegen (vgl. Budszus et al. 2011, 10), was mit Blick auf die oben gemachten Ausführungen schwierig erscheint. Zusätzlich müssen neben der Anforderung, dass der Dienstleister sich den Safe-Harbor-Grundsätzen unterworfen hat, noch weitere Kontrollen durchgeführt und Bedingungen eingehalten werden (vgl. Budszus et al. 2011, 11f.). Allerdings erscheint das Safe-Harbor-Abkommen fragwürdig in Anbetracht der Tatsache, dass lediglich eine Gebühr für die Mitgliedschaft erhoben wird. Zertifizierung oder Evaluation finden nicht statt. Zudem bleiben Missach-

tungen ohne Folgen (vgl. Schulzki-Haddouti/Ziegler 2010, 1; Lederer 2011, 1f.; o.V. 2011, 1f.).

Umgebung

Ein weitere Besonderheit beim Cloud-Computing ist die Tatsache, dass Angreifer und Nutzer u.U. auf einer Stufe stehen, zumindest in der Hinsicht, dass beide von außen auf die Dienste und Daten zugreifen (vgl. Schwenk 2011, 74). Da der Zugriff für beide über die gleiche physikalische Schnittstelle (das Internet) erfolgt, können Firewalls etc. nicht mehr generell vor externen Zugriffen schützen. Daraus lässt sich erkennen, dass die Sicherheit der Identitäten einen großen Einfluss auf die Sicherheit der Daten hat (vgl. Schwenk 2011, 74). Dem Identitätsmanagement kommt eine große Bedeutung für das Cloud-Computing zu.

Web Services

Die neuen Technologien zur Nutzung von Cloud-Services machen neue Protokolle erforderlich. Daher wurden auf dem SOAP-Protokoll („Simple Object Access Protocol“) aufbauende Web-Services-Protokolle entwickelt. Mit Hilfe von „WS Security“ soll die Integrität von SOAP-Nachrichten gewährleistet werden. McIntosh/Austel (2005) konnten nachweisen, dass dies nicht zuverlässig geschieht. Eine Variante dieses Problems (vgl. Gruschka/Iacono 2009) führte dazu, dass Programme unter einer fremden Identität in der Amazon-Cloud ausgeführt werden konnten (vgl. Schwenk 2011, 86).

Unzureichende Datenlöschung/interne Angriffe

Da sich Kunden in Public-Clouds mit anderen Kunden in der selben Systemumgebung bzw. sogar auf dem selben System befinden, besteht die Möglichkeit von internen Angriffen. Wenn der Hypervisor, also das Verwaltungssystem, das bei der Virtualisierung die Ressourcen unter den Gast-Systemen verteilt, kompromittiert wird, kann ein Angreifer u.U. sämtliche Daten der auf dem System laufenden Instanzen auslesen (vgl. ENISA 2009, 54). Ein weiteres Problem ist die unzureichende Trennung von Instanzen auf einem System (vgl. ENISA 2009, 54). Ristenpart et al. (2009) zeigten, dass es möglich ist so lange gezielt Instanzen in der Amazon-Cloud zu starten, bis die eigene Instanz parallel mit einer Zielinstanz auf einem System läuft. Im Anschluss konnten Informationen über die Zielinstanz ausgelesen werden.

Weiterhin ist die nicht vorhandene Kontrollmöglichkeit, ob Daten zuverlässig gelöscht werden, problematisch. Im Fall von unzureichender Löschung könnte eine nachfolgende Instanz Daten der Vorgängerinstanz wiederherstellen und auslesen (vgl. ENISA 2009, 10). Bisher fehlt ein zertifizierbarer Standard, der die veränderten Prozesse im Cloud-Computing berücksichtigt und so Transparenz erzeugt und damit Vertrauen aufbauen kann (vgl. Bernd-Striebeck 2011, 19). Dabei ist zu bedenken, ob der Aufwand zur Erfüllung

der Anforderungen, die sich aus dem Bundesdatenschutzgesetz ergeben, die bezweckte Kostenreduzierung nicht zunichte macht (vgl. Duisberg 2011, 60).

Im Gegenzug kann die Nutzung von Cloud-Computing aber auch eine Verbesserung der Sicherheit bedeuten. Durch starke Vereinfachung der Zugriffsmöglichkeiten und Prozesse, durch Reduzierung von Schnittstellen und durch automatisierte Bereinigungen nicht genutzter Ressourcen reduzieren sich die benötigten Sicherheitskontrollen und Abwehrmaßnahmen (vgl. Waidner 2010, 13). Die Angriffsmöglichkeiten werden dadurch ebenfalls reduziert. Es besteht sogar die Möglichkeit Sicherheitsfunktionen als „Security-as-a-Service“ in die Cloud auszulagern (vgl. Mather et al. 2009, 217). Die starke Vereinfachung kann jedoch auch ein Problem darstellen, wenn der Dienstleister unsorgfältig arbeitet. Beim Cloud-Speicherdienst „Dropbox“ konnten sich nach einem fehlerhaften Softwareupdate Nutzer in beliebige Accounts anmelden (vgl. Singel 2011a, 1). Dropbox verschlüsselt zwar die Daten (vgl. Dropbox 2011, 1), hat die Verschlüsselung jedoch so implementiert, dass sie praktisch bedeutungslos ist (vgl. Singel 2011b). Auch Amazons Verschlüsselungsservice für den Speicherdienst S3 ist fragwürdig: Es werden zwar pro Kunde individuelle Schlüssel verwendet, jedoch liegt die gesamte Schlüsselverwaltung bei Amazon selbst, obwohl hier dem Nutzer die Hoheit über die Daten zurückgegeben werden könnte (vgl. Lippert/Kirsch 2011, 1). An diesen Beispielen wird deutlich, wie wichtig und zugleich schwierig die Transparenz des Cloud-Dienstleisters ist.

Eine Möglichkeit diesen Problemen zu begegnen, besteht im Verzicht auf Verarbeitung von Daten in der Cloud. Dies stünde mit einem reinem Speicherdienst gleich. Gleichzeitig ermöglicht dies durchgängige (nutzerseitige) Verschlüsselung. Eine Möglichkeit verschlüsselte Daten zu verarbeiten ist die „vollhomomorphe“ Verschlüsselung (vgl. ENISA 2009, 55). Diese erlaubt die Verarbeitung von Daten auch im verschlüsselten Zustand. In diesem Bereich gibt es bisher nur Fortschritte im akademischen Bereich (vgl. Simonite 2010). Eine Zwischenlösung ist die temporäre, nur für die jeweilige Verarbeitung vorgenommene Entschlüsselung (vgl. Wang 2010, 1). Wobei darauf geachtet werden sollte, dass die Schlüssel separat aufbewahrt werden (vgl. Krutz/Vines 2010, 246).

Aufgrund von Datenverlusten in der Vergangenheit (z.B. bei Amazon, Google und Microsoft, vgl. Haupt 2011; Ihlenfeld 2011; Pakalski 2009) wird klar, dass Daten in der Cloud auch nicht vor Verlust vollständig geschützt sind. Backups außerhalb von Cloud-Dienstleistern sind also sinnvoll.

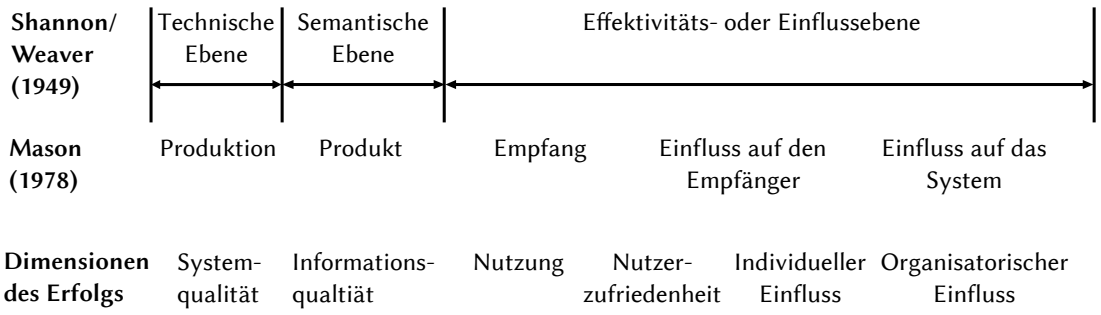


Abbildung 3-1: Dimensionen und Ebenen des Erfolgsmodells von DeLone/McLean (1992, 62)

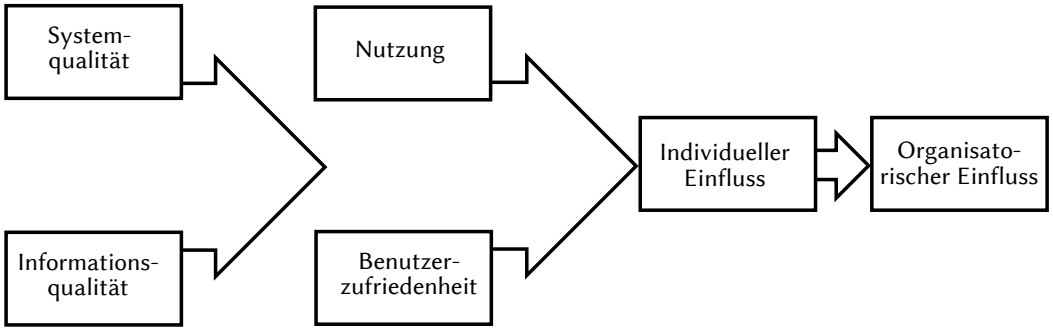


Abbildung 3-2: Erfolgsmodell für Informationssysteme von DeLone/McLean (1992, 87)

3 Entwicklung eines Modells zur Informationssicherheit im Cloud-Computing

Im folgenden Abschnitt wird ein hypothetisches Modell zur Bewertung der Informationssicherheit im Cloud-Computing entwickelt.

3.1 Erfolgsmodell für Informationssysteme nach Delone/McLean

Um das Modell zur Informationssicherheit zu entwickeln wird zunächst auf das von DeLone/McLean 1992 erstellte und 2003 überarbeitetes Modell zur Erfolgsmessung von Informationssystemen zurückgegriffen. Die Autoren verglichen in ihrer ersten Veröffentlichung 180 wissenschaftliche Beiträge zum Thema „Erfolg von Informationssystemen“ und führten diese zu einem multidimensionalen Modell zusammen. Das Modell ist in verschiedene Kategorien (bzw. Dimensionen) eingeteilt, die unterschiedlich miteinander in Beziehung stehen. Dazu projizieren sie die Kategorien auf die Einflussebene nach Mason (1978) und die drei Ebenen der Kommunikationstheorie von Shannon/Weaver (1949). Dieser Zusammenhang und die sechs Kategorien sind in Abbildung 3-1 und 3-2 dargestellt.

2003 erweiterteten die beiden Autoren ihr Modell um die Komponenten Servicequalität,

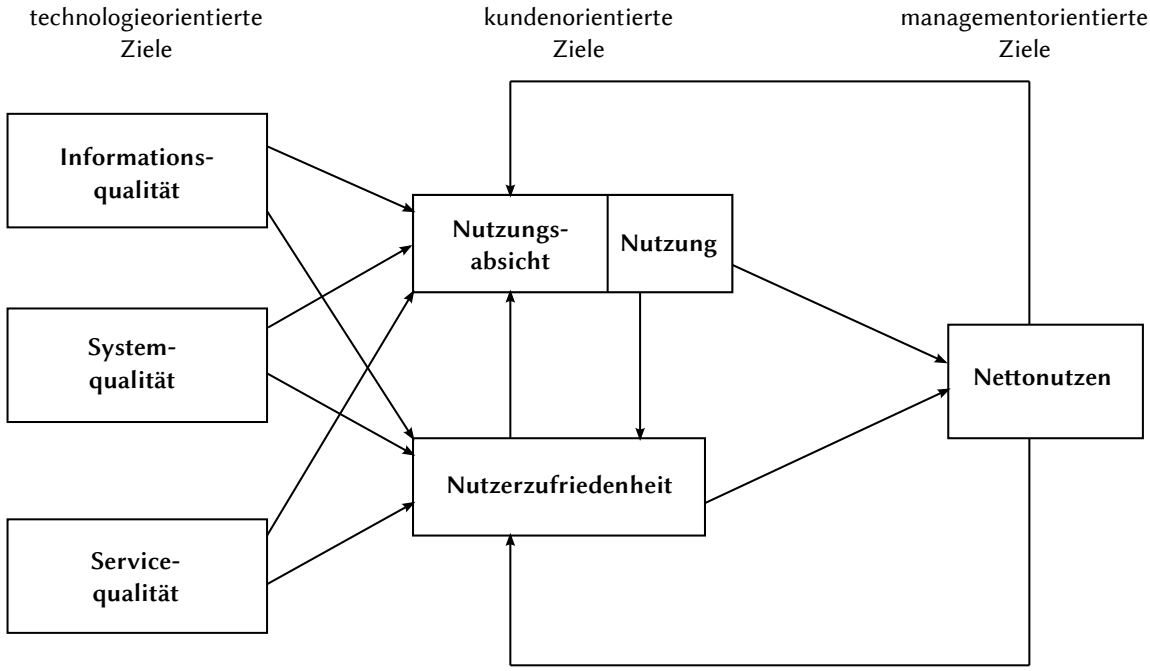


Abbildung 3-3: Erweitertes Erfolgsmodell von DeLone/McLean (2003, 24) (In Anlehung an Blattmann et al. (2010, 1234))

beabsichtigte Nutzung und Nettonutzen. Das Resultat ist das Modell mit den Kategorien und deren Zusammenhängen in Abbildung 3-3.

Um die Popularität dieses Modells zu belegen, wurde eine Recherche in verschiedenen Wissenschaftsdatenbanken durchgeführt. Diese Popularität bezieht sich auf den wissenschaftlichen Bereich; Neumann et al. (2011) wiesen Einschränkungen für die Anwendbarkeit in der Praxis nach.

Suchportal	Durchsuchte Datenbanken
sciverse.com	Publikationen des Elsevier-Wissenschaftsverlags und andere
isiknowledge.com	Wissenschaftsdatenbank des ehemaligen „Institute for Scientific Information (ISI)“ (heute Thomson Reuters)
search.ebscohost.com	wissenschaftliche Literatur- und Volltextdatenbanken hauptsächlich für Universitätsbibliotheken
portal.acm.org	Journals und Proceedings der „Association for Computing Machinery“
aisel.aisnet.org	Journals und Proceedings der „Association for Information Systems“
ieeexplore.ieee.org	Journals und Proceedings des „Institute of Electrical and Electronics Engineers“
emeraldinsight.com	Publikationen des Fachzeitschriftenverlags „Emerald Group Publishing“
springerlink.com	Publikationen des Wissenschaftsverlags „Springer Science+Business Media“
ovidsp.tx.ovid.com	wissenschaftliche Literaturdatenbanken der Firma „Ovid Technologies“
dblp.mpi-inf.mpg.de	Vom „Digital Bibliography & Library Project“ indizierte Journals und Proceedings
gso.gbv.de/DB=2.2	Katalog des Bibliotheksverbundes „Gemeinsamer Bibliotheksverbund“ inkl. der „Online Contents“-Datenbank (GVK-PLUS)
wiso-net.de	Fachzeitschriftendatenbank des Unternehmens „GBI-Genios Deutsche Wirtschaftsdatenbank“

Abbildung 3-4: Suchportale

Die Recherche erfolgte unter folgenden Annahmen: Bei Vorkommen der Wörter „DeLone“ und „McLean“ im Titel, der Zusammenfassung oder den Keywords[1] kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass das Modell ein Kernthema in der betreffenden Publikation ist. Dies wurde durch Stichproben bestätigt. In den meisten Fällen handelt es sich um Adaptionen des Modells an neue Untersuchungsgegenstände. Um die Häufigkeit der Verwendung der Version von 2003 zu messen, wurde innerhalb der Suchergebnisse im Volltext oder den Literaturangaben nach „A Ten-Year Update“, dem Titel der Veröffentlichung von 2003, gesucht. Eine Zitierung der neueren Version wurde demnach mit ihrer Verwendung in der Publikation gleichgesetzt. Die Ergebnisse der Recherche sind in Abbildung 3-4 und 3-5 dargestellt. Es wurde keine zeitliche Einschränkung hinsichtlich des Veröffentlichungsdatums vorgenommen.

[1]Keywords sind von den Autoren angegebene Stichwörter, die den Inhalt eines Artikels wiedergeben.

Suchart	Suchportal	1992	2003	Gesamt
Gesamttreffer: Vorkommen der Wörter „DeLone“ und „McLean“ in Titel oder Zusammenfassung oder Keywords Treffer für die Version von 2003: zusätzliches Vorkommen von „A Ten-Year Update“ im Volltext bzw. im Literaturverzeichnis Treffer für die Version von 1993: Differenz aus Gesamttreffer und Treffer für 2003	sciverse.com	62	28	90
	search.ebscohost.com	52	15	67
	portal.acm.org	50	4	54
	aisel.aisnet.org	11	22	33
	ieeexplore.ieee.org	11	15	26
	emeraldinsight.com	1	5	6
Vorkommen der Wörter „DeLone“ und „McLean“ in Titel oder Zusammenfassung	springerlink.com	×	×	14
	ovidsp.tx.ovid.com	×	×	11
Vorkommen der Wörter „DeLone“ und „McLean“ im Titel	dblp.mpi-inf.mpg.de	×	×	25
	GVK-PLUS	×	×	22
	isiknowledge.com	×	×	13 (89)[2]
	wiso-net.de	×	×	8

Abbildung 3-5: Popularität des Erfolgsmodells von DeLone/Mclean (Suchergebnisse vom 30.05.2011)

3.2 Qualitätsmodell nach Rodríguez/Casanovas

Der Erfolg einer Organisation hängt u.a. von der (Service-)Qualität der verwendeten Informationssysteme ab (vgl. Ferguson/Zawacki 1993, 24; Saaksjarvi/Saarinen 1994, 84). Sicherheit und Verlässlichkeit wiederum sind Schlüsselfaktoren für die Qualität von Informationssystemen (vgl. Toval et al. 2002, 206; Chung 1993, 234; Zahedi 1987). Daher sieht der Autor statt eines Erfolgsmodells ein Qualitätsmodell für die Bewertung der Informationssicherheit im Cloud-Computing als geeigneter an. Rodríguez/Casanovas entwickelten 2010 eine solche Variante des DeLone/McLean-Modells. Dazu reicherten sie es mit existierenden Qualitätsmodellen an. Das Ergebnis ist in Abbildung 3-6 zu sehen.

Die in diesem Modell verwendeten Dimensionen der Qualität sind (vgl. Rodríguez/Casanovas 2010, 5):

Information quality Informations- bzw. Datenqualität der Informationssysteminputs und -outputs. Die Messung erfolgt in Form von Fehlerfreiheit, Genauigkeit, Aktua-

[2]Die höhere Zahl an Treffern kommt zustande, wenn neben dem Titel auch Zusammenfassung und Keywords durchsucht werden, jedoch werden in diesem Fall aus dem Literaturverzeichnis automatisch generierte, ggf. verfälschende Keywords (vgl. ISI 2000, 3), ebenfalls durchsucht.

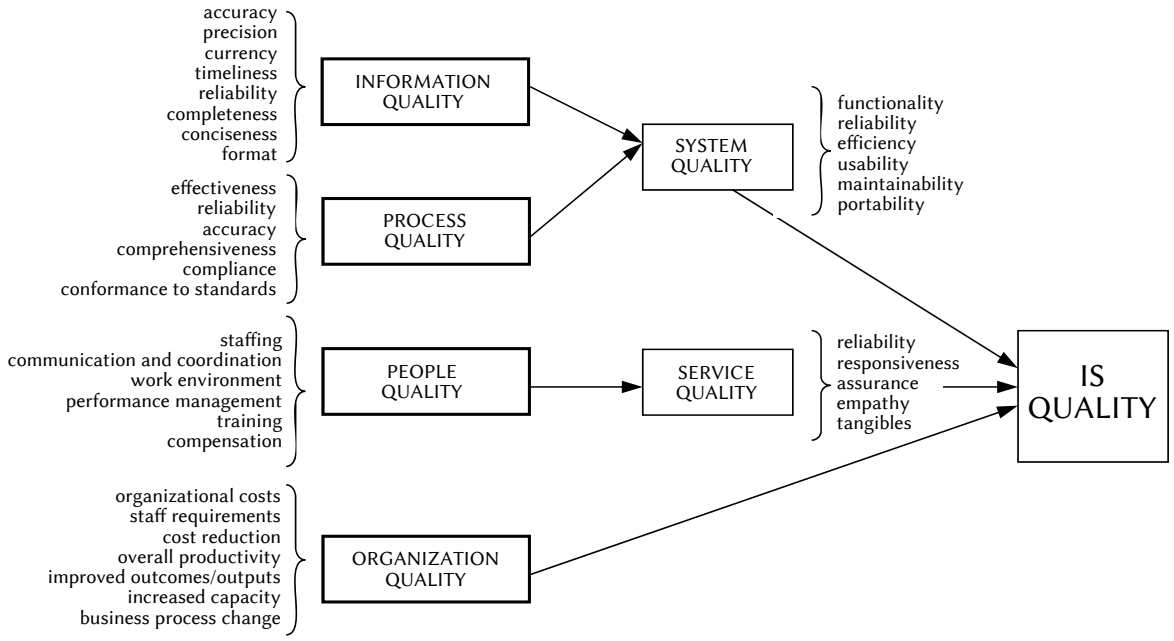


Abbildung 3-6: Modell zur Qualität von Informationssystemen (Quelle: Rodríguez/Casanovas 2010)

lität, Pünktlichkeit, Zuverlässigkeit, Vollständigkeit, Prägnanz, Input- und Outputformat und Relevanz (vgl. Bailey/Pearson 1983).

System quality Qualität des eigentlichen Informationssystems, welche auch als Produktqualität bezeichnet werden kann. Die Messungen erfolgen in Bezug auf Funktionalität, Zuverlässigkeit, Effizienz, Benutzerfreudlichkeit, Wartbarkeit und Portabilität (vgl. Chutimaskul et al. 2008; Franch/Carvallo 2003).

Service quality Qualität des Dienstleister-Supports. Die Kategorien sind aus dem von Parasuraman et al. (1988) entwickelten SERVQUAL-Ansatz zur Messung der Dienstleistungsqualität abgeleitet. Diese lauten Zuverlässigkeit, Antwortverhalten (im Sinne von Kundenfreundlichkeit), Auftreten, Einfühlungsvermögen und äußeres Erscheinungsbild (vgl. Pitt et al. 1995).

Process quality Qualität des Prozesses, das Informationssystem zu entwickeln und zu betreiben. Die Messgrößen wurden vom „Capability Maturity Model Integration for Development“ (CMMI-DEV 2006) des „Software Engineering Institute“ und von Urbach et al. (2009) abgeleitet. Die Größen lauten Effektivität, Zuverlässigkeit, Fehlerfreiheit, Umfang, Compliance und Standardkonformität.

Organization quality Qualität aus organisatorischer Sicht. Abgeleitet vom Ansatz von Sedera et al. (2004): Organisatorische Kosten, Personalbedarf, Kostenreduktion, Produktivität, verbesserter Erfolg/Output, mehr Kapazität und Geschäftsprozessanpassungen.

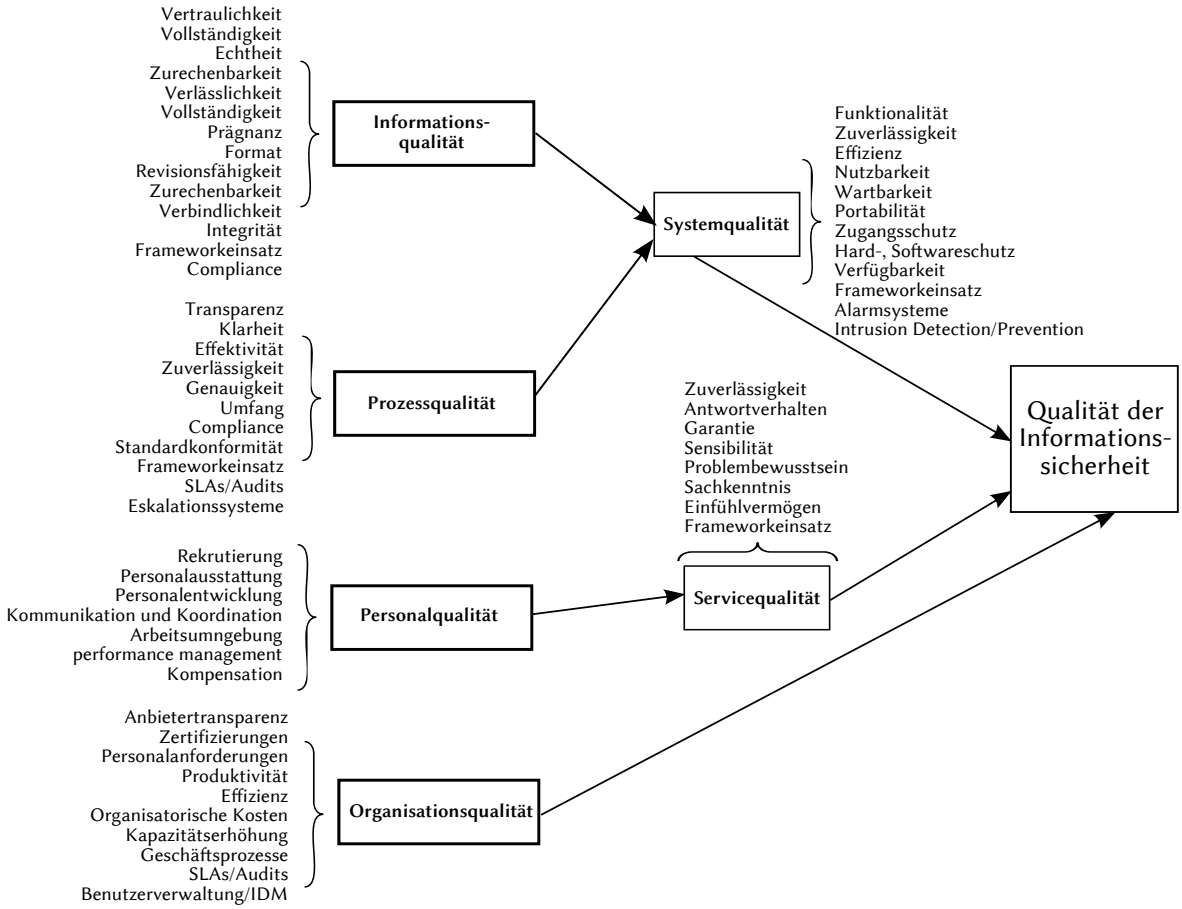


Abbildung 3-7: Hypothetisches Modell zur Informationssicherheit im Cloud-Computing

People quality Qualität der Stakeholder, die an allen Phasen des Lebenszyklus' beteiligt sind. Abgeleitet vom „People Capability Maturity Model" (P-CMM 2001). Darunter fallen Stellenbesetzung, Kommunikation und Koordination, Arbeitsumgebung, Leistungsmanagement, Aus- und Fortbildung und Vergütung.

3.3 Hypothetisches Modell zur Informationssicherheit im Cloud-Computing

Das Modell von Rodríguez/Casanovas wird nun an die Informationssicherheit im Cloud-Computing angepasst. Wie oben angedeutet wurde, ist die Informationssicherheit ein Qualitätsmerkmal (vgl. Zapf 2007), daher können ähnliche Kriterien angesetzt werden.

Die beeinflussenden Faktoren zur Informationssicherheit werden zunächst aus dem Modell von Rodríguez/Casanovas übernommen (Abbildung 3-7). Die Informationsqualität wird beispielsweise durch den Aspekt „Klassifikation der Daten" beeinflusst. Die zugrundeliegende Hypothese lautet: Wird eine sorgfältige Klassifikation vorgenommen, wirkt sich dies positiv auf die Systemqualität und dadurch auf die Informationssicherheit aus. Die Systemqualität wird von anderen Faktoren wie etwa „Zugangsschutz" beeinflusst.

Diese Argumentation ist analog auf die Prozessqualität anwendbar: wenn z.B. die Prozesse eines Cloud-Anbieters transparent sind, wirkt sich dies positiv auf die Prozessqualität aus.

Weiterhin beeinflusst die Personalqualität über die Servicequalität die Informationssicherheit. Gemeint sind Aspekte wie: „Der Cloud-Dienstleister achtet darauf welche Mitarbeiter eingestellt werden“. Dies wirkt sich positiv auf die Servicequalität aus. Sie hat wiederum Einfluss auf die Informationssicherheit.

Die Organisationsqualität wirkt sich direkt auf die Informationsqualität aus. Hier fließen Aspekte wie z.B. das Identitätsmangement oder die Anbietertransparenz mit ein.

4 Empirische Studie zur Informationssicherheit im Cloud-Computing

Im Rahmen des empirisch forschenden Teils dieser Arbeit wurden Unternehmen zum Thema „Informationssicherheit im Cloud-Computing“ befragt. Im folgenden wird die Entwicklung eines Fragebogens beschrieben, der den Stellenwert der Informationssicherheit beim Cloud-Computing in Unternehmen abbilden soll. Anschließend wird mit Hilfe deskriptiver (beschreibender) Statistik die Stichprobe analysiert. Im darauffolgenden, induktiven (schließenden) Teil werden die Hypothesen bzw. das entwickelte Modell überprüft.

4.1 Untersuchungsdesign/Fragebogen

Der Fragebogen ist in unterschiedliche Blöcke gruppiert. Die Blöcke bestehen aus verschiedenen Themenbereichen wobei die Reihenfolge so gewählt wurde, dass die allgemeineren Fragen, die i.d.R. einfacher zu beantworten sind, weiter vorne im Fragebogen erscheinen. In Abbildung 4-1 ist der Aufbau des Fragebogens dargestellt. Ein vollständiger Fragebogen befindet sich im Anhang auf Seite 84.

Versandt wurde der Fragebogen per Brief an 560 CIOs deutscher Unternehmen. Parallel dazu wurde in mehreren geschlossenen CIO-, bzw. Cloud-Computing-Diskussionsgruppen des sozialen Netzwerks „XING“ (2011) um die Teilnahme an diesem Fragebogen geworben. Somit ergaben sich weit über 1000 potentielle Teilnehmer. Die Rücklaufquote der per Brief verschickten Fragebogen betrug 9,5%. Für die Onlineversion konnten 15 Teilnehmer gewonnen werden. Insgesamt waren 66 Rückläufer auswertbar.

Die Anonymität wurde durch einen beigelegten (anonymen) Rücksendeumschlag gewahrt. Um die Anonymität durch die Angabe einer Empfangs-E-Mailadresse für die Ergebnisse der Studie nicht zu gefährden, wurde die Möglichkeit gegeben, die Adresse unabhängig vom Fragebogen mitzuteilen.

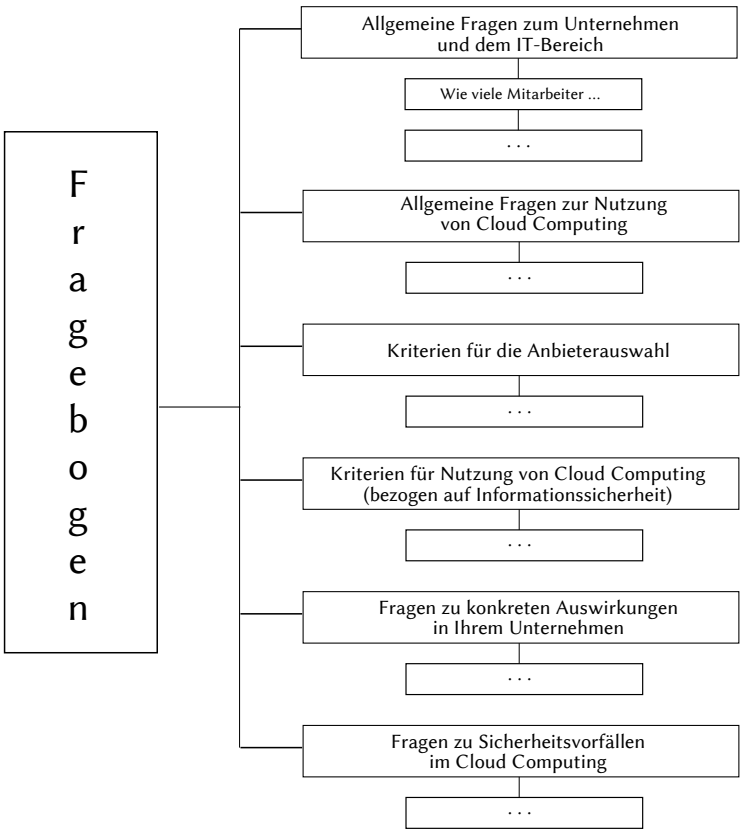


Abbildung 4-1: Gliederung des Fragebogens

4.2 Deskriptive Statistik

Deskriptive Statistik kann empirisch erhobene Daten — mit Hilfe von Graphiken und Charakterisierungen durch Kennzahlen — verdichtet und übersichtlich darstellen. Um später das entwickelte Modell schätzen und testen zu können, müssen die erhobenen Daten zunächst beschrieben und gemessen werden (vgl. Mosler/Schmid 2006, 5f.). Aus diesem Grunde geht die deskriptive Statistik der induktiven voraus.

4.2.1 Fragenblock 1: Allgemeine Fragen zum Unternehmen und dem IT-Bereich

Die Stichprobe setzt sich zum größten Teil aus größeren Unternehmen mit mindestens 5000 Vollzeitstellen oder einem Umsatz von mindestens 500 Mio. € zusammen (Abbildung 4-2). Mittelständische Unternehmen mit weniger als 500 Mitarbeitern bzw. einem Jahresumsatz von weniger als 50 Mio. € bilden eine Minderheit von 21% bzw. 16%. 41% der befragten Unternehmen beschäftigen mindestens 5000 Angestellte bzw. 56% haben einen Umsatz von mindestens 500 Mio. €.

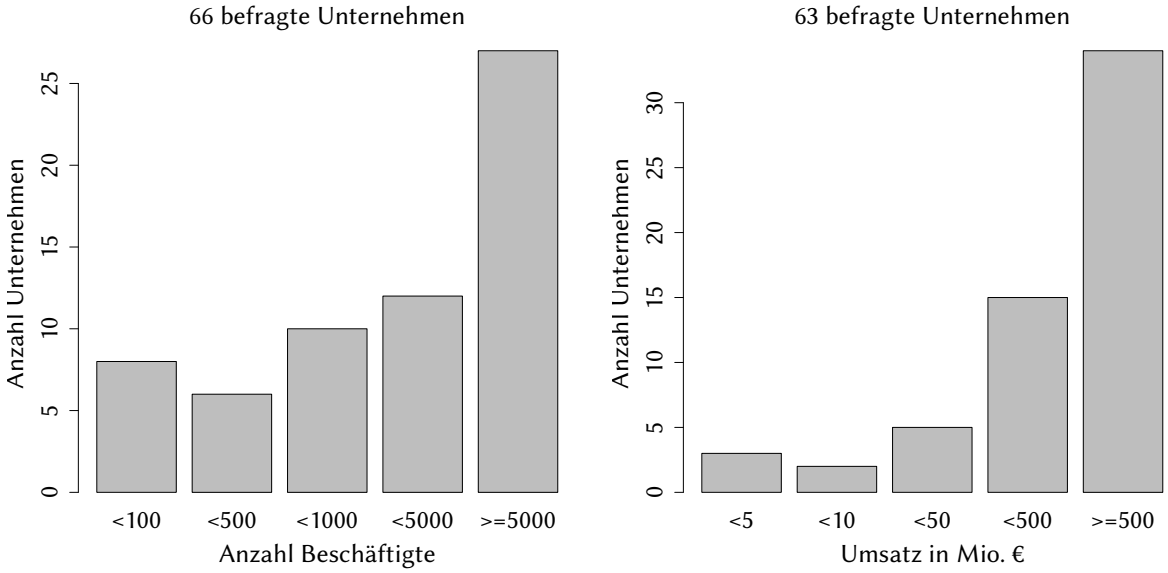


Abbildung 4-2: Unternehmensgröße

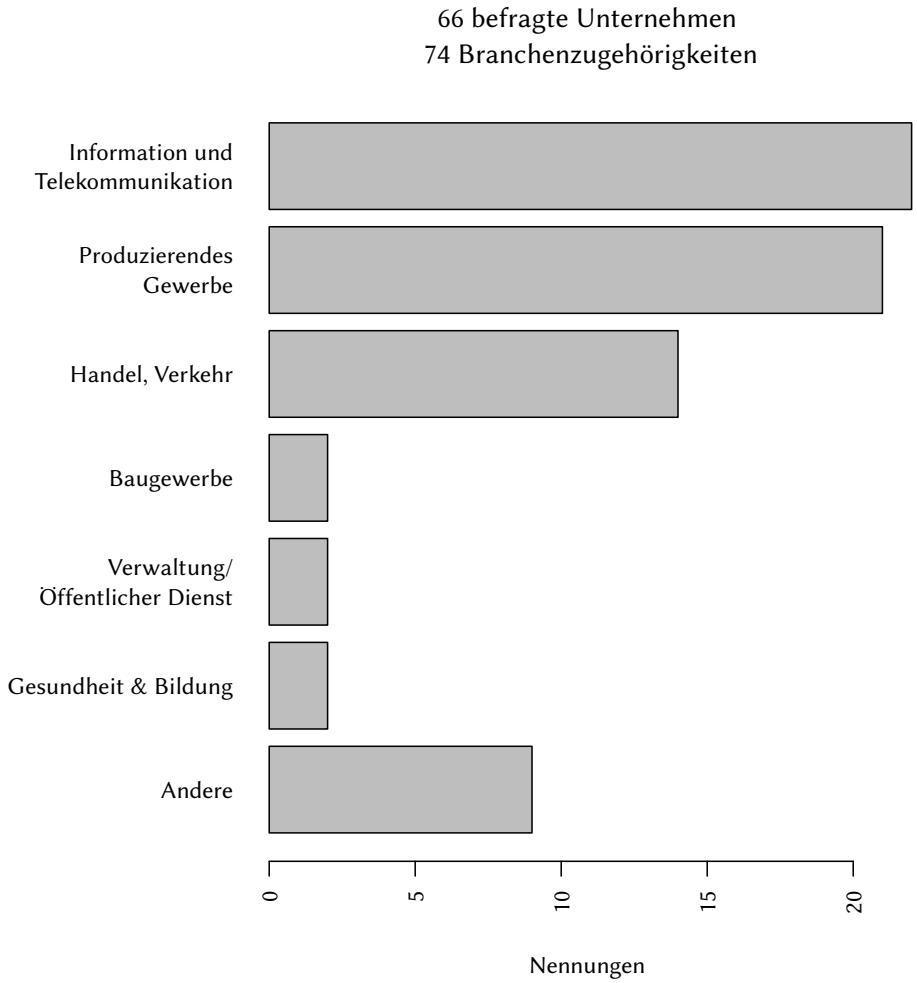


Abbildung 4-3: Branchenzugehörigkeit

Die Branchenzugehörigkeit der Unternehmen, die an der Befragung teilgenommen

haben, gliedert sich wie folgt: Die Branchen Information/Telekommunikation, Produzierendes Gewerbe und Handel/Verkehr bilden mit 77% der gesamten Nennungen den dominierenden Teil (Abbildung 4-3).

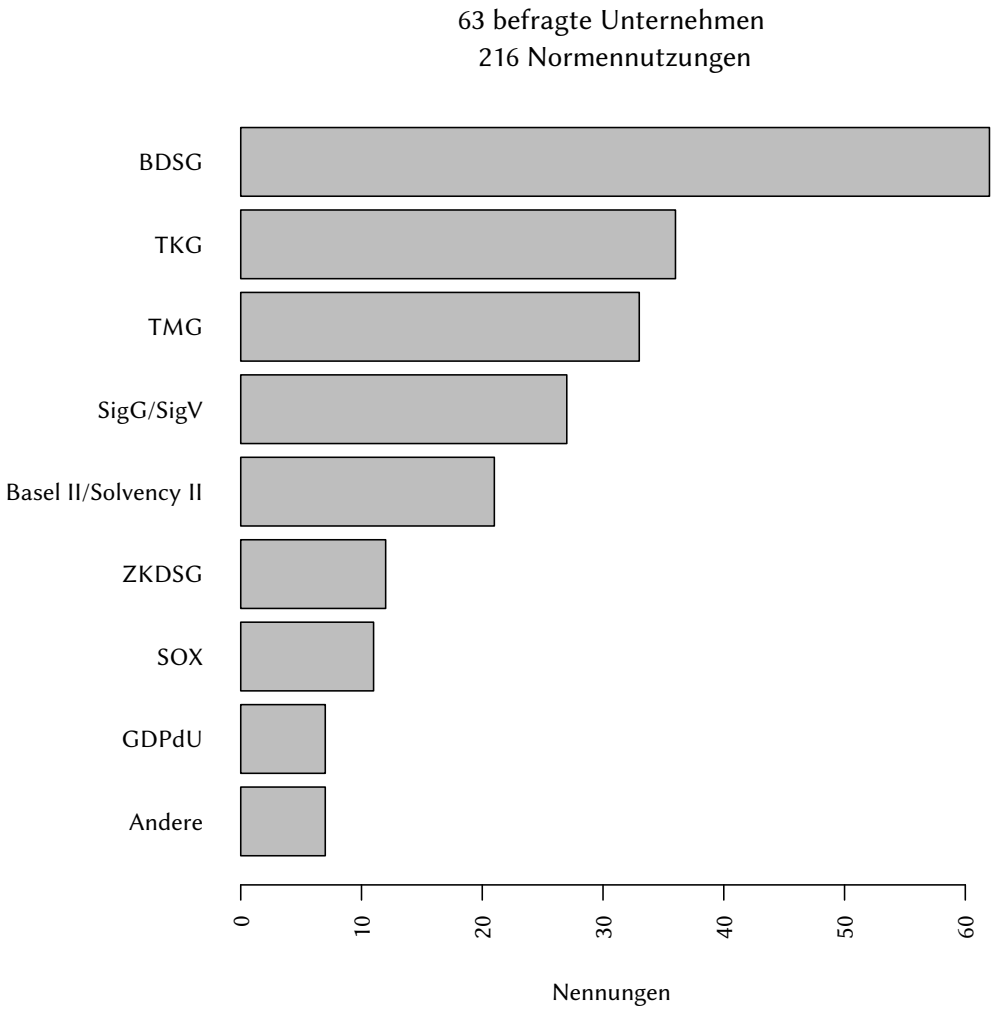


Abbildung 4-4: Normen

Bei den eingesetzten Normen und Gesetzen, die von den teilnehmenden Unternehmen eingesetzt bzw. beachtet werden, ist das Bundesdatenschutzgesetz mit 29% am weitesten verbreitet. Zusammen mit Telekommunikationsgesetz, Telemediengesetz und Signaturgesetz ergeben sich dadurch über 70% (Abbildung 4-4).

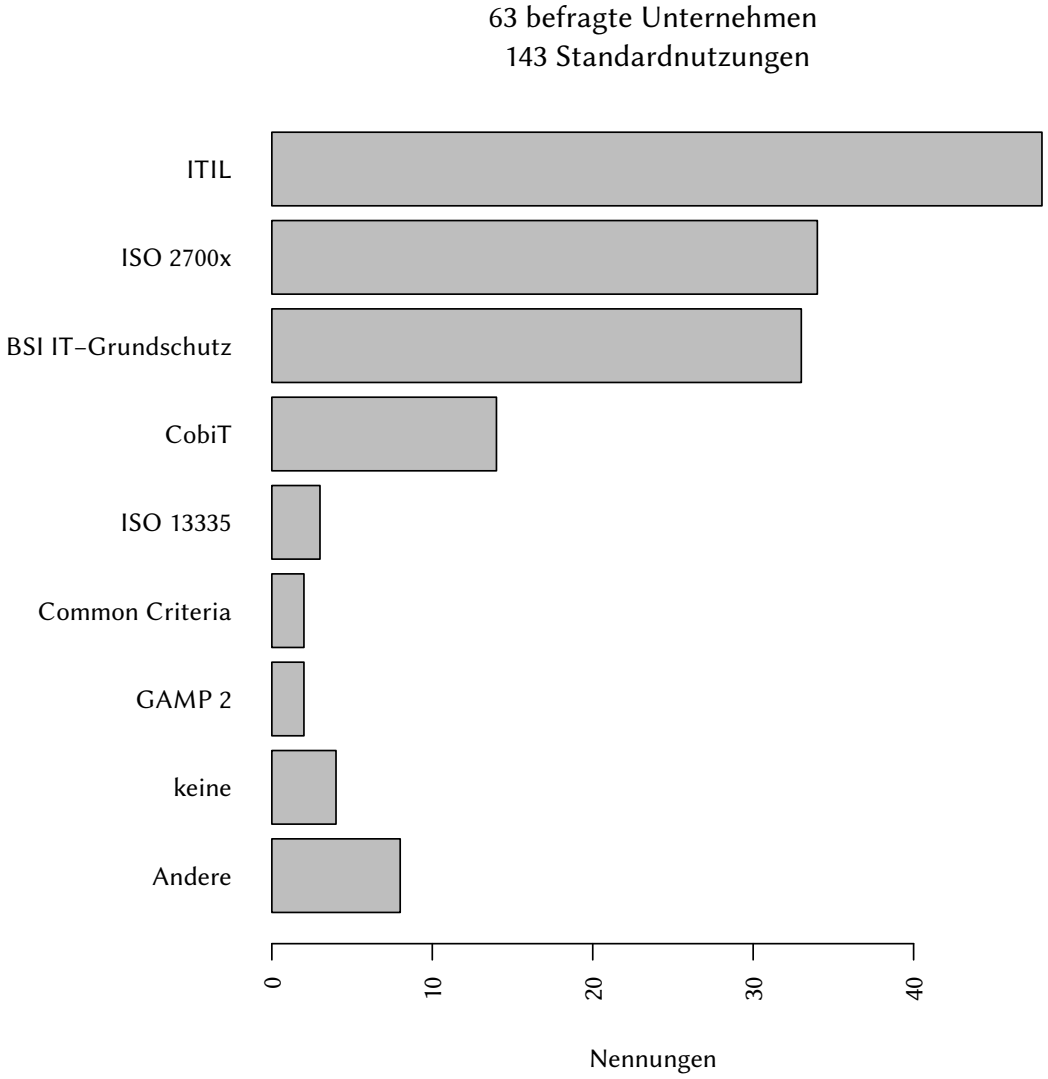


Abbildung 4-5: Standards und Frameworks

Bei den eingesetzten Standards ist ITIL mit 34% am weitesten verbreitet. Zusammen mit der Standard-Familie ISO 27000 f., dem IT-Grundschutz und dem CobiT-Framework ergeben sich 90% (Abbildung 4-5).

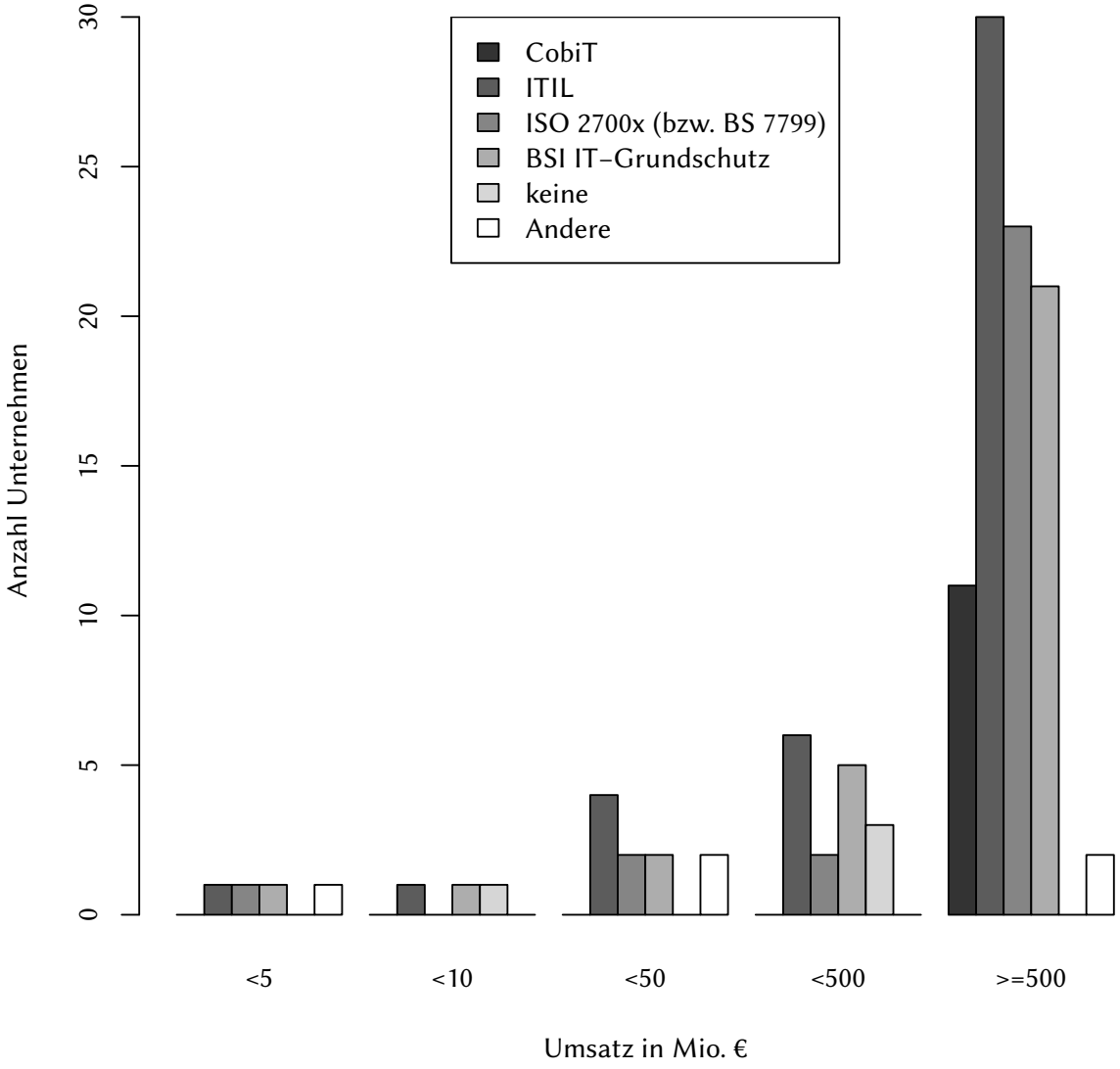


Abbildung 4-6: Standards in Abhängigkeit vom Umsatz

Das CobiT-Framework sticht dahingehend hervor, dass es nur bei großen Unternehmen mit einem Jahresumsatz von mindestens 500 Mio. € eingesetzt wird. Abbildung 4-6 veranschaulicht dies.

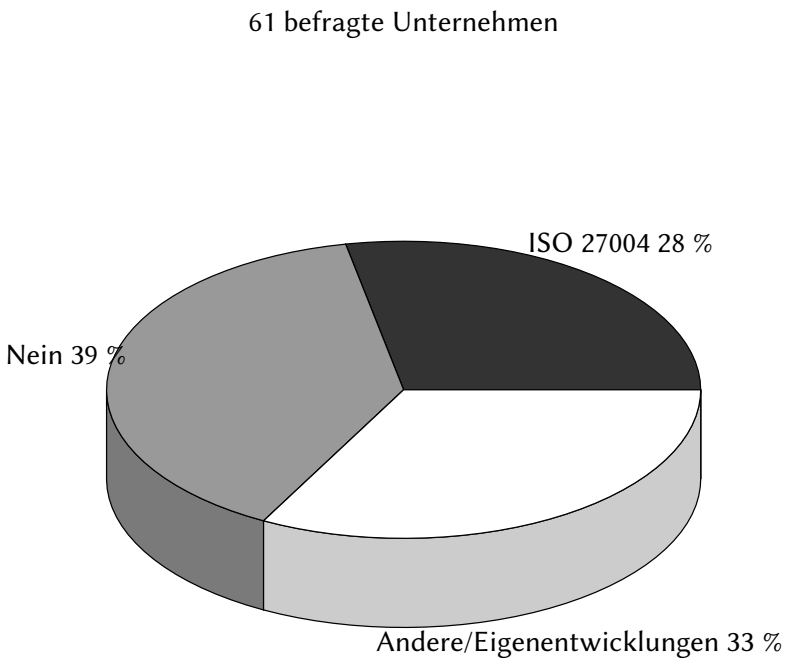


Abbildung 4-7: Controlling der Informationssicherheit

Abbildung 4-7 zeigt den Einsatz von Standards, die das Controlling bzw. den Reifegrad oder auch Effizienz und Effektivität der Informationssicherheit zum Ziel haben. Auffällig ist hierbei, dass 39% der befragten Unternehmen auf ein Controlling der Informationssicherheit verzichten. Neben dem Standard ISO 27004 ließ sich kein mehrfacher Einsatz von anderen Standards oder Frameworks erkennen. Eigenentwicklungen sind in diesem Bereich weit verbreitet.

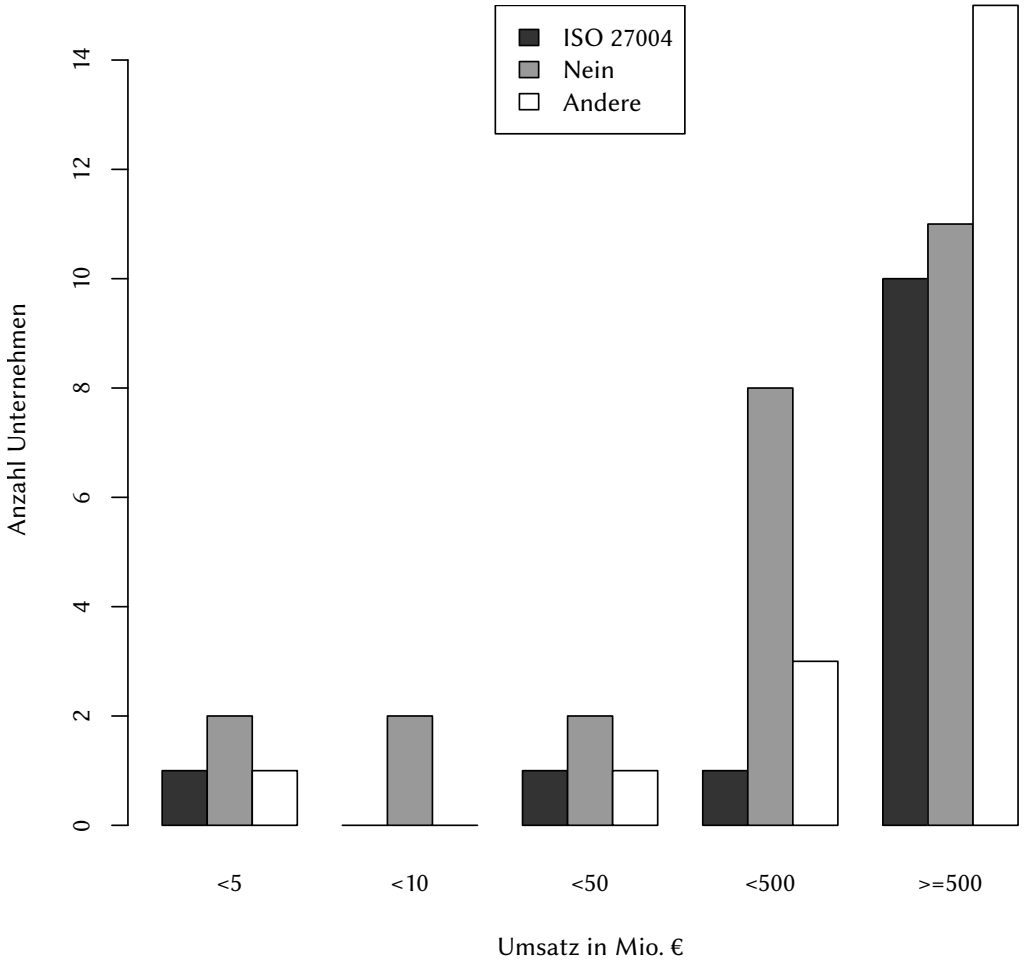


Abbildung 4-8: Controlling in Abhängigkeit vom Umsatz

Abbildung 4-8 zeigt, ob und wie ein Controlling der Informationssicherheit stattfindet. Der Verzicht auf das Controlling der Informationssicherheit gilt insbesondere für Unternehmen mit einem Umsatz weniger als 500 Mio. Euro.

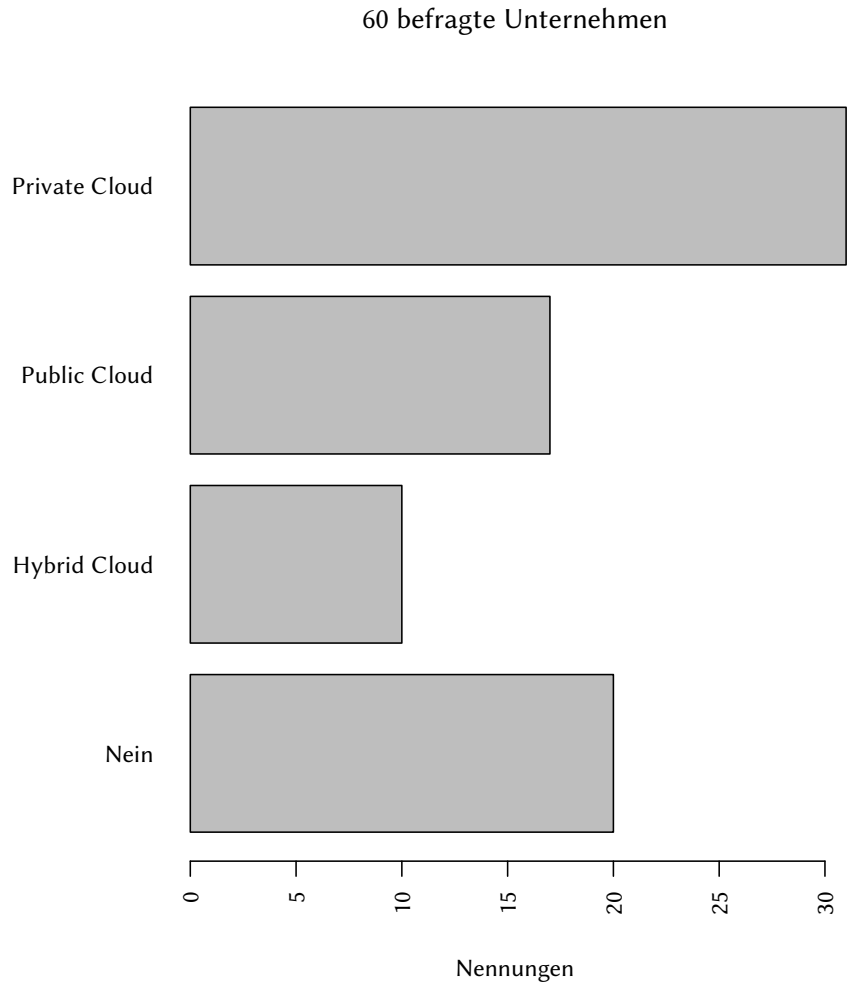


Abbildung 4-9: Cloud-Infrastrukturen

4.2.2 Fragenblock 2: Allgemeine Fragen zur Nutzung von Cloud-Computing

Von den befragten Unternehmen setzen zwei Drittel Cloud-Computing ein. Wobei die Private-Cloud mit 53% die am häufigsten eingesetzte Nutzungsform darstellt (Abbildung 4-9).

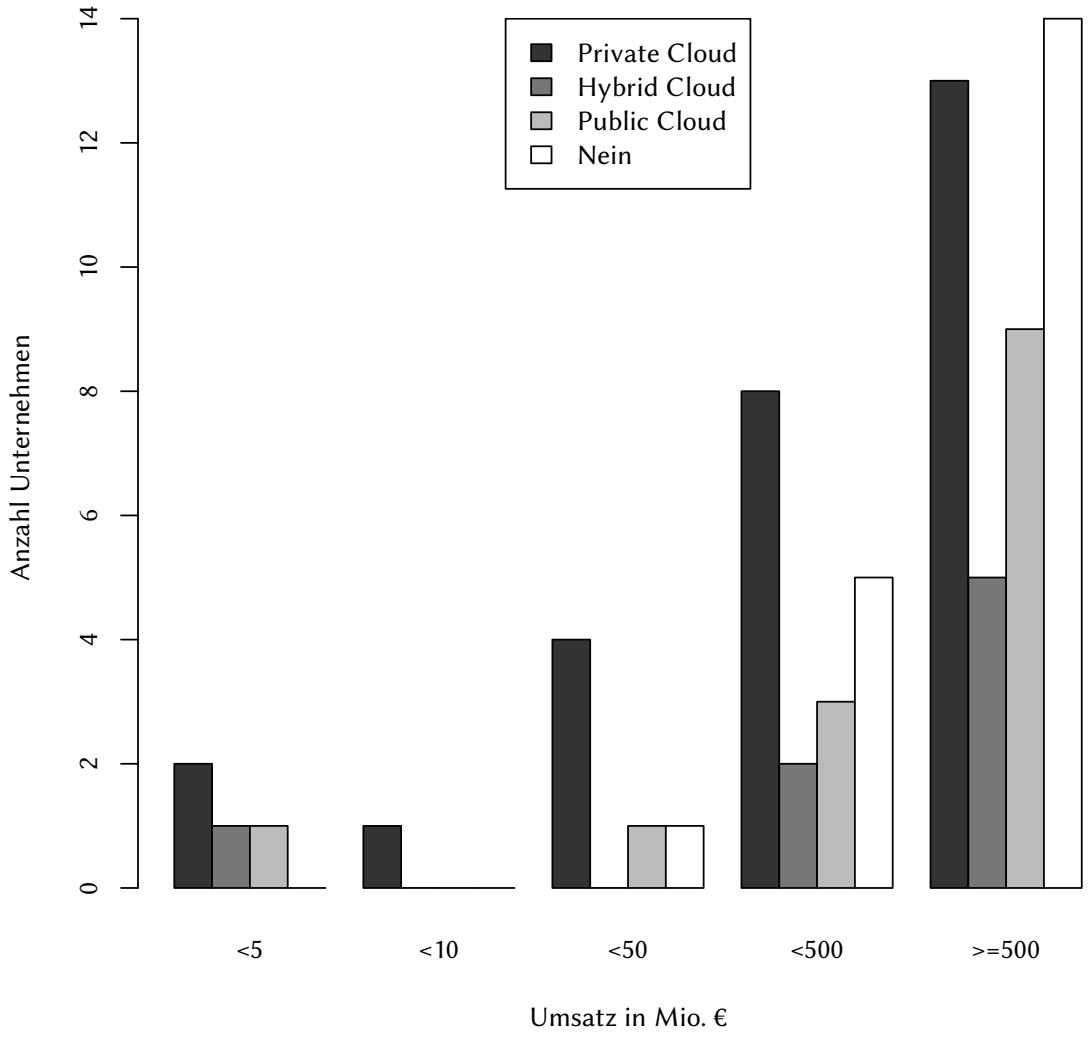


Abbildung 4-10: Cloud-Infrastrukturen in Abhängigkeit vom Umsatz

Die Häufigkeit des Einsatzes und die Verteilung der verschiedenen Nutzungsformen scheint unabhängig von der Größe der Unternehmen zu sein (Abbildung 4-10).

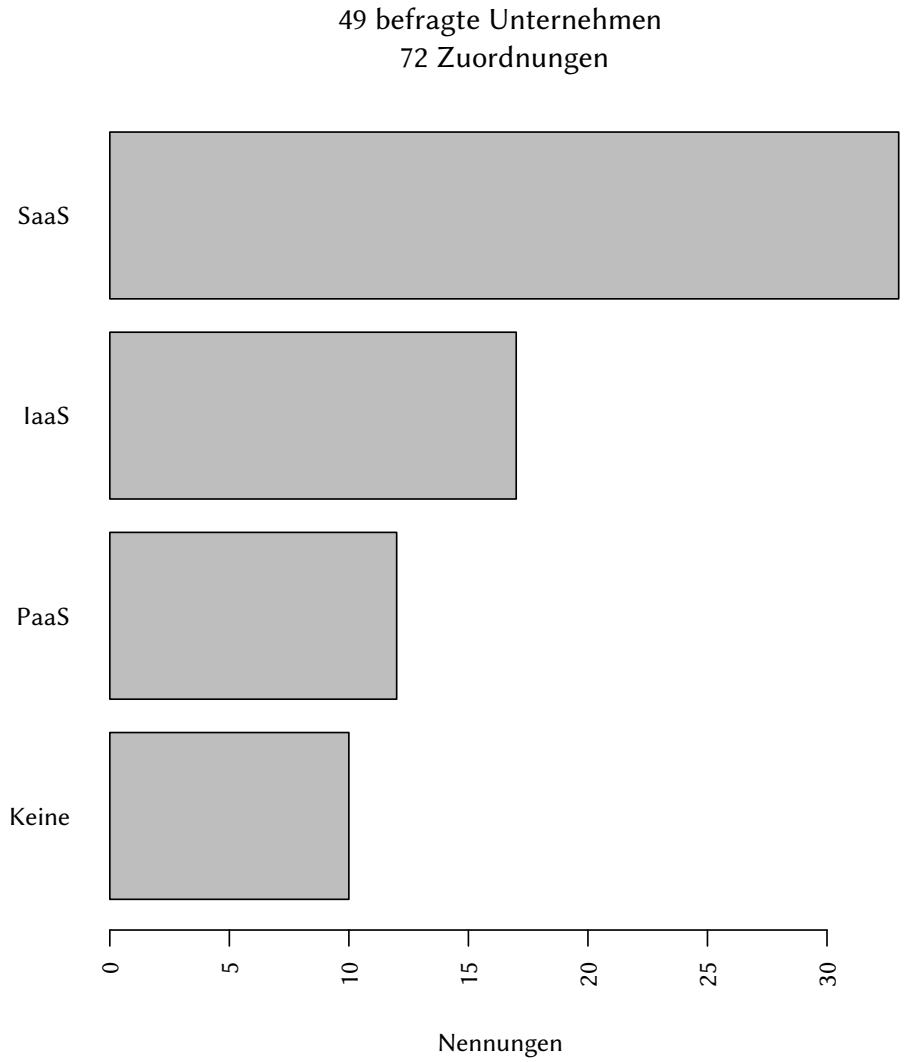


Abbildung 4-11: Cloud-Nutzungsformen

Bei den unterschiedlichen Nutzungsformen ist SaaS mit einem Anteil von 53% am stärksten repräsentiert (Abbildung 4-11).

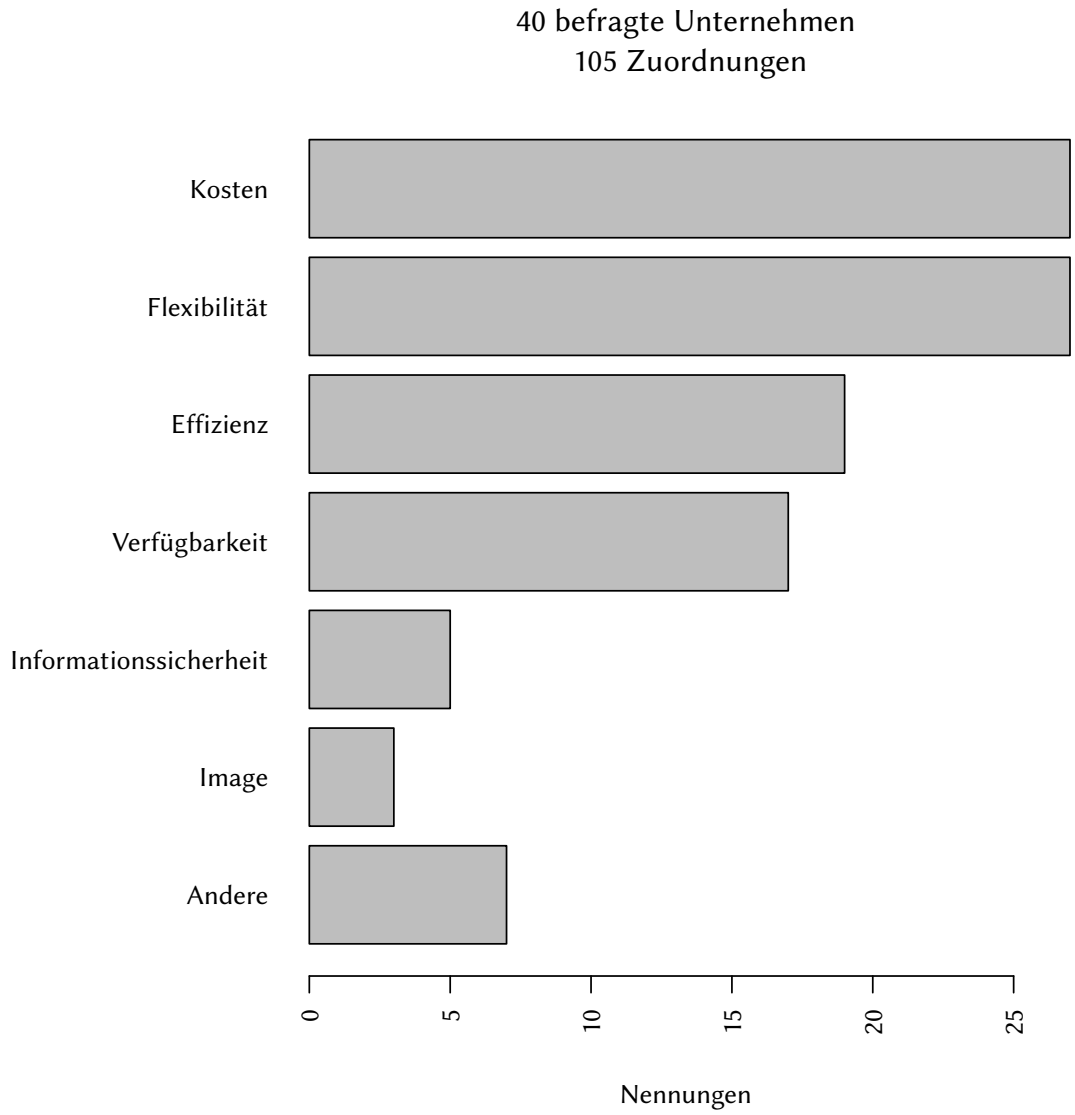


Abbildung 4-12: Gründe für die Nutzung von Cloud-Computing

Die Gründe für die Nutzung von Cloud-Computing sind in erster Linie Kostenreduktion und Flexibilität, aber auch die erhöhte Effizienz und Verfügbarkeit spielen eine wichtige Rolle (Abbildung 4-12). Zusammen machen die vier genannten Aspekte 86% der gesamten Nennungen aus.

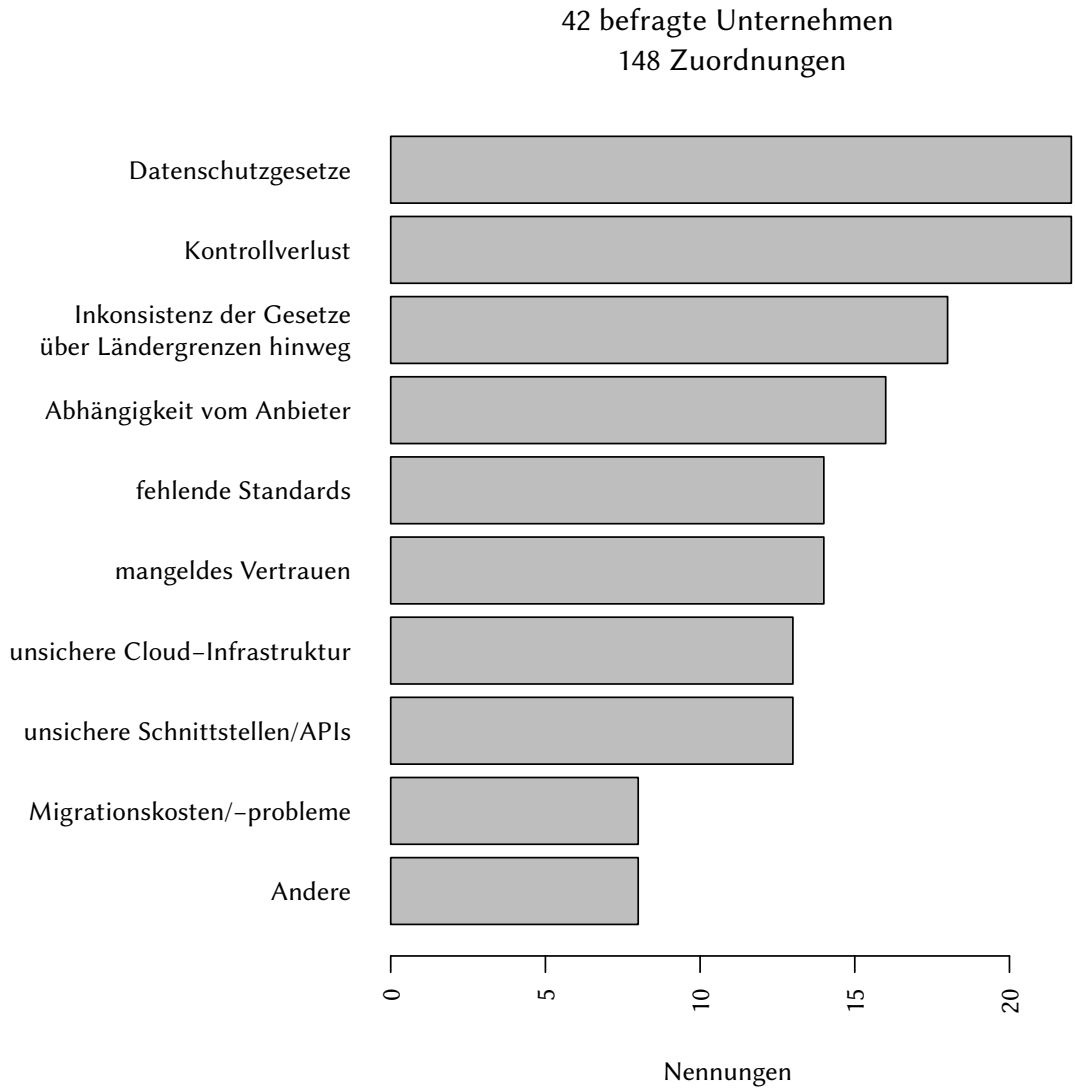


Abbildung 4-13: Ablehnungsgründe für den Einsatz von Cloud-Computing

Der mit dem Einsatz von Cloud-Computing einhergehende Kontrollverlust und die Datenschutzgesetze sind die Hauptgründe, die gegen den Einsatz von Cloud-Computing sprechen. Insgesamt sind die Ablehnungsgründe vielfältig verteilt (Abbildung 4-13).

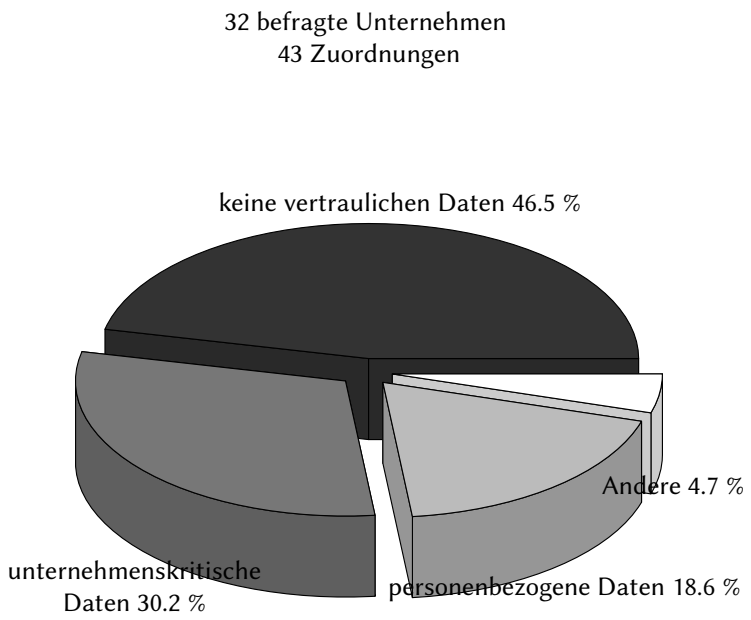


Abbildung 4-14: Datenarten im Cloud-Computing

Die Verteilung der in der Cloud genutzten Daten ist aus Abbildung 4-14 ersichtlich. Fast 50% der Daten sind als unternehmenskritisch bzw. personenbezogen einzustufen.

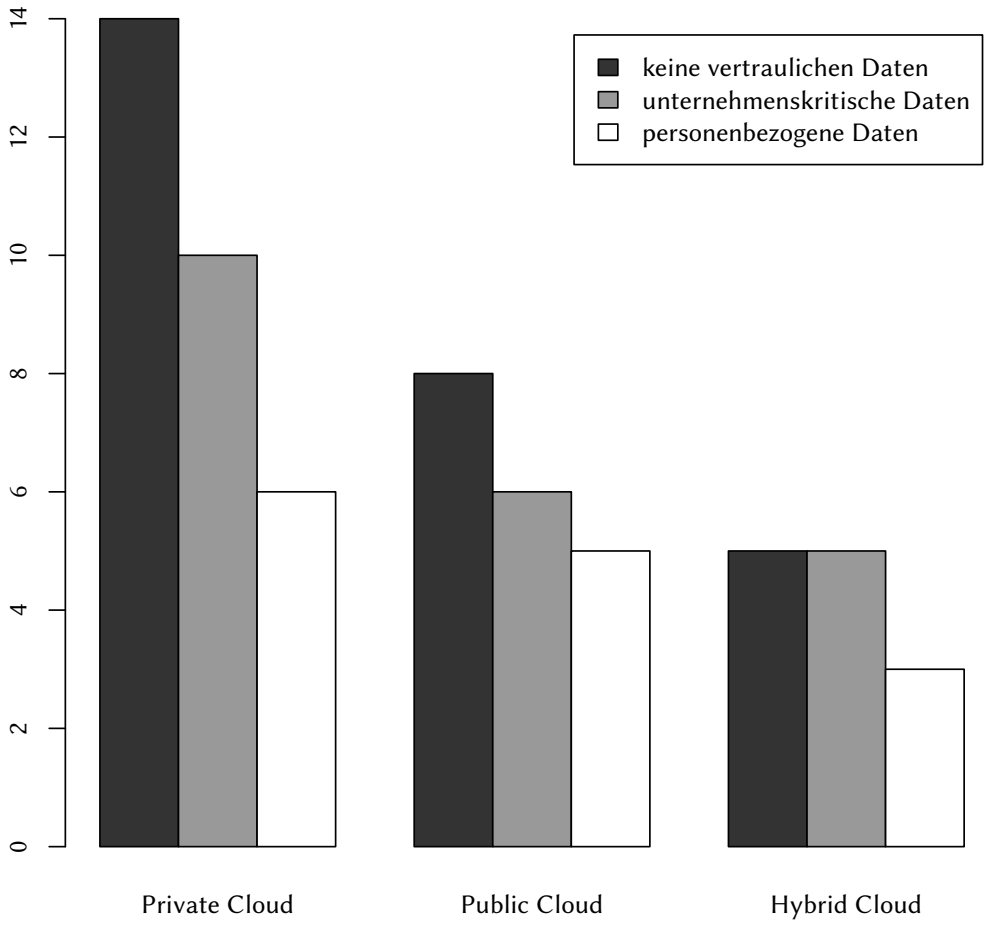


Abbildung 4-15: Datenarten in Abhängigkeit der Infrastrukturform

Wenn die Verteilung gemeinsam mit den einzelnen Nutzungsformen betrachtet wird, ist kein Zusammenhang erkennbar (Abbildung 4-15). Es wäre denkbar gewesen, dass personenbezogene Daten vorwiegend in Private Clouds genutzt werden.

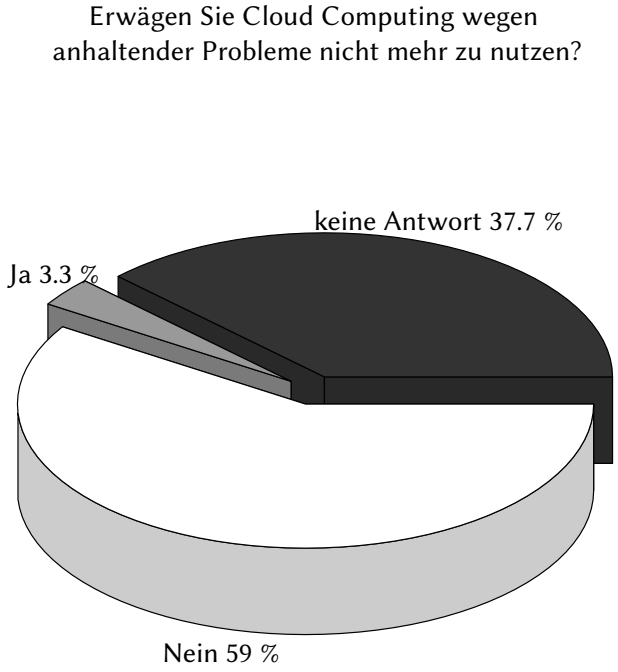


Abbildung 4-16: Nutzung von Cloud-Computing beenden

Nur wenige Unternehmen erwägen wegen negativer Erfahrungen mit Cloud-Computing die Nutzung zu beenden (Abbildung 4-16). 59% wollen die Nutzung beibehalten. Beachtlich ist der Prozentsatz an Teilnehmern, der diese Frage nicht beantwortet hat. Dies resultiert weitgehend daraus, dass Cloud-Nichtnutzer diesen Teil des Fragebogens übersprungen haben.

4.2.3 Fragenblock 3: Kriterien für die Anbieterauswahl

Im dritten Block konnten die meisten Fragen mit Bewertungen auf einer fünfstufigen Ordinalskala von unwichtig bis wichtig beantwortet werden. Diese Skala wird auch „Likert-Skala“ (vgl. Bortz/Döring 2009, 224) oder Rangplatzskala genannt (vgl. Eckstein 2010, 25). Bei ausreichender Differenzierung, symmetrischer und äquidistanter Formulierung können diese Skalen als (metrische) Intervallskalen interpretiert werden (vgl. Oppl 2010, 347). Dies ermöglicht die Nutzung von „Box-Whisker-Plots“ (kurz: „Boxplots“) zur aggregierten Darstellung der Antworten. Mit Hilfe von Boxplots können metrische Daten in besonders einfacher und anschaulicher Weise graphisch dargestellt werden (vgl. Mosler/Schmid 2005, 33). In den hier verwendeten Boxplots bezeichnen die Kreise die Ausreißer, die Enden der gestrichelten Linien („Whisker“) sind minimal bzw. maximal auftretende Werte. Die Box in der Mitte besteht aus den drei Quartilen[3], wobei der mittlere Strich den Median darstellt. Der Median ($\widetilde{x}_{0,5}$), auch als Zentralwert bezeichnet,

[3]Hier werden Boxplots mit der Funktion „boxplot“ aus dem Statistikpaket „R“ dargestellt. Diese Funktion verwendet beim ersten Quartil den sogenannten unteren „hinge“ und beim dritten Quartil den oberen „hinge“. Diese unterscheiden sich nicht wesentlich von den Quartilen (vgl. Groß 2010, 60).

ist der Wert, der die unteren 50% der Daten von den oberen 50% trennt und ist damit robust gegenüber ausreißern (vgl. Mosler/Schmid 2005, 32f.). Das Quantil $\widetilde{x}_{0,25}$ bezeichnet man als unteres Quartil, $\widetilde{x}_{0,75}$ als oberes Quartil. Die Quartile $\widetilde{x}_{0,25}$, $\widetilde{x}_{0,5}$, $\widetilde{x}_{0,75}$ teilen die Daten in vier Blöcke, die jeweils 25% der Daten umfassen. Die Verteilung der Antworten wird so veranschaulicht.

14. Transparenz des Anbieters
15. Zertifizierungen/externe Audits des Anbieters
16. Mehrstufige Authentifizierungen
17. Wie und welche Mitarbeiter der Anbieter einstellt
18. Überprüfung der physischen Sicherheit des Anbieters (Zugangs- und Katastrophenschutz)
19. Regelungen, wie bei Auflösung/Übernahme des Anbieters zu verfahren ist
20. Der Anbieter sollte Daten auf verschiedenen Sites vorhalten (Vorbeugung vor Datenverlust, Erhöhung der Verfügbarkeit)
21. Kontrollpflichten des Anbieters (z.B. über SLAs)
22. Prüfungsrechte des Kunden (z.B. über SLAs)
23. Dritte dürfen keinen Zugang zur Infrastruktur/Datenhaltung des Anbieters haben
24. Festlegung von Verantwortlichkeiten und Haftungen bei Sicherheitsvorfällen (z.B. über SLAs)
25. Konsequente Verschlüsselung von Daten, sodass nur sich in Bearbeitung befindliche Daten unverschlüsselt vorliegen
26. Reporting des Anbieters über Sicherheitsvorfälle (Informationspflicht nach § 42a BDSG)
27. Vom Anbieter versprochene Sicherheit muss nachvollziehbar sein
28. Vereinbarung klarer Prozesse im Fall von Datenverlusten
29. Physikalische Aufbewahrung der Daten ausschließlich innerhalb der EU

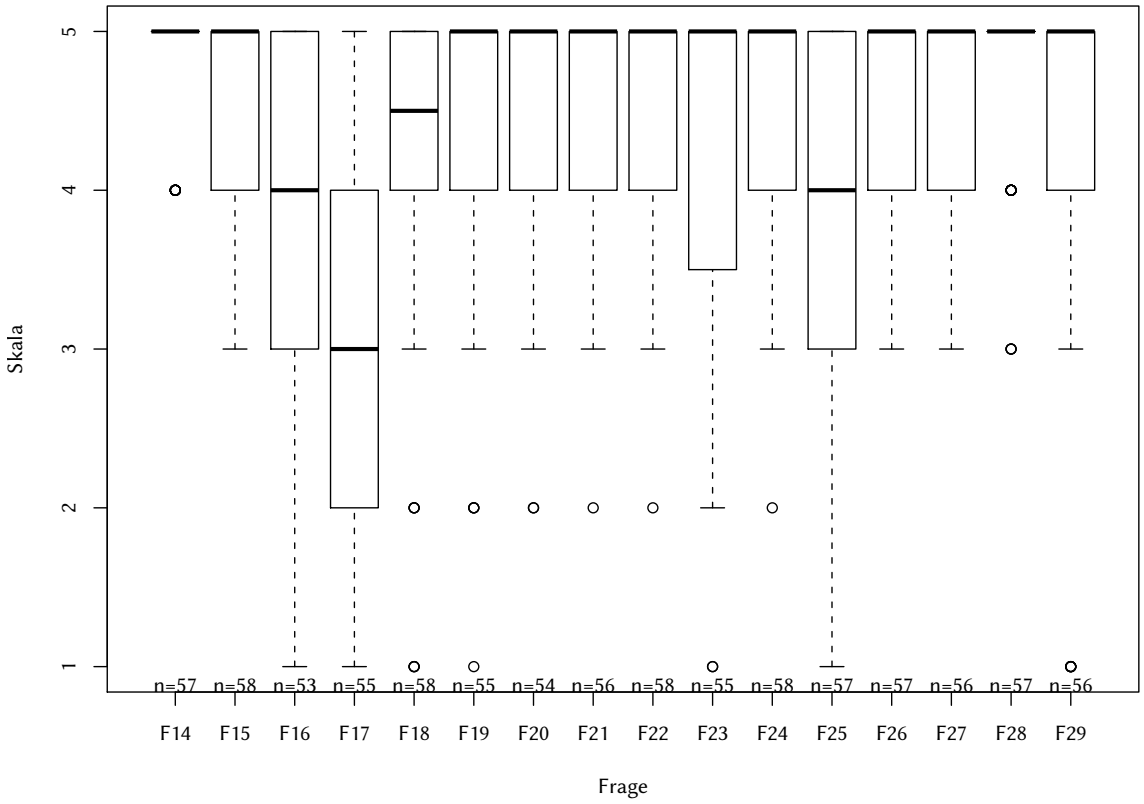


Abbildung 4-17: Boxplots der Fragen 14-29

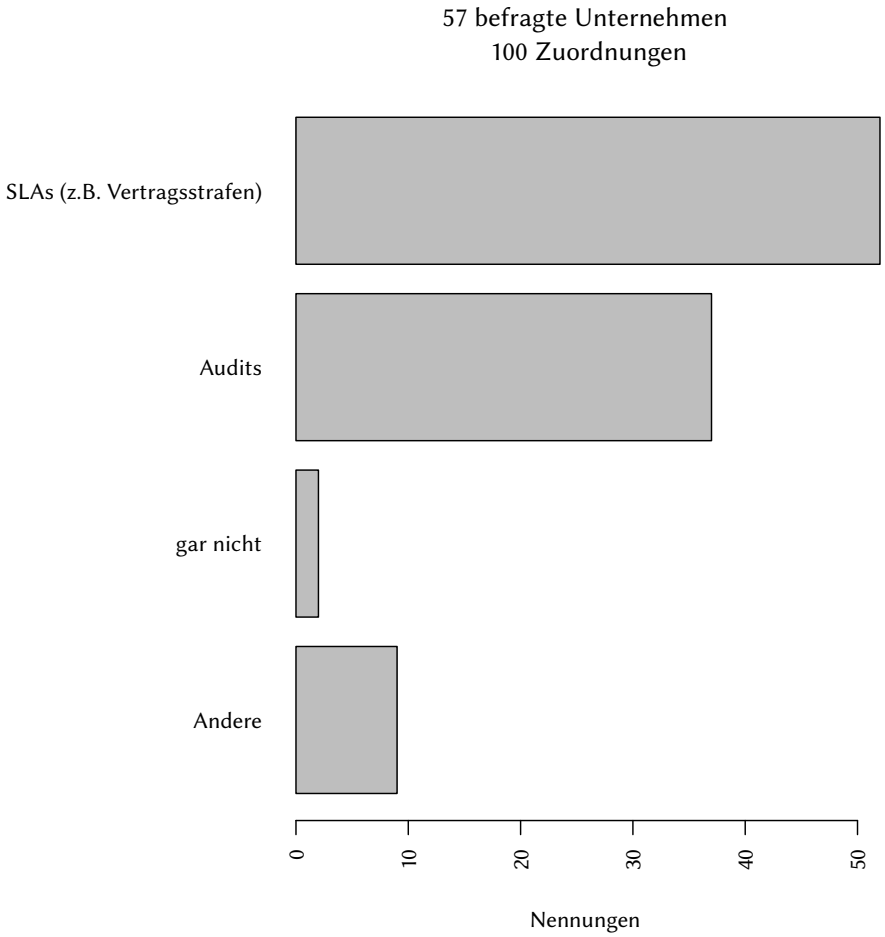


Abbildung 4-18: Sicherstellung des Vertrauens zum Cloud-Anbieter

Mit „wichtig“ wurden die Fragen 14 und 28 beantwortet (Abbildung 4-17). D.h. die Transparenz des Anbieters und die Vereinbarung klarer Prozesse im Fall von Datenverlusten haben die höchste Priorität. Neutral wird Frage 17 eingestuft, die einen Median von 3 hat.

Abbildung 4-18 zeigt, wie das Vertrauen zum Cloud-Anbieter sichergestellt wird. Das am häufigsten eingesetzte Mittel sind SLAs. Aber auch regelmäßige Audits sind weit verbreitet.

4.2.4 Fragenblock 4: Kriterien für die Nutzung von Cloud-Computing (bezogen auf Informationssicherheit)

Bei Frage 36 (Abbildung 4-19) tritt die Wichtigkeit der detallierten Regelung von Schadensszenarien deutlich hervor. Zusammen mit Frage 21, 22 und Abbildung 4-18 ergibt sich, dass sehr detallierte SLAs eine wichtige Rolle bei der Nutzung von Cloud-Computing spielen.

31. Berücksichtigung des Browsers (als Universalclient mit vielen Angriffspunkten)
32. Klassifikation von Daten mit Richtlinien zur Weitergabe/Löschung
33. Backups außerhalb des Cloud-Dienstleisters
34. Ausschließlich verschlüsselte Daten in die Public/Hybrid Cloud auslagern
35. Schulung der Mitarbeiter im Umgang mit Cloud-Computing und dessen Sicherheitsaspekten
36. Regelung möglichst aller Schadensszenarien (z.B. durch SLAs)

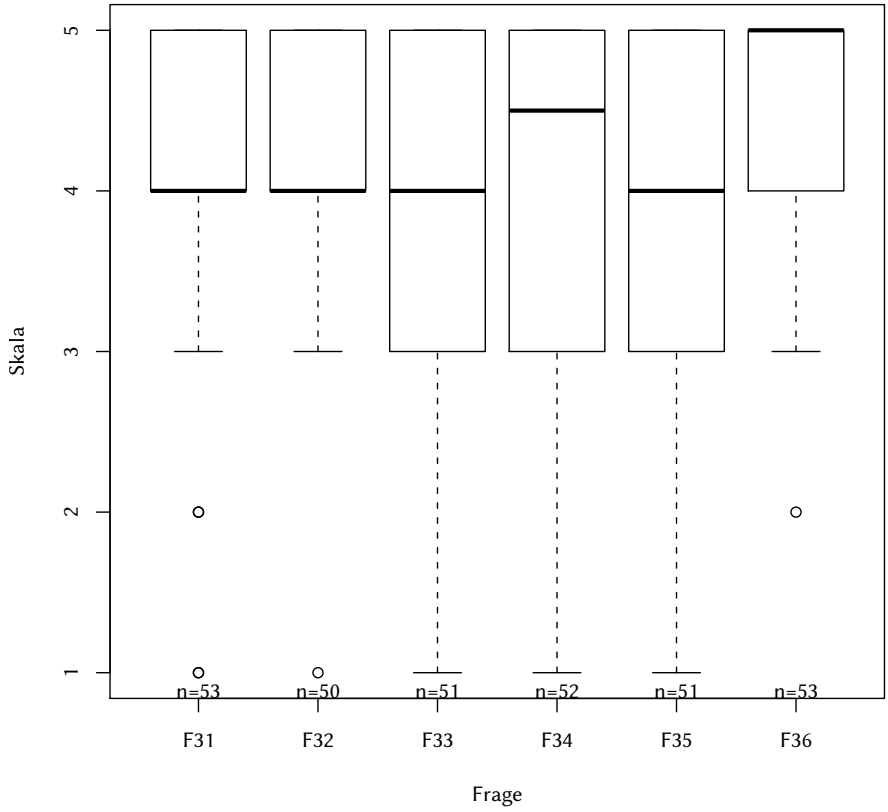


Abbildung 4-19: Boxplots der Fragen 31 bis 36

Der Browser ist als Universalclient für viele Anwendungen vermehrt Gefahren ausgesetzt. Häufig ist er auch für Anwendungen des Cloud-Computing im Einsatz. Daher findet er entsprechend Beachtung (Frage 31, Abbildung 4-19). Die Klassifikation von Daten (Frage 32) und Backups außerhalb des Cloud-Dienstleistern (Frage 33) sind ebenfalls wichtig, wobei es bei den externen Backups eine wesentlich größere Streuung gibt.

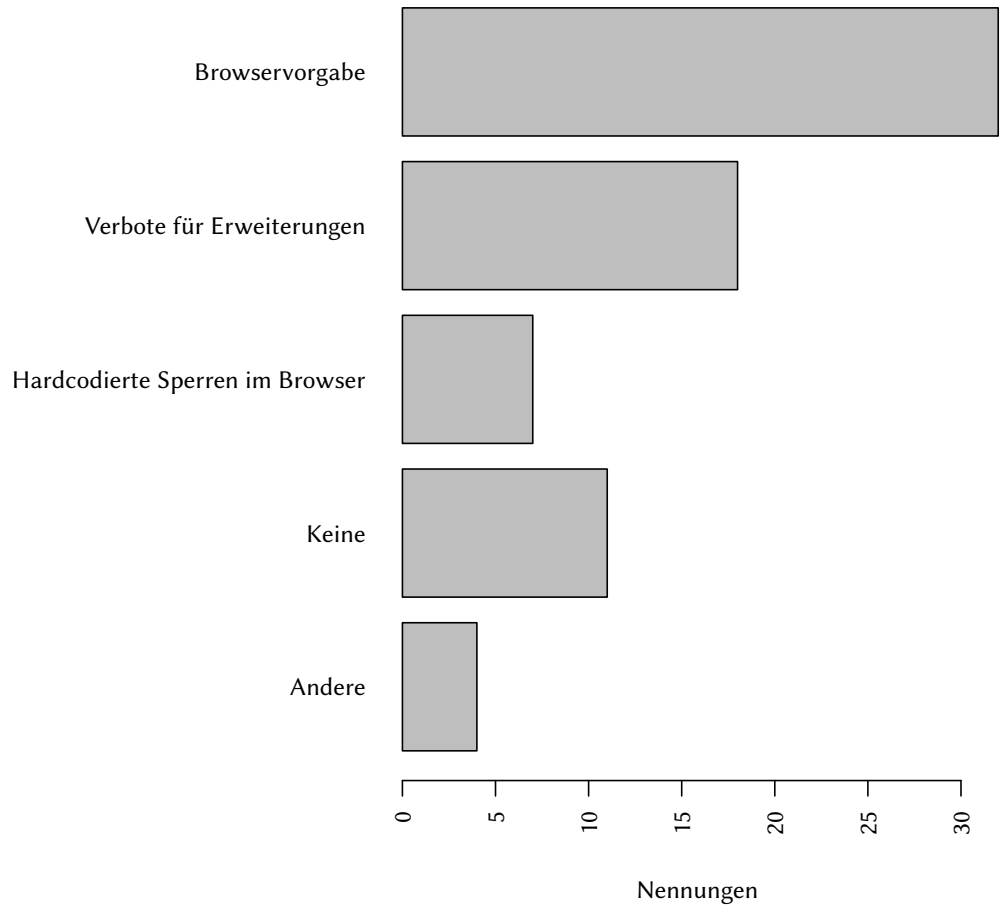


Abbildung 4-20: Browsersicherheit

Unternehmen sehen als effektivstes Mittel die Browsersicherheit zu erhöhen, die Vorgabe eines bestimmten Browsers an (Abbildung 4-20).

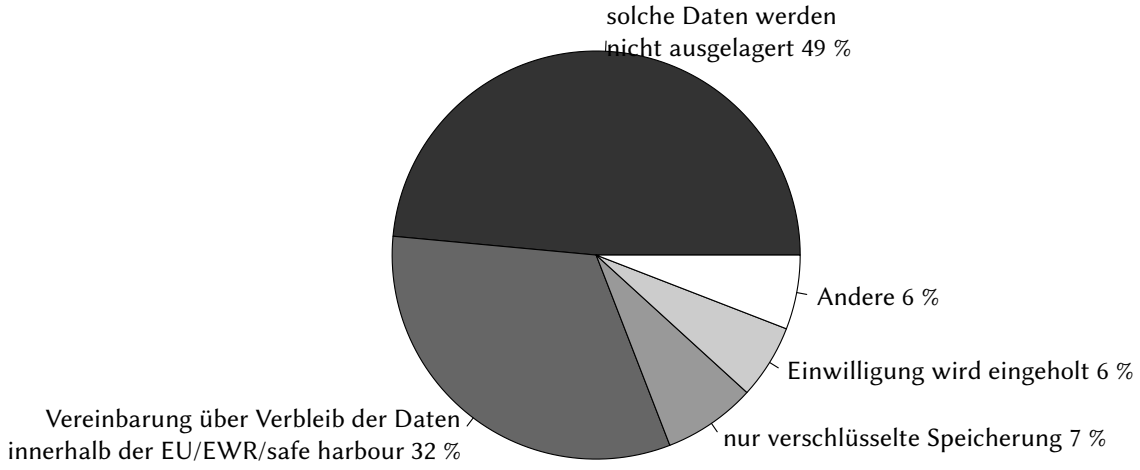


Abbildung 4-21: Personenbezogene Daten in der Cloud

Laut § 4b des Bundesdatenschutzgesetzes dürfen personenbezogene Daten nicht in ein unsicheres Drittland gelangen. Unsichere Drittländer bzw. Anbieter können außer-

europäische Länder sein, die nicht der Europäischen Wirtschaftsgemeinschaft (EWG) angehören oder Anbieter aus den USA, die kein „Safe Harbor"-Abkommen unterzeichnet haben. Mit dieser Anforderung gehen die befragten Unternehmen wie folgt um (Abbildung 4-21): 49% nutzen solche Daten nicht in der Cloud, 32% vereinbaren einen Verbleib der Daten ausschließlich innerhalb des erlaubten Rahmens.

4.2.5 Fragenblock 5: Fragen zu konkreten Auswirkungen in Ihrem Unternehmen

In diesem Teil des Fragebogens wurden Auswirkungen mit Bezug zur Informationssicherheit im Cloud-Computing betrachtet. Die fünfstufige Skala reicht hier von „trifft nicht zu" bis „trifft voll zu".

Bei Frage 40 tritt zu Tage, dass das Benutzen von Standardanwendungen wie Officeprogramme oder Anwendungsentwicklung nicht in der Cloud stattfinden sollte (Abbildung 4-22). Ebenso wird deutlich, dass die Herausforderungen des Cloud-Computings durch bestehende Standards nicht ausreichend abgedeckt werden (Frage 41). Die Frage über die rückblickend finanzielle Vorteilhaftigkeit des Cloud-Computings gegenüber traditioneller IT hat überraschend nur eine geringe Tendenz zur Zustimmung ergeben. Allerdings muss hier die geringe Anzahl von 28 Antworten berücksichtigt werden. Deutlich erkennbar ist das Misstrauen gegenüber Anbietern, die in staatliche Zwänge geraten können und aufgrund dessen Daten trotz Garantieerklärungen an Dritte außerhalb des Territoriums der EU übergeben (Frage 46 und 47).

39. Auslagern von Sicherheitsmaßnahmen in Form von Security-as-a-Service ist sinnvoll und sicher (Proxy, Spam- und Virenschutz)
40. Datenschutzsensible Standardanwendungen auszulagern, ist sinnvoll und sicher (Mail, Office, Anwendungsentwicklung)
41. Die neuen Gefahren des Cloud-Computing sind durch bestehende Standards und Sicherheits-Frameworks ausreichend abgedeckt
42. Das Konzept Ihres Unternehmens zum Informationssicherheitsmanagement im Cloud-Computing ist gut
43. Die Ausgaben für die Informationssicherheit sind gestiegen
44. Der Wechsel zu Cloud-Computing hat sich aus finanzieller Sicht gelohnt
45. Eine Private Cloud verspricht weniger Sicherheitsrisiken bei verringerter Vorteilhaftigkeit; sie ist dennoch vorteilhaft gegenüber traditioneller IT-Landschaft
46. Nicht-EU-Anbietern mit „safe harbor“-Abkommen kann man nicht vertrauen
47. Die Gefährdung durch unbemerkte staatliche Eingriffe bei Nicht-EU-Anbietern (z.B. durch „national security letters“), auch wenn die Datenhaltung in der EU garantiert wird bzw. das „safe harbor“-Abkommen unterzeichnet wurde, ist hoch
48. Effizienz im Informationssicherheitsmanagement lässt sich bei Cloud-Computing leichter erreichen
49. Schadenssummen bei Vorfällen mit Cloud-Computing sind gestiegen

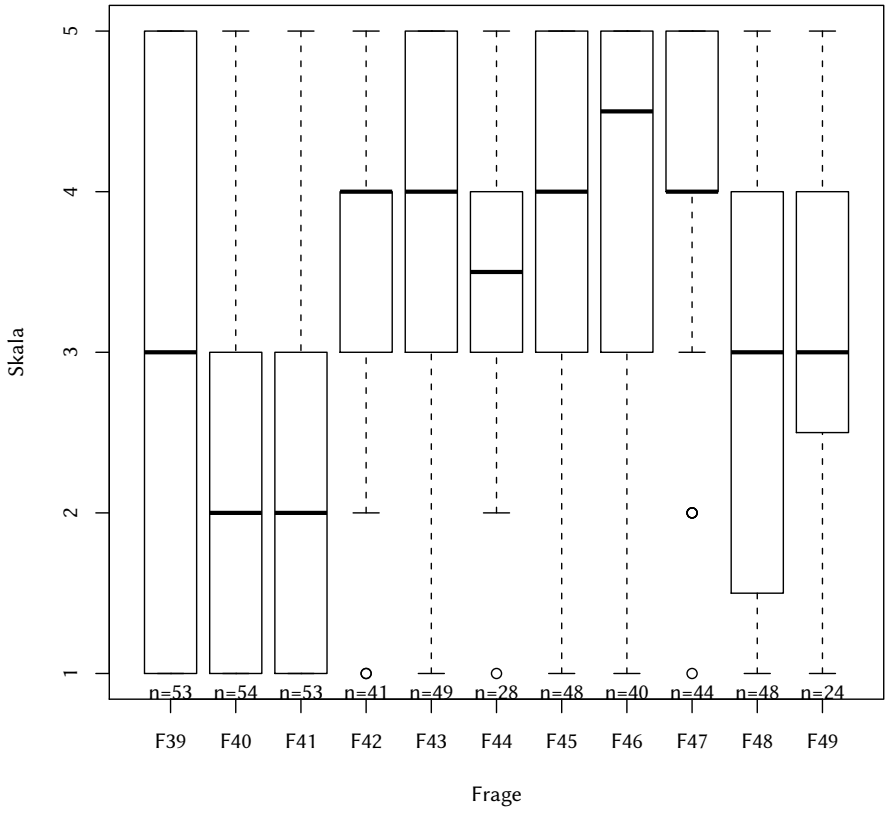


Abbildung 4-22: Boxplots der Fragen 39 bis 49

4.2.6 Fragenblock 6: Fragen zu Sicherheitsvorfällen im Cloud-Computing

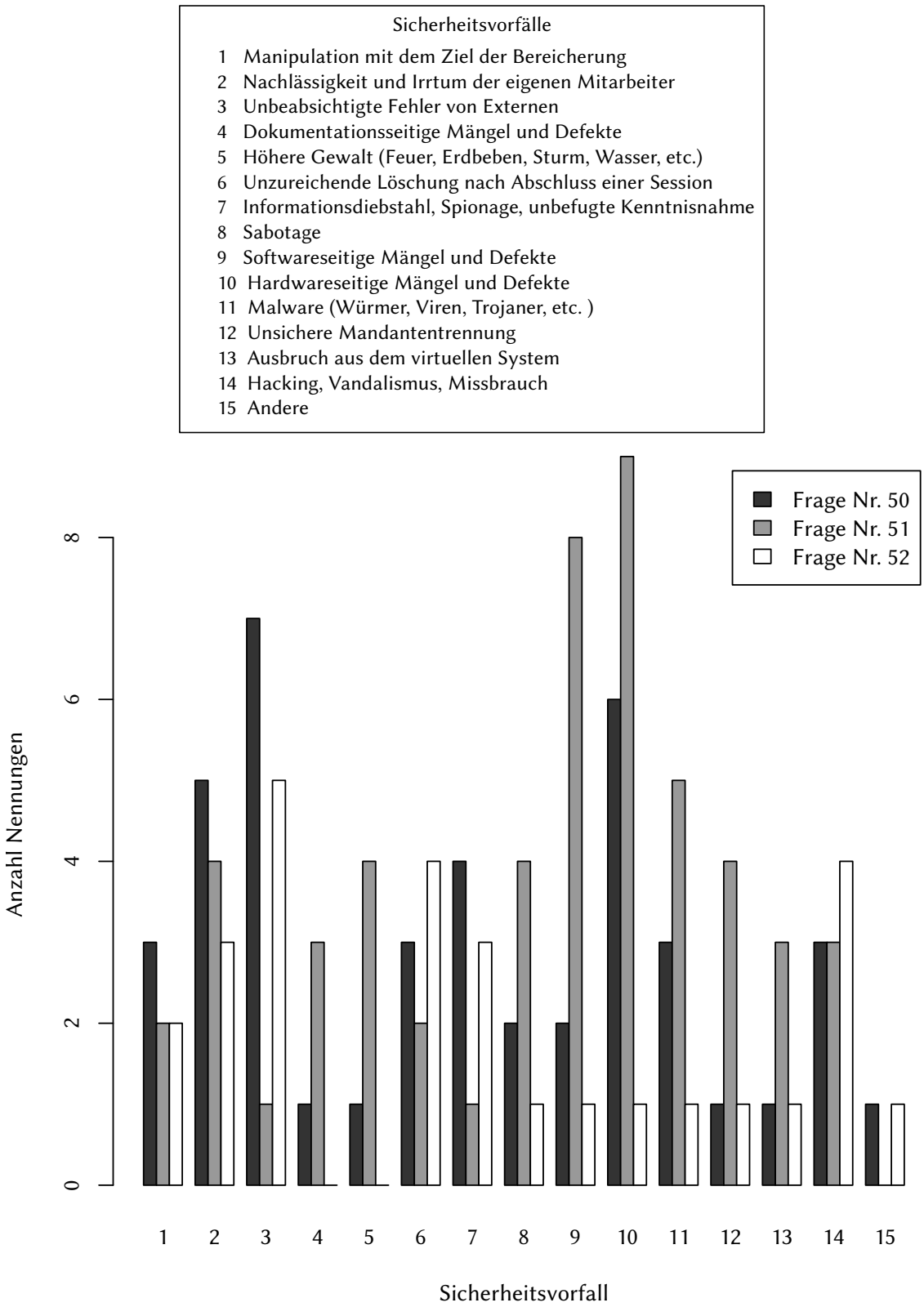
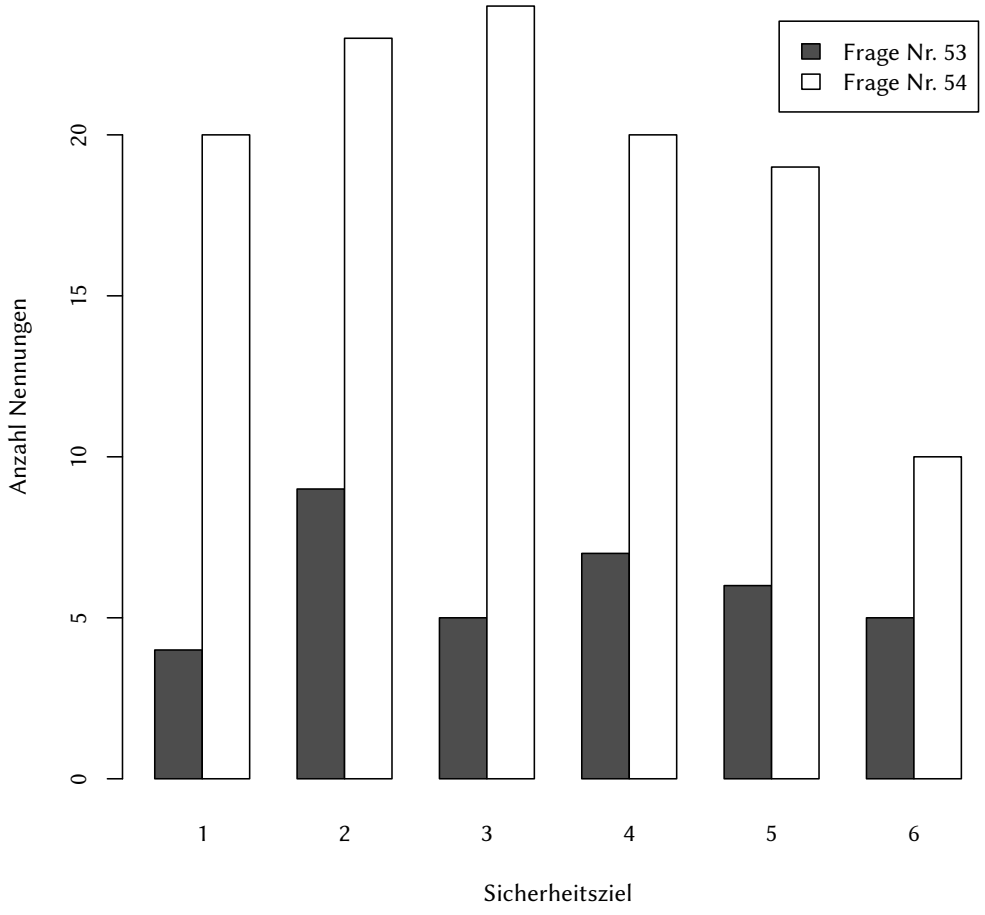


Abbildung 4-23: Sicherheitsvorfälle (Frage 50 bezieht sich auf stattgefundene Sicherheitsvorfälle in der Vergangenheit; Frage 51 fragt danach, welche Vorfälle mit Cloud-Computing vermindert auftreten; Frage 52 welche Vorfälle vermehrt auftreten.)

Die Fragen 50, 51 und 52 (Abbildung 4-23) sind mit Einschränkungen zu betrachten, da sie nur von wenigen Teilnehmern beantwortet wurden (an der geringen Anzahl an Nennungen erkennbar).

Abbildung 4-23 macht deutlich, dass vor allem hardwareseitige Mängel, die früher auftraten, deutlich seltener auftreten. Diese Tendenz ist auch bei softwareseitigen Mängeln und bei Malware zu beobachten. Unbeabsichtige Fehler von Externen sind mit dem Einsatz von Cloud-Computing deutlich gestiegen.



Sicherheitsziele

1 Revisionsfähigkeit
2 Verfügbarkeit
3 Integrität (Unversehrtheit, Verlässlichkeit)
4 Authentizität (Echtheit, Zurechenbarkeit
5 Vertraulichkeit
6 Nichtabstreitbarkeit, Verbindlichkeit

Abbildung 4-24: Ziele der Informationssicherheit

Frage 53 behandelt die bei den Vorfällen verletzten Sicherheitsziele, Frage 54 welche Ziele besondere Priorität haben (Abbildung 4-24). Die häufigste Verletzung besteht aus

mangelnder Verfügbarkeit. Die Datenintegrität hat hingegen die höchste Priorität.

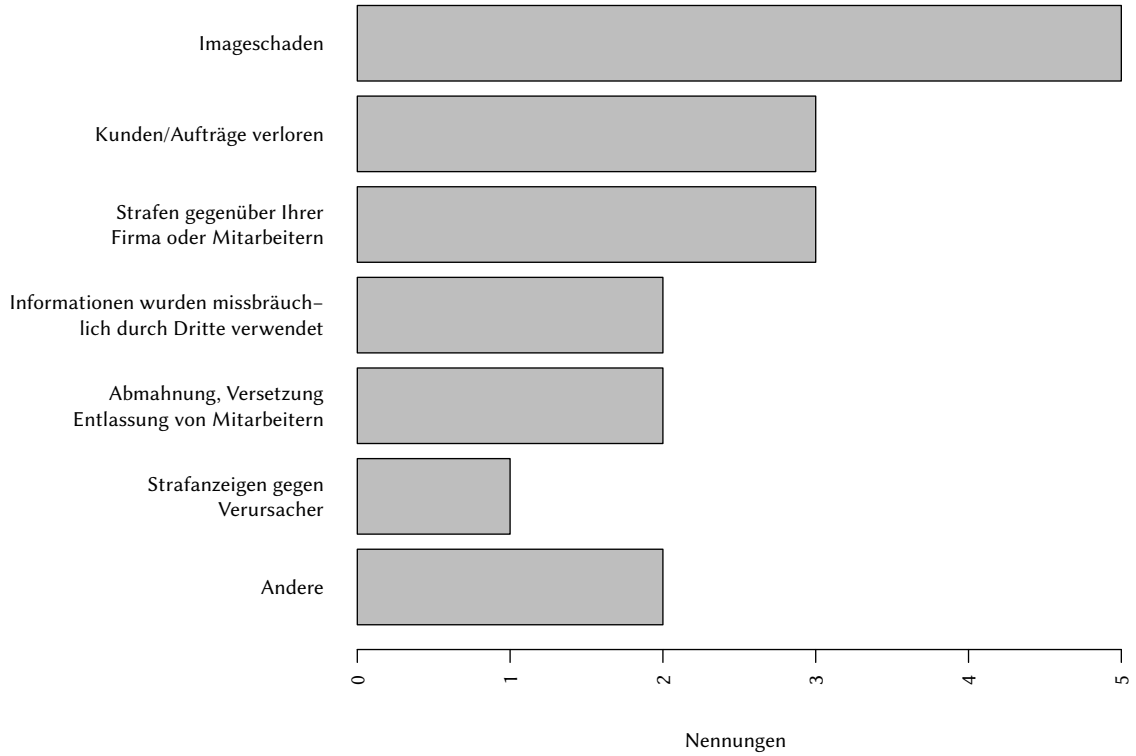


Abbildung 4-25: Konsequenzen der Verletzungen

Die Konsequenzen, die aus den Zielverletzungen hervorgingen, waren in erster Linie Imageschäden, aber auch Kundenverlust und Strafen wurden häufig genannt (Abbildung 4-25). Allerdings ist hier die geringe Anzahl von Antworten zu berücksichtigen.

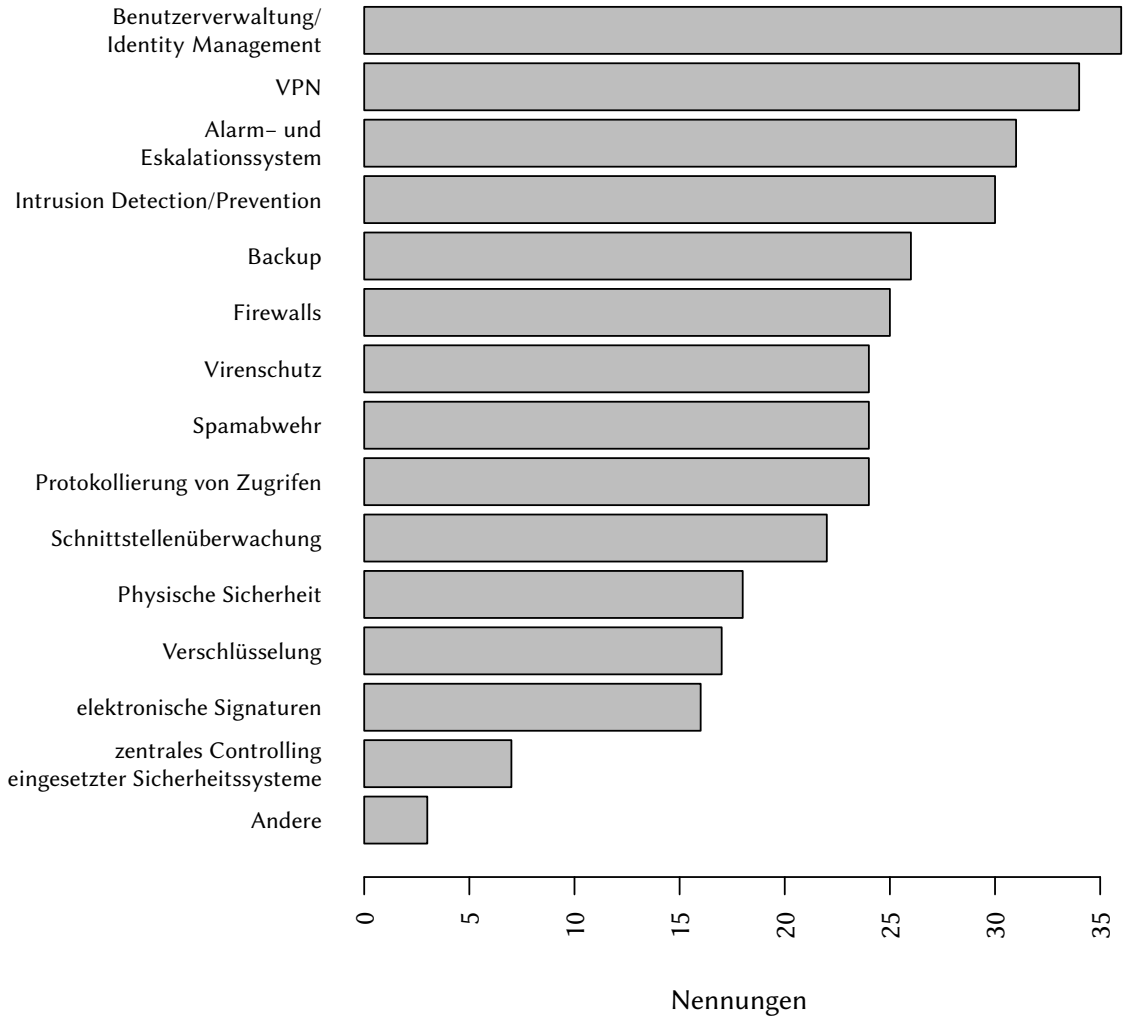


Abbildung 4-26: Bausteine für Informationssicherheit im Cloud-Computing

Wichtige Bausteine für die Informationssicherheit im Cloud-Computing ergeben sich aus Abbildung 4-26. Demnach ist das Identity Management der wichtigste Baustein, gefolgt von VPNs, Alarm- und Eskalationssystemen und Intrusion-Detection- und -Prevention-Systemen.

4.3 Induktive Statistik

In diesem Kapitel werden zunächst Verfahren zur Analyse von Modellen vorgestellt. Im Anschluss erfolgt eine Umsetzung und Anwendung eines Verfahrens, mit dem das hypothetische Modell anhand der erhobenen Daten überprüft wird.

4.3.1 Strukturgleichungsmodelle

Mit Hilfe von Strukturgleichungsmodellen („Structural Equation Modeling“, SEM) können Konstrukte aus komplexen Wirkzusammenhängen analysiert werden (vgl. Egle 2008, 95). Die Schätzung von Strukturmodellen entspricht dem statistischen Verfahren der

(multiplen) Regressionsanalyse (vgl. Ringle 2004b, 10). Häufig wird dieses Vorgehen als multivariate Methode bezeichnet, die Elemente der Regressionsanalyse und Faktorenanalyse miteinander verbindet (vgl. Hildebrandt 1998, 95). SEM-Analysen kombinieren die Vorteile von Faktoren- und Pfadanalyse (vgl. Langer 2002, 1). Mit dem Begriff Regressionsanalyse werden Verfahren bezeichnet, die den Einfluss von einer oder mehreren Variablen auf eine Zielgröße untersuchen (vgl. Duller 2007, 149). Die Grundidee einer Faktorenanalyse besteht darin, aus einer bestimmten und meist größeren Anzahl beobachteter und „gleichartiger" metrischer Merkmale aufgrund ihrer korrelativen Beziehungen eine kleinere Anzahl „neuer" und voneinander unabhängiger Variablenkonstrukte in Gestalt von „Faktoren" zu „extrahieren" (vgl. Eckstein 2010, 381). Die Pfadanalyse versucht die Beziehungen in einem SEM zu schätzen, bzw. genauer die Effektstärke von Pfaden in einem Pfaddiagramm zu bestimmen (vgl. Hair et al. 2010, 634). Diese Effektstärke wird duch die Pfadkoeffizienten repräsentiert. Diese sind die Regressionskoeffizienten, die den Effekt auf eine Variable im Pfadmodell angeben (vgl. Garson 2011, 2). Eine solche Untersuchung wird auch „Kausalanalyse" genannt. Bei der Kausalanalyse handelt es sich um ein strukturüberprüfendes, bzw. konfirmatorisches Verfahren zur empirischen Überprüfung theoretisch abgeleiteter (kausaler) Wirkungszusammenhänge (vgl. Ringle 2004b, 9). Die Bezeichnung „Kausalanalyse" suggeriert die Möglichkeit, „mit Hilfe eines statistischen Verfahrens Kausalität zu untersuchen, was im strengen wissenschaftstheoretischen Sinn nur mittels [...] kontrollierter Experimente möglich ist" (Homburg/Hildebrandt 1998, 17). Grundsätzlich können mit Hilfe statistischer Verfahren nur Beziehungen zwischen Variablen, aber keine Kausalitäten bestimmt werden (vgl. Hansmann/Ringle 2003, 70). Dennoch wird hier — aufgrund der Verbreitung in der Literatur — dieser Begriff für empirische Methoden zur Schätzung von Strukturgleichungsmodellen verwendet (vgl. Ringle 2004b, 7). „Charakteristisch für die Kausalanalyse ist, daß der methodische Ansatz es erlaubt, explizit zwischen beobachteten und theoretischen Variablen zu trennen, statistisch Substanz- und Meßfehleranteile zu separieren und vermutete kausale Beziehungsstrukturen auf der Ebene von theoretischen Variablen zu testen" (Homburg/Hildebrandt 1998, 17).

Latente und manifeste Variablen

SEM haben seit ihrer Einführung in die Marketingwissenschaft (vgl. Bagozzi 1980) eine starke Verbreitung gefunden (vgl. Egle 2008, 103), „da sie in der Lage sind, prognoseorientierte ökonometrische Verfahren mit dem eher psychometrisch fokussierten Konzept der latenten Variablen zu verbinden" (Eberl 2004, 11). Baumgartner/Homburg (1996, 140f.) stellen in einer Metastudie über internationale Journals eine überragende Rolle der Strukturgleichungsmodelle bei der Untersuchung von Zusammenhängen zwischen beobachtbaren und nicht beobachtbaren Variablen fest.

Das Konstrukt ist i.d.R. ein Modell aus nicht direkt messbaren Komponenten, soge-

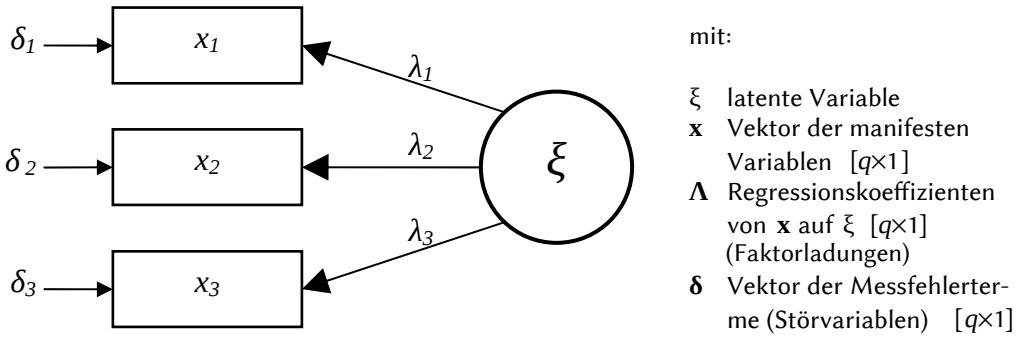


Abbildung 4-27: Beispielhaftes reflektives Messmodell (Quelle: Eberl 2004, 3)

nannten „latenten“ Variablen. Diese latenten Variablen werden durch direkt messbare Indikatoren, sogenannte „manifeste“ Variablen, beschrieben.

Reflektive und formative Messgleichungen

Die Zusammenhänge der latenten Variablen werden auch als regressionsanalytisches „Stukturgleichungssystem“ bezeichnet, die der manifesten als faktorenanalytisches „Messgleichungssystem“ (vgl. Egle 2008, 95). Die Messgleichungen können aus „reflektiven“ oder „formativen“ Varianten bestehen. Reflektiv heißt in diesem Zusammenhang: Die Ausprägungen der manifesten Variablen werden durch die latente Variable kausal verursacht. Dies bedeutet aber, dass sich bei Änderung der latenten Variable die manifesten Indikatorvariablen allesamt gleichmäßig ändern müssen. Die einzelnen Variablen einer Komponente sollten also korrelieren, damit die Komponente als reflektiv betrachtet werden kann (vgl. Eberl 2004, 4). In Abbildung 4-27 ist eine reflektive Komponente in Strukturgleichungsmodellnotation zu sehen.

Bei einer formativen Komponente ist die Beziehungsrichtung umgekehrt: Die manifesten Indikatoren sind kausal für die latente Komponente. Veränderungen eines einzelnen Indikators führen zu einer Veränderung der Latenten (vgl. Eberl 2004, 5f.). Diese müssen nicht Auswirkungen auf andere Indikatoren haben. Ob es welche gibt, kann durch die Korrelation bestimmt werden. Dies bedeutet auch, dass eine Änderung der latenten Komponente Änderungen bei nur einer manifesten Variablen zur Folge haben kann (vgl. Eberl 2004, 6). Abbildung 4-28 zeigt ein beispielhaftes formatives Messmodell mit einer latenten und drei manifesten Variablen.

Die Eigenschaft „reflektiv“ oder „formativ“ ist eher eine Eigenschaft der manifesten Indikatoren denn der latenten Komponenten (vgl. Eberl/Schwaiger 2004, 10). Wenn beispielsweise alle Indikatoren reflektive Eigenschaften aufweisen, kann von einer reflektiven Komponente gesprochen werden.

Im vorliegenden Fall ist das hypothetische Modell mit seinen (latenten) Komponenten in Kapitel 3.3 auf Seite 31 beschrieben worden. Die manifesten Variablen, also die einzelnen Fragen des Fragebogens, wurden im vorhergehenden Kapitel zur deskriptiven

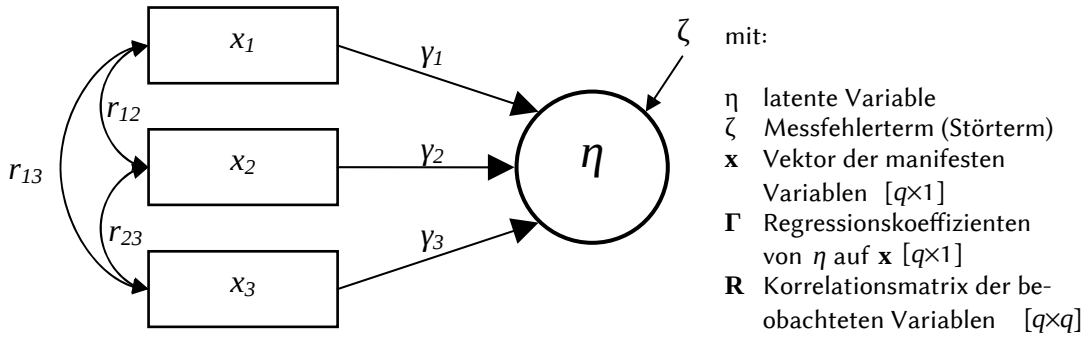


Abbildung 4-28: Beispielhaftes formatives Messmodell (vgl. Eberl 2004, 5)

Auswertung der empirischen Studie vorgestellt.

Im folgenden sollen die Ursache-Wirkungszusammenhänge zwischen den oben entwickelten latenten Variablen analysiert und letztlich das gesamte Modell damit überprüft werden. Die SEM-Analyse liefert dabei in erster Linie die Größe der Koeffizienten, die auf die Variablen einwirken. Es stellt also erst einmal keine Hypothesenprüfung dar, sondern eine Anpassung an empirische Daten (vgl. Egle 2008, 96).

Die Entscheidung, ob eine Komponente als reflektiv oder formativ anzusehen ist, ist schwierig und kann teilweise nur subjektiv erfolgen (vgl. Eberl 2004, 15). Sicher ist die Annahme, dass Indikatoren reflektiver Komponenten korrelieren sollten. Die Entscheidung, ob eine Komponente reflektiv oder formativ zu betrachten ist, sollte sorgfältig geschehen, da eine Fehlspezifikation zu inhaltlichen Problemen führen kann (vgl. Eberl 2004, 12). Huber et al. (vgl. 2007, 19) geben einen Kriterienkatalog an, der bei der Festlegung helfen kann. Eberl (2004, 16) schlägt eine systematisiertere Vorgehensweise bei der Entscheidung vor. Unter anderem könnte mit einem Tetraden-Test festgestellt werden, ob eine Komponente reflektive oder formative Eigenschaften aufweist. Z.B. wird die Komponente „Pünktlichkeit“ durch die reflektiven Indikatoren „Annahme von Last-Minute-Aufträgen“, „Antwortverhalten des Services“ und „pünktliche Lieferung“ beschrieben, während die Komponente „Lebensstreß“ durch formative Faktoren wie „Jobverlust“, „Scheidung“, „Unglücksfälle in der Familie“ beeinflusst wird (abgewandelte Beispiele von Haenlein/Kaplan (2004, 284)). Es können sogar je nach Definition Argumente für beide Varianten gefunden werden, wie das Beispiel „Trunkenheit“ (vgl. Ringle 2004b, 22) verdeutlicht. Im reflektiven Fall verursacht eine Erhöhung der Komponente eine Erhöhung der Variable „Blutalkohol“ und gleichzeitig eine Abnahme der Variable „Reaktionsfähigkeit“. Im umgekehrten formativen Fall könnte die Komponente „Trunkenheit“ durch die Variable „konsumierte Biermenge“ erhöht werden. Jedoch kann das unabhängig von der Variable „konsumierte Weinmenge“ geschehen.

Nach einer Vorstellung der benötigten statistischen Verfahren, werden die manifesten Variablen den jeweiligen latenten Komponenten des Modells zugeordnet, zu denen sie zugehörig erscheinen. Daraufhin wird geprüft, ob die Komponente formativ oder reflektiv

ist.

4.3.2 Faktorenanalyse

Um gleichartige, reflektive Gruppen innerhalb der Indikatorvariablen zu finden, könnte eine Faktorenanalyse durchgeführt werden. Wie aus dem Verhältnis der vielen Indikatorvariablen mit den wenigen latenten Variablen ersichtlich wird, muss die große Zahl an Indikatorvariablen auf die Zahl der latenten Komponenten „reduziert“ werden. Es ist zu beachten, dass das Modell aufgrund theoretischer Überlegungen entstehen sollte, nicht aufgrund von zueinander passenden Daten. Da die Faktorenanalyse ein Bestandteil der SEM-Analyse ist, wird sie hier vorgestellt. Als Faktorenanalyse bietet sich die Hauptkomponentenanalyse „Principal Components Analysis“ (PCA) und die Clusteranalyse an. Die PCA wird zudem im späteren Verlauf zur Überprüfung der reflektiven Messmodelle benötigt.

Mit Hilfe der Faktorenanalyse können mehrere gleichartige Variablen zu neuen Variablenkonstrukten (Faktoren) zusammengefasst werden (die gegenseitig unabhängig sind), sodass die wesentlichen Beziehungen in den Ausgangsdaten reproduziert werden (vgl. Eckstein 2010, 381). Laut Hair et al. (2010, 102) sind für eine Faktorenanalyse mindestens 50 Datensätze nötig. Im Übrigen gilt als generelle Regel zur Bestimmung der Mindestanzahl an Datensätzen, dass das fünffache der zu analysierenden Variablen benötigt wird. Dieser Wert (33 zu analysierende Fragen ergeben 165 erforderliche Datensätze) wird nicht erreicht, jedoch ist die an dieser Stelle durchgeführte Analyse zur Veranschaulichung gedacht. Die im späteren Verlauf auf die Messmodelle angewandten Analysen erfüllen diese Anforderung.

Hauptkomponentenanalyse

Die Hauptkomponentenanalyse ist nur auf vollständige und gleichartige Datensätze anwendbar. Daher werden zunächst nur die Ordinalskala-Fragen wegen ihrer Gleichartigkeit mit einbezogen. Um die Vollständigkeit der Datensätze herzustellen, können fehlende Werte geschätzt werden. Eine einfache Möglichkeit fehlende Werte zu schätzen ist das Ermitteln des Durchschnitts der Variable. Dies liefert befriedigende Ergebnisse, so lange nicht zu viele Werte fehlen (vgl. Husson 2011, 28). Bessere Ergebnisse lassen sich mit iterativen Schätzalgorithmen ermitteln, welche in die Erweiterung „missMDA“ des Softwarepakts „R“ eingeflossen sind (vgl. Husson 2011, 28). Im vorliegenden Fall wurden fehlende Werte mit letzterem Verfahren geschätzt.

Bei der Hauptkomponentenanalyse in Abbildung 4-29 werden nur die ersten beiden (wichtigsten) Dimensionen dargestellt. D.h. aus dieser Sicht sind nur die längsten Pfeile interpretierbar, da die kürzeren in andere Dimensionen zeigen. Abbildung 4-30 zeigt die Sicht aus den nächsten beiden Dimensionen. Die sehr kurzen, in andere Dimensionen zeigenden Pfeile wurden in der zweiten Abbildung entfernt. Die Prozentzahlen in den

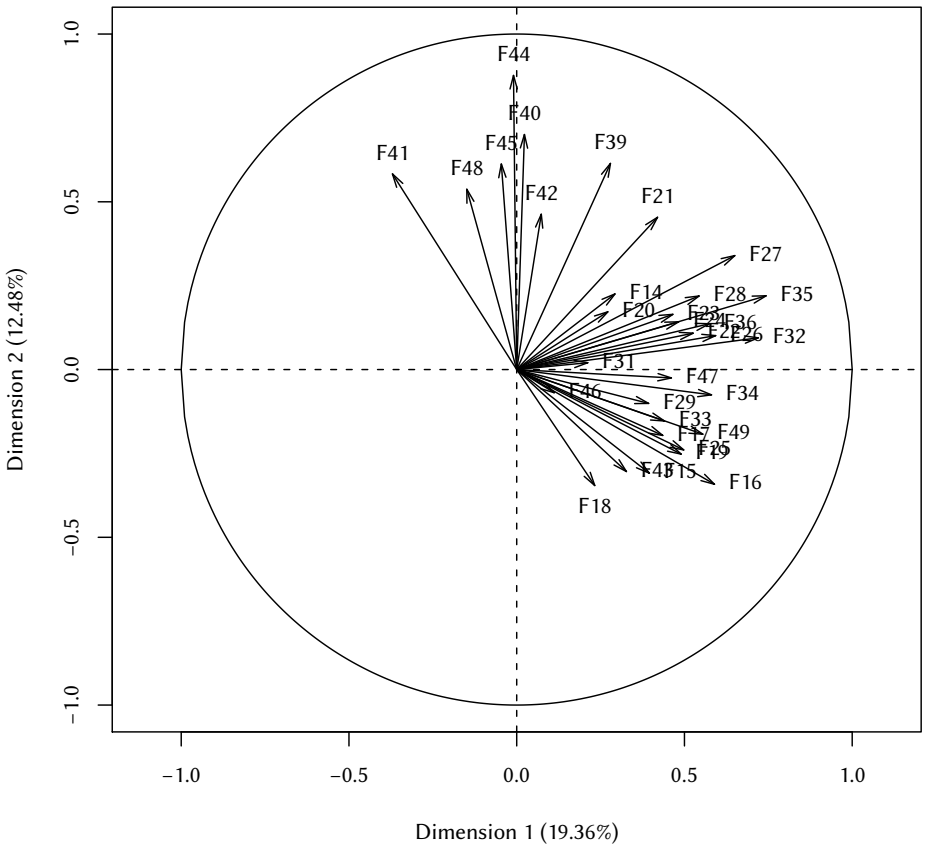


Abbildung 4-29: PCA: Dimensionen 1 und 2

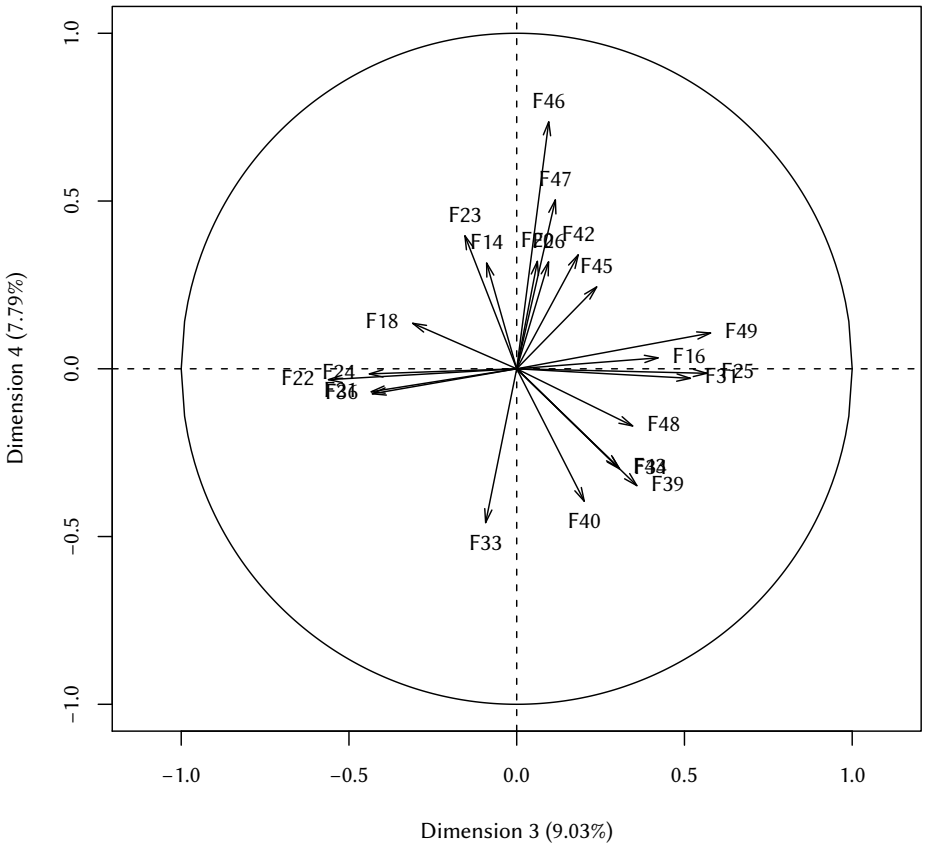


Abbildung 4-30: PCA: Dimensionen 3 und 4

Klammern stellen die Varianz dar, die mit der Dimension erklärt werden kann. Aus beiden Abbildungen lassen sich folgende Gruppen erkennen: Die Fragen 44, 40, 48 weisen gewisse Ähnlichkeiten auf, ebenso wie die Fragen 27, 35, 32. Die Fragen 49, 47, 25, 19, 16, 15 ebenfalls. Aus Sicht der Dimensionen 3 und 4 fallen die Fragen 24, 22, 21 und 36 mit Ähnlichkeiten auf. Einen zweiten Block bilden die Fragen 49, 16, 25, 31, die schon aus der ersten Sicht bekannt waren. Dass die Blöcke sich nicht decken verdeutlicht die Schwierigkeit dieser Darstellung.

Die Ergebnisse der Hauptkomponentenanalyse, d.h. die ermittelten Variablen für jede Dimension inklusive deren Korrelation sind in Abbildung 4-31 aufgeführt.

Clusteranalyse

Eine weitere Methode, Gruppen innerhalb von Daten zu identifizieren, ist die Clusteranalyse. Sie versucht Objekte so zu bündeln, dass sie innerhalb einer Gruppe möglichst homogen sind, während die Gruppen selber jedoch möglichst heterogen bleiben (vgl. Eckstein 2010, 401). Das Grundprinzip einer numerischen Clusterbildung besteht dabei in der Messung bzw. Berechnung der Distanz zwischen den Merkmalen (vgl. Eckstein 2010, 402). Dabei deutet man die Merkmale als ähnlich oder homogen, wenn ihre Distanz zueinander vergleichsweise gering ist. Abbildung 4-32 zeigt eine Clusteranalyse, wobei zunächst die Euklidischen Distanzen berechnet wurden, die anschließend mit dem hierarchisch-agglomerativen Klassifikationsverfahren „complete linkage“ (größte Distanz zwischen zwei Objekten zweier Cluster) kombiniert wurden (vgl. Eckstein 2010, 409). Es wird dabei von zunächst einelementigen Clustern ausgegangen, die zu größeren Clustern zusammengefasst werden (vgl. Eckstein 2010, 409). Es lassen sich Ähnlichkeiten mit den Ergebnissen der PCA feststellen.

4.3.3 Verfahren zur Analyse von SEM

Zur Schätzung von Modellen mit latenten Variablen gibt es zwei etablierte Verfahren, die Kovarianzstrukturanalyse und das „Partial Least Squares“-Verfahren (PLS). Sie unterscheiden sich grundlegend (vgl. Temme et al. 2006, 1; Eberl 2004, 11; Ringle 2004b, 1).

Kovarianzstrukturanalyse

Mit dem Verfahren der Kovarianzstrukturanalyse lassen sich die Parameter für komplexe Hypothesensysteme und Abhängigkeitsstrukturen modellieren und schätzen (vgl. Homburg/Pflesser 2000, 636). Allerdings sollten für valide Schätzungen von Kovarianzstrukturmodellen empirische Daten hohen Umfangs vorliegen (vgl. Ringle 2004b, 15). In der Literatur genannte Empfehlungen liegen bei einem Stichprobenumfang von 200 und mehr, abhängig von der Anzahl zu schätzender Modellparameter (vgl. Bagozzi/Yi 1994,

```
$Dim.1
$Dim.1$quanti
    correlation      p.value
F35   0.7436137 2.282220e-11
F32   0.7201984 1.861057e-10
F27   0.6503016 3.298321e-08
F26   0.5932016 9.247763e-07
F16   0.5895996 1.117196e-06
F34   0.5807840 1.757583e-06
F36   0.5741567 2.449630e-06
F49   0.5549868 6.150798e-06
F28   0.5438156 1.024993e-05
F22   0.5261618 2.215431e-05
F25   0.4979657 6.964932e-05
F19   0.4904761 9.286829e-05
F24   0.4828977 1.234201e-04
F23   0.4656192 2.303808e-04
F47   0.4611346 2.694503e-04
F33   0.4405888 5.376428e-04
F17   0.4354936 6.339073e-04
F21   0.4199070 1.032899e-03
F15   0.3955661 2.116530e-03
F29   0.3933911 2.250880e-03
F43   0.3270935 1.220365e-02
F14   0.2930122 2.560313e-02
F39   0.2794697 3.362175e-02
F20   0.2717814 3.903752e-02
F41  -0.3704071 4.208492e-03


$Dim.2
$Dim.2$quanti
    correlation      p.value
F44   0.8767052 1.915907e-19
F40   0.7005917 9.229358e-10
F39   0.6144017 2.897102e-07
F45   0.6127475 3.181473e-07
F41   0.5831449 1.558766e-06
F48   0.5375260 1.355630e-05
F42   0.4630049 2.524753e-04
F21   0.4539694 3.445525e-04
F27   0.3397012 9.084685e-03
F43  -0.3040640 2.031315e-02
F15  -0.3090950 1.823132e-02
F16  -0.3419552 8.607034e-03
F18  -0.3458199 7.838737e-03


$Dim.3
$Dim.3$quanti
    correlation      p.value
F49   0.5778893 2.033675e-06
F25   0.5668692 3.499900e-06
F31   0.5177378 3.152923e-05
F16   0.4215037 9.835546e-04
F39   0.3581888 5.766867e-03
F48   0.3456678 7.867811e-03
F34   0.3064107 1.931827e-02
F43   0.3043061 2.020858e-02
F18  -0.3101526 1.781762e-02
F36  -0.4302894 7.480757e-04
F21  -0.4335801 6.739098e-04
F24  -0.4392178 5.621493e-04
F22  -0.5610993 4.614722e-06
```

```
$Dim.4
$Dim.4$quanti
    correlation      p.value
F46   0.7360436 4.607635e-11
F47   0.5034213 5.624123e-05
F23   0.3963776 2.068271e-03
F42   0.3395944 9.107871e-03
F20   0.3201564 1.428459e-02
F26   0.3186624 1.477056e-02
F14   0.3151436 1.597153e-02
F32  -0.2681512 4.183466e-02
F19  -0.2799368 3.331396e-02
F43  -0.2946444 2.475562e-02
F34  -0.2982909 2.294735e-02
F39  -0.3483196 7.374264e-03
F40  -0.3947576 2.165611e-03
F33  -0.4585332 2.947919e-04


$Dim.5
$Dim.5$quanti
    correlation      p.value
F18   0.5822017 1.635528e-06
F20   0.5302565 1.859864e-05
F33   0.4820885 1.271761e-04
F23   0.4086162 1.450339e-03
F48   0.3479334 7.444413e-03
F34   0.3308854 1.118079e-02
F17   0.3163667 1.554496e-02
F46   0.3072748 1.896253e-02
F49  -0.2833202 3.115373e-02
F43  -0.2938328 2.517405e-02
F28  -0.3829447 3.007882e-03
F31  -0.4393918 5.589840e-04


$Dim.6
$Dim.6$quanti
    correlation      p.value
F17   0.4900169 9.450062e-05
F42   0.4166100 1.141908e-03
F43   0.3793023 3.320622e-03
F32   0.3315023 1.102161e-02
F23   0.3111060 1.745154e-02
F31   0.3029869 2.078415e-02
F34  -0.2958916 2.412411e-02
F19  -0.3441067 8.171602e-03
F26  -0.3564666 6.022953e-03
F24  -0.3699157 4.263137e-03
F15  -0.5059593 5.085261e-05
```

Abbildung 4-31: Ergebnisse der Hauptkomponentenanalyse

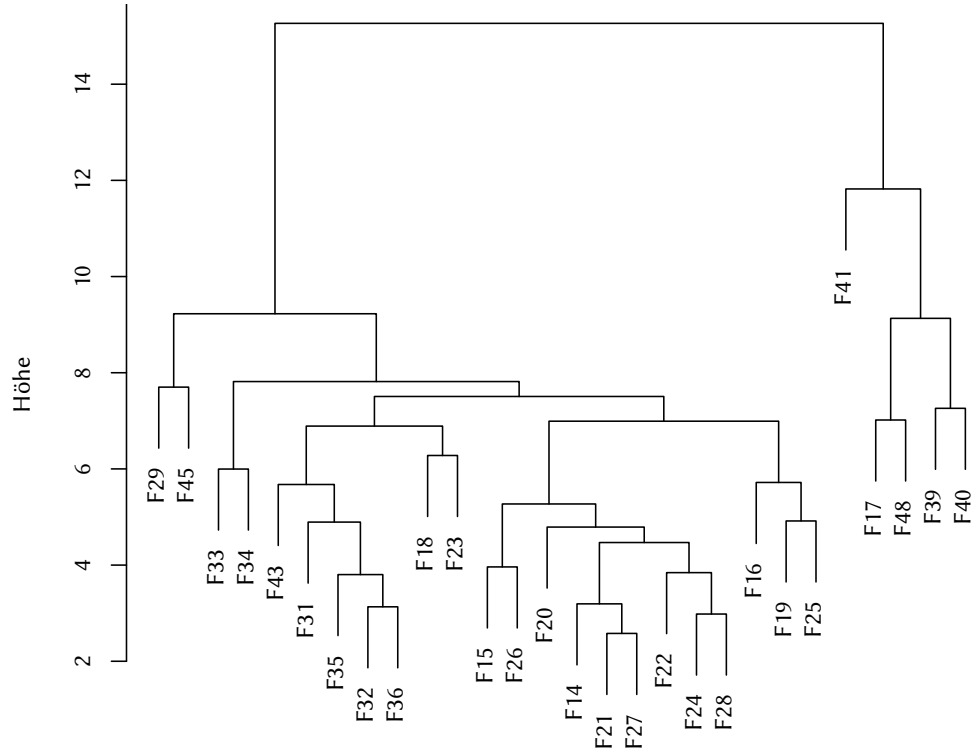


Abbildung 4-32: Clusteranalyse der Fragen

19). Aufgrund von Komplexität und Restriktionen können mit der Kovarianzstrukturanalyse nicht immer alle realen Phänomene abgebildet werden. Daher steht sie unter Kritik (vgl. Ringle 2004b, 17). Sie kann nur Modelle mit reflektiven Komponenten schätzen (vgl. Eberl 2004, 12).

Für die Kovarianzstrukturanalyse bieten sich unter anderem die kommerziellen Softwarepakte „LISREL“ (Linear Structural Relationships) und „AMOS“ (Analysis of Moment Structures) an.

„Partial Least Squares Path Modeling“ (PLSPM)

Das PLS-Verfahren stellt eine Alternative zur Schätzung von Kausalmodellen dar, die mit dem Kleinste-Quadrate-Verfahren arbeitet (vgl. Ringle 2004b, 18). Anstatt auf die Erklärung der Kovarianzen in einem Modell (wie bei der Kovarianzstrukturanalyse) zielt das PLS-Verfahren darauf ab, die Varianz in den latenten Variablen zu erklären bzw. zu prognostizieren (vgl. FU Berlin 2008, 1). PLSPM ist ein Analyse-Framework, um (mehrfache) Beziehungen zwischen Blöcken von Variablen (Komponenten) zu analysieren (vgl. Sanchez 2010, 1). Dabei wird angenommen, dass zuvor eine Theorie besteht, wie diese Blöcke in Beziehung stehen und dass die Blöcke latente Variablen in dem theoretischen Konzept darstellen. Die Berechnung erfolgt iterativ mit mehrfachen „Ordinary Least Squares Regressions“. Obwohl Herman Wold 1971 erste Algorithmen entwickelte, findet dieses Verfahren erst im letzten Jahrzehnt größere Verbreitung (vgl. Temme et al. 2006, 1). Aufgrund der partiellen Schätzung einzelner Elemente des Kausalmodells werden für die

Ermittlung verlässlicher Ergebnisse mit dem PLS-Verfahren weniger empirisch erhobene Fälle benötigt als für die Kovarianzstrukturanalyse (vgl. Chin/Newsted 1999, 314, 326). Selbst Modelle, denen nur 20 empirisch erhobene Fälle zu Grunde liegen, lassen sich mit dieser Methode zufriedenstellend schätzen (vgl. Chin/Newsted 1999, 335). Eine Heuristik besagt, dass die Stichprobe zehn mal größer als die Anzahl der Pfade eines formativen Messmodells oder einer latenten Komponente sein sollte (vgl. Ringle 2004a, 12; Winkler/Ernst 2011, 1139). Im vorliegenden Fall liegt die größte Anzahl an Pfaden bei latenten Komponenten bei drei (siehe unten, Abbildung 4-34 auf Seite 71). Die größte Pfadanzahl eines formativen Messmodells besitzt die Informationsqualität mit 7 Pfaden. Das nach der Heuristik geforderte Maß wird mit der Stichprobengröße von 58[4] verwertbaren Datensätzen nicht ganz erreicht. Die Größe sollte für die übrigen Messmodelle und das Strukturmodell aber ausreichend sein.

Für das PLS-Verfahren existiert u.a. die Software SmartPLS und die quelloffene Erweiterung „plspm“ des Softwarepakets „R“.

Sowohl weil der Umfang der benötigten Stichprobe geringer ist (vgl. FU Berlin 2008, 1) als auch aufgrund der Tatsache, dass mit diesem Verfahren nicht nur reflektive, sondern auch formative Komponenten verarbeitet werden können (vgl. Temme et al. 2006, 2; Eberl 2004, 12), fällt die Entscheidung zugunsten des PLS-Verfahrens aus. Zudem ist es fehlertoleranter (vgl. Ringle 2004b, 1; FU Berlin 2008, 1).

Aufgrund der quelloffenen und kostenlosen Nutzungsmöglichkeit sowie der Aktualität (Oktober 2010) erfolgt die Überprüfung mit plspm. Dazu wird das Pfadmodell in eine Matrix überführt, die von plspm eingelesen werden kann. Das Pfadmodell der Beziehungen zwischen den Blöcken kann aus dem abgewandelten Modell von Rodríguez/Casanovas aus Abbildung 3.3 auf Seite 31 gewonnen werden. Die Überführung in die Matrix ist in Abbildung 4-33 zu sehen.

Weiterhin muss eine Datenaufbereitung stattfinden, da mit plspm nur vollständige Datensätze verarbeitet werden können. Wie für die PCA wurden die fehlenden Werte mit „missMDA“ geschätzt. Im Anschluss werden die manifesten Variablen den latenten Komponenten zugeordnet. Zur Überprüfung der Zuordungsqualität gibt es lokale Gütekriterien für die Messmodelle und globale Gütekriterien für das Strukturmodell.

Lokale Gütekriterien

Im weiteren Verlauf wird geprüft, ob durch die manifesten Variablen die latenten Komponenten hinreichend beschrieben werden können (auch als „lokale Gütekriterien“ bezeichnet (vgl. Zinnbauer/Eberl 2004, 15)). Die Anforderungen bei reflektiven Komponenten sind Homogenität und Eindimensionalität der manifesten Variablen (vgl. Vinzi et al. 2010, 50).

[4] Die Ordinalskala-Fragen wurden nicht von jedem Teilnehmer beantwortet, sodass sich für die hier eingeflossenen Fragen die Stichprobengröße von der weiter oben genannten Zahl unterscheidet.

	Informations-qualität	Prozess-qualität	Personal-qualität	Organisa-tionsqualität	System-qualität	Service-qualität	Qualität der Informations-sicherheit
Informations-qualität	**0**						
Prozess-qualität	0	**0**					
Personal-qualität	0	0	**0**				
Organisa-tionsqualität	0	0	0	**0**			
System-qualität	1	1	0	0	**0**		
Service-qualität	0	0	1	0	0	**0**	
Q. d. Informations-sicherheit	0	0	0	1	1	1	**0**

Abbildung 4-33: PLS-Matrix

Homogenität Die Homogenität wird durch den Reliabilitätskoeffizienten α (alpha) von Cronbach (1951) bzw. dem Koeffizienten ρ (rho) von Dillon/Goldstein (1984, 480) — der im Wesentlichen auf Werts et al. (1974) basiert (vgl. Grimpe 2005, 218) — bestimmt (vgl. Zinnbauer/Eberl 2004, 15). Diese Koeffizienten messen die interne Konsistenz der betrachteten manifesten Variablen, indem die durchschnittliche Korrelation gemessen wird (vgl. Chongsuvivatwong 2007, 249). ρ wird dabei als der bessere Indikator angesehen (vgl. Vinzi et al. 2010, 51). Der Wert sollte bei beiden größer als 0,7 sein (vgl. Vinzi et al. 2010, 50).

Eindimensionalität Der Test auf Eindimensionalität erfolgt mit Hilfe einer Hauptkomponentenanalyse des jeweiligen Blocks (vgl. Vinzi et al. 2010, 50) (Ein Beispiel dazu folgt weiter unten auf Seite 72). Der Eigenwert der ersten Variable sollte dabei größer eins sein, der der übrigen kleiner eins (vgl. Vinzi et al. 2010, 50).

Kommunalitäten Um festzustellen wie gut die latente Komponente die Ausprägungen der Indikatorvariablen erklären kann, wird ein „Kommunalitäts"-Index herangezogen. Dieser misst, in wie weit die Varianz der jeweiligen manifesten Variablen durch die latente Komponente reproduziert werden kann. Mit anderen Worten: Er misst die Varianz, die eine Indikatorvariable mit der Varianz der latenten Komponente gemeinsam hat. Dieser Wert sollte über 0,5 liegen (Sanchez 2009, 15; Grimpe 2005, 217).

Anschließend kann (z.B. mit Hilfe des χ^2-Tests) geprüft werden, ob sich die reflektiven Komponenten genügend voneinander unterscheiden, um sicherzustellen, dass es sich jeweils um eigene Gebilde handelt (vgl. Zinnbauer/Eberl 2004, 16). Um sicherzugehen, dass keine manifeste Variable stärker auf eine andere Komponente lädt als die, die sie eigentliche beschreiben soll (vgl. Sanchez 2009, 14), werden die Korrelationen zwischen

den latenten und manifesten Variablen bestimmt. Die Ladungen sind gleich den Koordinaten der Variablen geteilt durch die Quadratwurzel der zugehörigen Eigenwerte (vgl. Husson 2011, 27) und beschreiben die Korrelation zwischen den Indikatoren und den Komponenten (vgl. Dijkstra 2010, 28; Ho 2006, 207). Bei reflektiven Komponenten sollte die Ladung der latenten auf manifeste Variablen mehr als 0,7 betragen (vgl. Huber et al. 2007, 35).

Im Zusammenhang mit der PLS-Analyse werden Hilfsvariablen zur Bestimmung der Schätzparameter gebildet, die als „Gewichte“ (weights) bezeichnet werden (vgl. Huber et al. 2007, 6). Diese Gewichte sind die Koeffizienten der manifesten Variablen und dienen der Bestimmung von konkreten Werten für die latenten Variablen (vgl. Huber et al. 2007, 6; Sanchez 2009, 5). Der PLS-Algorithmus berechnet zuerst die Messmodelle, dann das Strukturmodell. Anfangs werden willkürliche Gewichte gewählt, die daraufhin genauer geschätzt werden (vgl. Huber et al. 2007, 7). Diese Schritte werden so lange wiederholt, bis sich keine Änderungen an den Gewichten mehr ergeben. Im Fall reflektiver Komponenten sind die Gewichte die Regressionskoeffizienten der Indikatorvariablen, die den Einfluss der latenten auf die manifesten Variablen beschreiben (vgl. Huber et al. 2007, 7). Im Fall formativer Komponenten sind dies die multiplen Regressionskoeffizienten, die den Effekt der manifesten Variablen auf die latente Variable beschreiben (vgl. Huber et al. 2007, 7).

Die Beurteilung formativer Komponenten mit statistischen Methoden ist problematisch (vgl. Eberl/Schwaiger 2004, 15; Zinnbauer/Eberl 2004, 9). Die Korrelationen können nicht wie bei den reflektiven Komponenten als Gütemaß herangezogen werden, da bei formativen Komponenten die Indikatorvariablen korrelieren können, aber nicht müssen. Daher wird hier nur ein Vergleich zwischen den einzelnen Datensätzen vorgenommen, um festzustellen, ob sie sich in Bezug auf die formative Komponente ähnlich verhalten. Dazu werden die Regressionkoeffizienten zwischen den manifesten Indikatoren und der latenten Komponente mit den Bootstrap-Standardabweichungen[5] verglichen (vgl. Eberl/Schwaiger 2004, 16). Je kleiner die Bootstrap-Standardfehler, desto signifikanter sind die Indikatoren (vgl. Eberl/Schwaiger 2004, 16). Die Indikatorreliabilität kann mit Hilfe der Indikatorladungen erfasst werden. Der Wert sollte über 0,7 sein (vgl. Chin/Dibbern 2010, 182). Der PLS-Algorithmus kann auch zusammen mit dem Bootstrapping erfolgen, wodurch die geschätzte Ladung jedes Indikators auf die latente Variable gemessen werden kann (vgl. Zinnbauer/Eberl 2004, 9). Dabei wird bei der Bootstrap-Prozedur dasselbe formative Faktormodell mehrfach geschätzt und daraus die Zuverlässigkeit der im Mittel errechneten Koeffizientenschätzer berechnet. Diese Koeffizientenschätzer können auch als Validitätskoeffizienten bezeichnet werden (vgl. Zinnbauer/Eberl 2004, 17).

[5] Bootstrapping ist eine Resampling-Technik, die die Verteilung durch eine mehrmalige Teilstichprobenentnahme (mit Zurücklegen) approximiert (vgl. Sachs/Hedderich 2006, 275f.; Grimpe 2005, 218). Es findet eine Rekombination von verschiedenen Werten der verschiedenen Datensätze statt (vgl. Seddon/Kiew 1996, 100).

Globale Gütekriterien

Nach Analyse der einzelnen latenten Komponenten wird geprüft, ob das Gesamtmodell mit den vorliegenden Daten in Einklang zu bringen ist, das Modell also schlüssig mit den vorliegenden Daten bestätigt werden kann (auch als „globale Gütemaße“ bezeichnet). Dabei gibt es verschiede Prüfindizes. Neben dem oben angesprochenen Kommunalitätsindex gibt es den Redundanzindex für das Strukturmodell, die R^2-Koeffizienten und den „Goodness of Fit“-Index (GoF) für das Gesamtmodell (vgl. Vinzi et al. 2010, 56ff.). Kein direktes Gütemaß, da es nur den Fit einer jeden Regressionsgleichung angeben kann, ist der R^2-Koeffizient (vgl. Vinzi et al. 2010, 57). Die R^2-Koeffizienten geben an, welcher Prozentsatz an Varianz einer Komponente durch die einwirkenden Komponenten erklärt werden kann. Die Pfadkoeffizienten geben den Einfluss der einwirkenden Komponenten auf die Zielkomponente an (vgl. Sanchez 2009, 13). Chin (1998) empfiehlt, dass die Pfadkoeffizienten mindestens 0,2 aber besser über 0,3 betragen sollten, um als bedeutungsvoll interpretiert werden zu können. Der GoF-Index ist der geometrische Mittelwert des durchschnittlichen Kommunalitätsindizes und des durchschnittlichen R^2-Wertes, wobei zwischen absolutem und relativem GoF-Index unterschieden wird (vgl. Vinzi et al. 2010, 58). Der relative GoF-Index liegt zwischen 0 und 1 und sollte mindestens 0,9 betragen, um klar für das Modell zu sprechen (vgl. Vinzi et al. 2010, 59). Anschließend kann mit einer Bootstrap-Prozedur die statistische Signifikanz der Pfadkoeffizienten gemessen werden (vgl. Vinzi et al. 2010, 60).

Zuordnung manifester Variablen zu latenten Komponenten

Zunächst werden nur Variablen herangezogen, die einheitlich skaliert sind. In diesem Fall sind dies alle Ordinalskala-Fragen.

Abbildung 4-34 zeigt das entwickelte Modell in Strukturgleichungsmodellnotation mit zugeordneten Fragen.

Informationsqualität Dieser Komponente werden zunächst die Fragen 25, 29, 32, 33, 34, 46, 47 zugeordnet. Diese Komponente wird als formativ eingeordnet, da es — nach Einschätzung des Autors — für diese latente Komponente Variablen geben kann, die unabhängig von einander die Informationsqualität verbessern oder verschlechtern können. Als Beispiel sei genannt: Offene Standards und Richtlinien zur Präzision bei der Datenerfassung können sich beide auf die Informationsqualität auswirken, müssen jedoch nicht korrelieren. Die Bootstrap-Ergebnisse befinden sich im Anhang.

Prozessqualität Dieser Komponente werden die Fragen 21, 22, 24, 28 zugeordnet. Diese Komponente wird als reflektiv eingestuft. Die Fragen betreffen allesamt Regelungen, die in SLAs festgehalten werden. Ist eine Regelung im SLA vergessen worden oder schlecht, ist das gesamte SLA schlecht. Nicht entscheidend ist, welche Variable

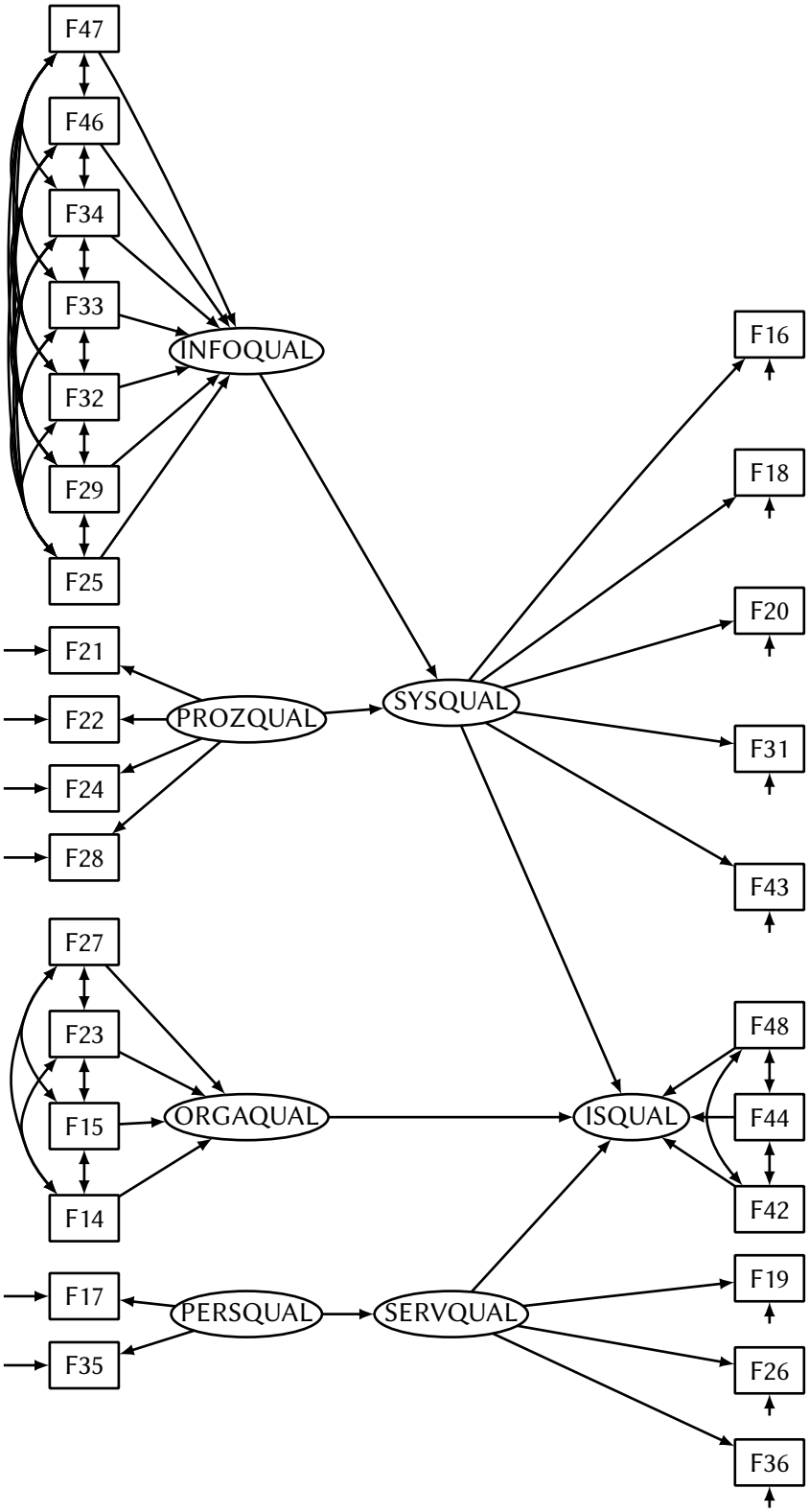


Abbildung 4-34: Vorläufiges Strukturgleichungsmodell

im Einzelnen verantwortlich ist. Mit $\alpha = 0,79$ und $\rho = 0,86$ ist die Homogenität ausreichend gegeben, die Eindimensionalität ist mit dem ersten Eigenwert größer 2 und dem zweiten Eigenwert kleiner 0,7 ausreichend. Die Kommunalitäten sind sämtlich größer 0,5. In Abbildung 4-36b ist eine Übersicht über alle Komponenten gegeben.

Personalqualität besteht aus den Fragen 17 und 35 und wird als reflektiv eingestuft.

Organisationsqualtiät besteht aus den Fragen 14, 15, 23, 27 und wird als formativ eingestuft, da es verschiedene Variablen geben kann, die die Organisationsqualität jeweils separat beeinflussen. Eine negative Eigenschaft muss nicht automatisch die gesamte Organisationsqualität in Frage stellen.

Systemqualität Diese Komponente besteht aus den Fragen 16, 18, 20, 31, 43 und wird als reflektiv eingestuft. Begründung: Ist nur eine Variable schlecht, so hat dies Konsequenzen für alle anderen Variablen: Wenn z.B. die Variable „mehrstufige Authentifizierung“ verletzt ist, können alle anderen Variablen noch so gut sein, sie können dennoch nicht die Qualität verbessern, wenn ein System kompromittiert wird. Die Reliabilitätskoeffizienten liegen allerdings weit unter den geforderten 0,7 und auch die Eindimensionalität ist nicht gegeben (Abbildung 4-35. Die Prozentzahlen der Achsenbeschriftungen geben den Anteil der Varianz, die mit den zwei dargestellten Dimensionen erklärbar ist, an.). Es ist erkennbar, dass alle Variablen zwar weitgehend in einer Ebene liegen, da die Pfeile ähnlich lang sind (wenn einer oder mehrere kurz wären, würden diese eine andere, in dieser zweidimensionalen Darstellung nicht erkennbare Dimension zeigen). Jedoch kann nicht davon gesprochen werden, dass sie in die gleiche Richtung zeigen würden. Z.B. zeigt Frage 20 eher nach „Norden“ während Frage 31 eher nach „Westen“ zeigt. Das bedeutet, dass entweder das Messmodell falsch ist und die Zuordnung der Indikatoren nicht stimmt oder diese Komponente nicht reflektiv ist. Im ersten Fall müsste die Indikatorzuordnung verändert werden. Hierbei darf das Modell nicht so lange an die Daten angepasst werden, bis ein rechnerisch richtiges Modell entsteht, welches mit der Realität nicht viel zu tun hat (vgl. Eberl 2004, 16f.). Im zweiten Fall müsste die Komponente als formativ spezifiziert werden. Vinzi (2009, 12) schlägt verschiedene Verfahren vor, um Eindimensionalität herzustellen:

1. Die Richtung von Variablen invertieren: Dies würde hier nicht helfen, da die Fragen eher um 90° auseinanderliegen, nicht um 180°.
2. Die Komponente formativ spezifizieren.
3. Falls mehrere eindimensionale Blöcke innerhalb der Komponente existieren: Eine zusätzliche Komponente dem Modell hinzufügen, die die Blöcke aus eindimensionalen Variablen zusammenführt.
4. Falls es mehrere eindimensionale Blöcke gibt: Die Blöcke splitten.

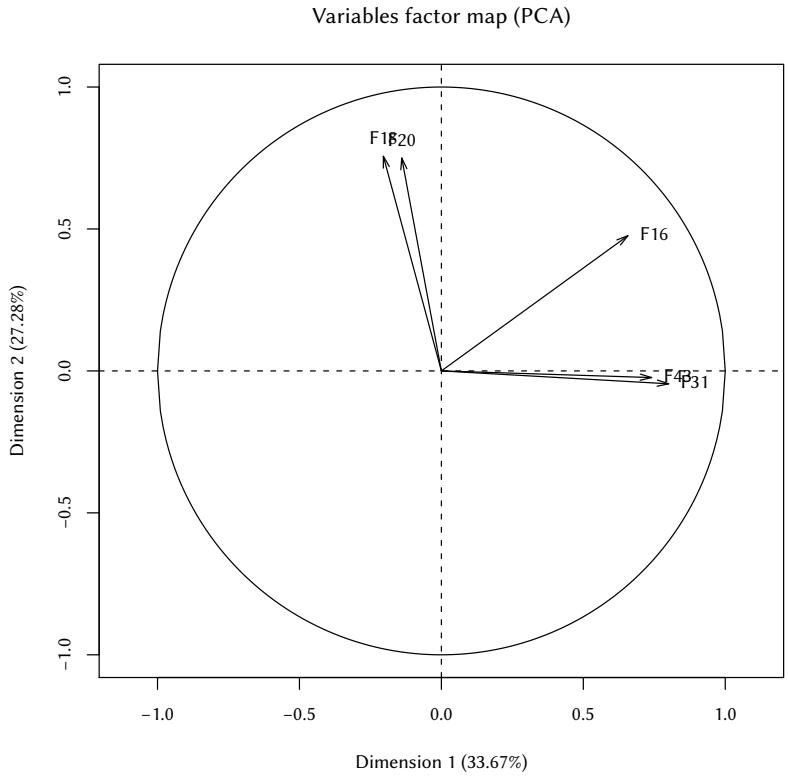


Abbildung 4-35: Dimensionen der Systemqualität

5. Weit entfernte Variablen entfernen: Wenn die Fragen 31 und 43 entfernt werden, werden die Homogenitätsanforderungen knapp erfüllt, jedoch erreicht Frage 20 nicht den erforderlichen Kommunalitätsindex von 0,5.
Da Variante zwei unter den gegebenen Gesichtspunkten am sinnvollsten erscheint, wird die Komponente im weiteren Verlauf als formativ spezifiziert.

Servicequalität besteht aus den Fragen 19, 26, 36 und wird als reflektiv eingestuft. Die Wahrnehmung der Servicequalität leidet immer wenn eine bestimmte Variable nicht den Erwartungen entspricht. Bzw. ist die Gefahr, die einer der drei nicht-eingehaltenen Variablen ausgeht immens, sodass die anderen noch so gut sein können. Die Anforderungen werden mit $\rho = 0,73$ und den Eigenwerten 1,42 und 0,88 erfüllt. Die Kommunalitäten von Frage 19 und 26 werden nicht erfüllt. Die Kommunalitäten befinden sich im Anhang.

Qualität der Informationssicherheit Ihr wird die Frage 42 zugeordnet. Die beeinflussenden Komponenten sind sich nicht ähnlich, folglich wird die Komponente als formativ eingestuft. Eine schlechte Qualität der Informationssicherheit kann durch eine schlechte Systemqualität verursacht werden. Die Servicequalität kann dennoch gut sein.

4.3.4 Interpretation

Zunächst folgt eine Übersicht über die Ergebnisse der PLS-Analyse (Abbildung 4-36).

Es fällt auf, dass der Einfluss der Prozessqualität auf die Systemqualität gering ist. Bei Betrachtung der R^2-Werte fällt auf, dass nur 32% der Varianz der Servicequalität durch die Personalqualität erklärt wird. Dies wird durch den relativ kleinen Pfadkoeffizienten von 0,26 bestätigt, d.h. der Einfluss der Personalqualität auf die Servicequalität ist in diesem Fall gering.

Weiterhin fällt auf, dass es zwei negative Koeffizienten gibt. Es könnte hier eine falsche Zuordnung vorliegen, die Fragestellungen könnten „falsch herum“ lauten, sodass eine Invertierung der Fragen in Betracht kommt, oder es besteht tatsächlich ein negativer Einfluss.

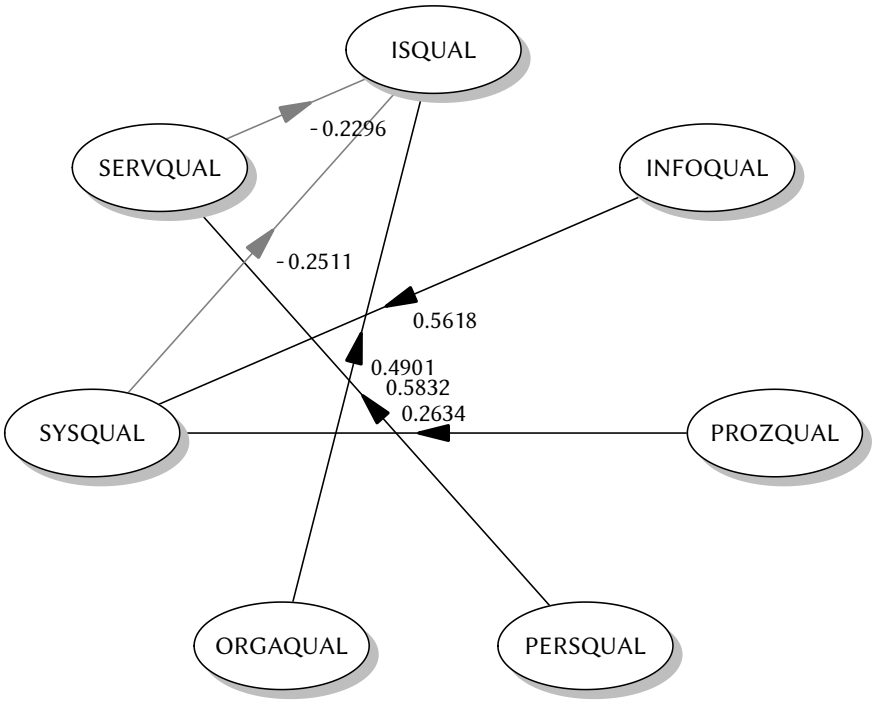
Wird ein Pfad von der Prozessqualität zur Servicequalität geführt, erreicht der R^2-Wert 54%. D.h. die Prozessqualität hat vermutlich einen nicht zu vernachlässigenden Einfluss auf die Servicequalität. Des Weiteren wird dadurch der Einfluss der Systemqualität positiv und der Pfad Prozessqualität $\rightarrow$ Systemqualität wird bedeutungslos und kann entfernt werden (Abbildung 4-37)

Dadurch steigt der relative GoF-Index von 0,75 auf 0,81. Dies entspricht nicht ganz den geforderten 0,9. Die Pfadkoeffizienten können bei Werten größer 0,3 als robust bezeichnet werden. Die Abbildungen

4-38, 4-39 und 4-40 zeigen die Ergebnisse der PLS-Analyse ohne den Pfad Prozessqualität $\rightarrow$ Systemqualität.

Die übrigen Ergebnisse der Analyse befinden sich im Anhang.

Schließlich ist der negative Koeffizient von der Servicequalität zur Informationsqualität zu erklären. Er kann nicht einfach entfernt werden, da sein Einfluss mit größer 0,3 signifikant ist. Es erscheint unwahrscheinlich, dass zwischen den beiden Komponenten ein negativer Zusammenhang besteht. Eventuell liegt ein Fehler vor. Eine Möglichkeit wäre, dass die der Servicequalität zugeordneten Fragen „falsch herum“ gestellt wurden und eine Invertierung helfen könnte. Eine Invertierung erscheint indes nicht sinnvoll. Eine andere Erklärung könnte ein Fehler im Modell an dieser Stelle sein, d.h. wenn beispielsweise die Servicequalität nicht direkt auf die Qualität der Informationssicherheit wirkt. Eine weitere Erklärung bietet die Qualität der Informationssicherheit, die von nur einem Indikator gemessen wird. Durch das Antwortverhalten mancher Teilnehmer kann es zu einer Verzerrung gekommen sein. Diesbezüglich gibt es eine Möglichkeit Gruppen innerhalb der Datensätze zu identifizieren, den REBUS-PLS-Algorithmus („Response Based Unit Segmentation in PLS Path Modeling“) (vgl. Vinzi et al. 2010, 68). Auch die nicht optimalen R^2- bzw. GoF-Werte könnten auf unbeobachtete Heterogenität im Datensatz hindeuten (vgl. Vinzi et al. 2010, 73). Es wäre denkbar, dass für Private-Cloud-Nutzer ein leicht geändertes Modell besser geeignet wäre. Dieser Test steht bisher allerdings



(a) Pfadkoeffizienten des Strukturmodells

	Type.measure	MVs	C.alpha	DG.rho	eig.1st	eig.2nd
INFOQUAL	Formative	7	0.0000000	0.0000000	2.400283	1.4600201
PROZQUAL	Reflective	4	0.7859347	0.8621094	2.443322	0.6941408
PERSQUAL	Formative	2	0.0000000	0.0000000	1.266563	0.7334365
ORGAQUAL	Reflective	4	0.5351696	0.7417835	1.712513	0.9933789
SYSQUAL	Formative	5	0.0000000	0.0000000	1.683269	1.3639006
SERVQUAL	Reflective	3	0.4395572	0.7271917	1.422879	0.8807409
ISQUAL	Formative	1	1.0000000	1.0000000	1.000000	0.0000000

(b) Homogenität und Eindimensionalität der reflektiven Komponenten

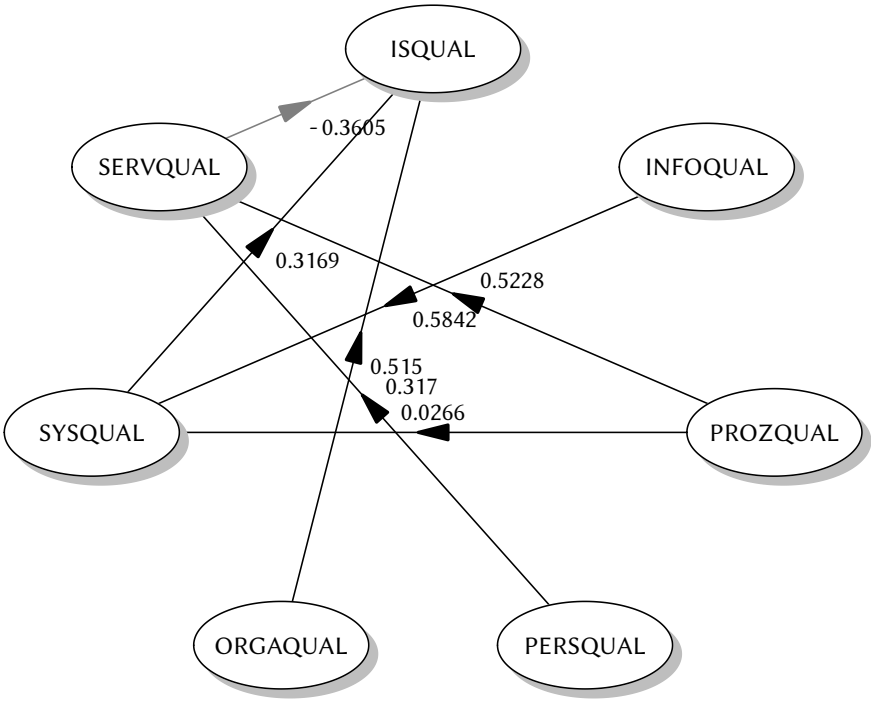
INFOQUAL	PROZQUAL	PERSQUAL	ORGAQUAL	SYSQUAL	SERVQUAL	ISQUAL
0.00	0.00	0.00	0.00	0.44	0.32	0.31

(c) R^2-Werte des Strukturmodells

	GoF	value
1	Absolute	0.3192782
2	Relative	0.7482134
3	Outer.mod	0.8286452
4	Inner.mod	0.9029358

(d) GoF-Index

Abbildung 4-36: Ergebnisse der PLS-Analyse



(a) Pfadkoeffizienten

	Type.measure	MVs	C.alpha	DG.rho	eig.1st	eig.2nd
INFOQUAL	Formative	7	0.0000000	0.0000000	2.400283	1.4600201
PROZQUAL	Reflective	4	0.7859347	0.8621094	2.443322	0.6941408
PERSQUAL	Formative	2	0.0000000	0.0000000	1.266563	0.7334365
ORGAQUAL	Reflective	4	0.5351696	0.7417835	1.712513	0.9933789
SYSQUAL	Formative	5	0.0000000	0.0000000	1.683269	1.3639006
SERVQUAL	Reflective	3	0.4395572	0.7271917	1.422879	0.8807409
ISQUAL	Formative	1	1.0000000	1.0000000	1.000000	0.0000000

(b) Homogenität und Eindimensionalität

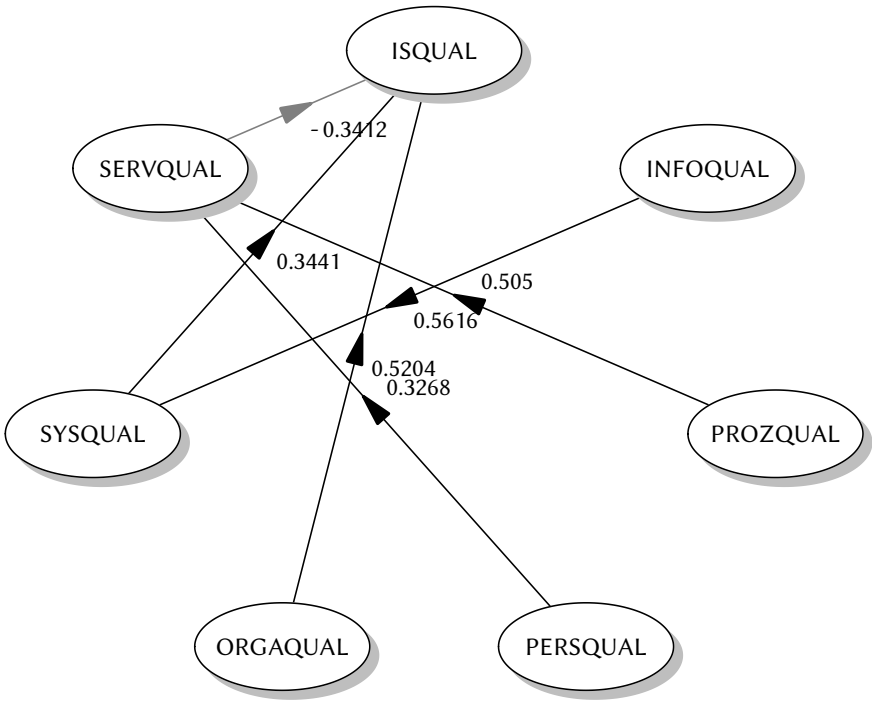
INFOQUAL	PROZQUAL	PERSQUAL	ORGAQUAL	SYSQUAL	SERVQUAL	ISQUAL
0.00	0.00	0.00	0.00	0.36	0.55	0.35

(c) R^2-Werte

	GoF	value
1	Absolute	0.3898533
2	Relative	0.8101836
3	Outer.mod	0.9176865
4	Inner.mod	0.8828545

(d) GoF-Index

Abbildung 4-37: Überarbeitetes Modell



(a) Pfadkoeffizienten

	Type.measure	MVs	C.alpha	DG.rho	eig.1st	eig.2nd
INFOQUAL	Formative	7	0.0000000	0.0000000	2.400283	1.4600201
PROZQUAL	Reflective	4	0.7859347	0.8621094	2.443322	0.6941408
PERSQUAL	Formative	2	0.0000000	0.0000000	1.266563	0.7334365
ORGAQUAL	Reflective	4	0.5351696	0.7417835	1.712513	0.9933789
SYSQUAL	Formative	5	0.0000000	0.0000000	1.683269	1.3639006
SERVQUAL	Reflective	3	0.4395572	0.7271917	1.422879	0.8807409
ISQUAL	Formative	1	1.0000000	1.0000000	1.000000	0.0000000

(b) Homogenität und Eindimensionalität

INFOQUAL	PROZQUAL	PERSQUAL	ORGAQUAL	SYSQUAL	SERVQUAL	ISQUAL
0.00	0.00	0.00	0.00	0.32	0.54	0.37

(c) R^2-Werte

	GoF	value
1	Absolute	0.3753661
2	Relative	0.8019874
3	Outer.mod	0.8997216
4	Inner.mod	0.8913729

(d) GoF-Index

Abbildung 4-38: Dritte Version des Modells

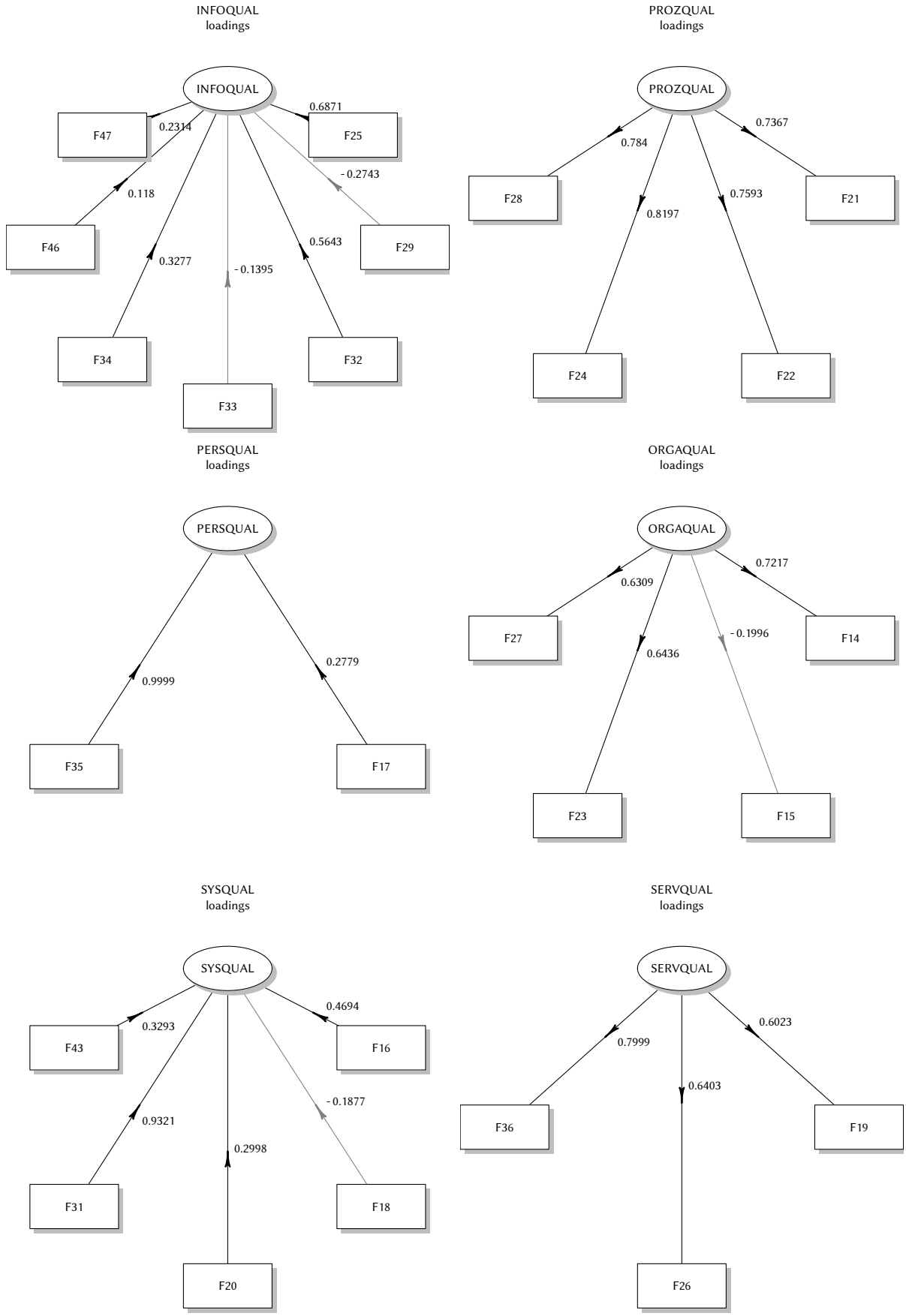


Abbildung 4-39: Ladungen der manifesten Variablen auf die latenten Komponenten

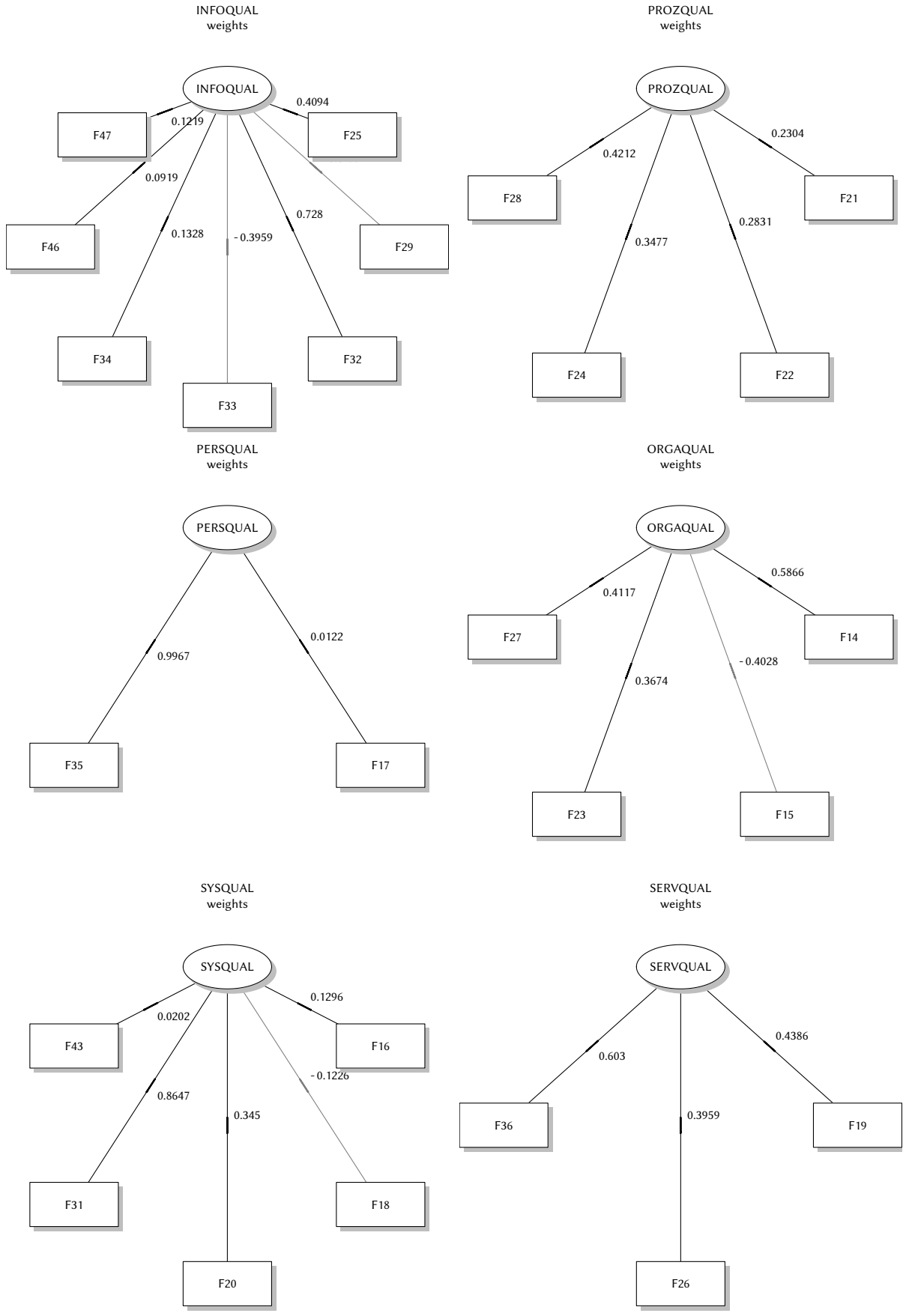


Abbildung 4-40: Gewichte der manifesten Variablen

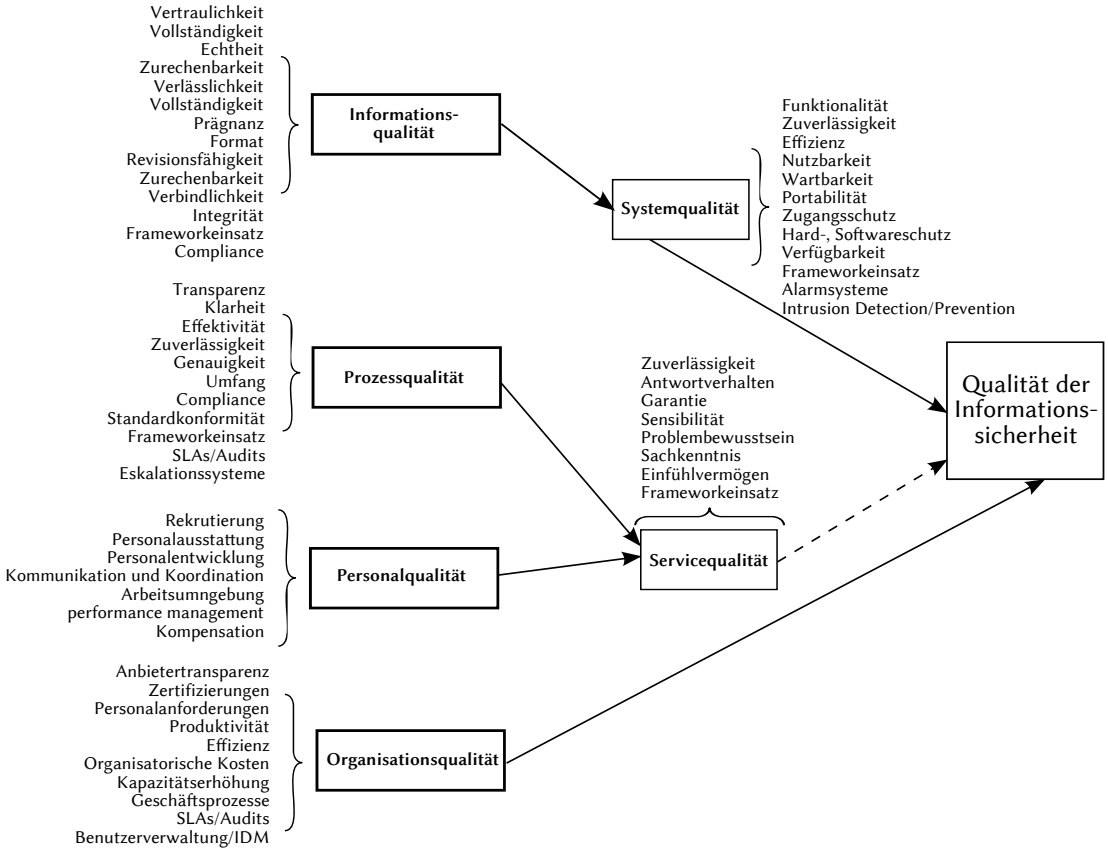


Abbildung 4-41: Überarbeitetes Modell zur Informationssicherheit im Cloud-Computing

nur für rein reflektive Modelle zur Verfügung, die Integration für formative befindet sich momentan in der Entwicklung (vgl. Vinzi et al. 2010, 71).

Das engültige Modell ist in Abbildung 4-41 dargestellt.

5 Fazit

Cloud-Computing verspricht sowohl Zeit- und Kosteneinsparungen als auch eine Risikoreduktion gegenüber traditioneller IT (vgl. Baun et al. 2010, 87). Daher war Cloud-Computing das „Top-Thema“ der CeBIT 2011 (vgl. Deutsche Messe AG 2011, 1) und ist laut Umfrage der Bitkom (2011, 1) wichtigster IT-Trend 2011. Durch dynamische Ressourcenallokation, Kostentransparenz und verursachungsgerechte Bezahlung ist das Interesse groß. Es werden nur noch Dienste und Ressourcen bezahlt, die auch aktiv genutzt werden. Die neuen Strukturen bringen neue Gefahren mit sich. Einige Aspekte der Informationssicherheit in der traditionellen IT verlieren an Bedeutung, andere rücken in den Vordergrund oder erscheinen neu. Um diese Entwicklung zu beleuchten, insbesondere die Möglichkeit der Bewältigung von Gefahren der Informationssicherheit aufzuzeigen, wurde eine empirische Studie durchgeführt; letztlich wurde hieraus ein Modell entwickelt, welches fähig ist die Informationssicherheit zu bewerten.

Gefährdungen und Anforderungen an die Informationssicherheit Die geänderten Strukturen im Cloud-Computing bedeuten, dass geänderte Gefährdungslagen und Sicherheitsaspekte, beachtet werden müssen. Diese sind sowohl technischer als datenschutzrechtlicher Natur.

Das meistgenannte Argument gegen Cloud-Computing stellt der Kontrollverlust dar (Abbildung 4-13 auf Seite 44). Die Hoheit über die Daten liegt nicht mehr beim Nutzer, sondern beim Betreiber. Dieser kann oder will oft nicht garantieren, dass die Daten „sicher“ sind. Daher ist Vertrauen ein wichtiger Aspekt bei der Informationssicherheit. Dies ist aus den Abbildungen 4-13 auf Seite 44 und 4-18 auf Seite 49 ersichtlich. Cloud-Dienstleister aus den USA übergeben Daten an amerikanische Institutionen, auch wenn die Daten ausschließlich in europäischen Rechenzentren gespeichert bzw. verarbeitet werden (vgl. Kirsch 2011b; Stölzel 2011, 1). Dies widerspricht den europäischen Datenschutzgesetzen, wenn es sich um personenbezogene Daten handelt. Daher sorgt die nicht auf den Euro-Raum begrenzbare Datenhaltung bei vielen Nutzern für Bedenken bei der Nutzung von Cloud-Computing: Unvereinbarkeit mit Datenschutzgesetze ist einer der wichtigsten Gründe für Ablehnung von Cloud-Computing (Abbildung 4-13 auf Seite 44). Das eben genannte Beispiel zu Cloud-Dienstleistern aus den USA verdeutlicht ein weiteres Problem: Die Dienstleister stehen in dem Konflikt, welche Gesetze sie brechen müssen, die europäischen oder die amerikanischen. Diese Inkonsistenz der Gesetze ist ein weiterer wichtiger Aspekt, der die Nutzung des Cloud-Computing beeinflusst (Abbildung 4-13 auf Seite 44). Daher fordert die in den USA ansässige Firma Dell, die derzeit in Europa Cloud-Rechenzentren aufbaut, eine Harmonisierung der Gesetzeslage (vgl. Kirsch 2011a, 1). Mit der momentanen Gesetzeslage bzw. den unzureichenden Prozeduren und Standards (Frage 41, Abbildung 4-22 auf Seite 53) zur Umsetzung der Anforderungen,

ist es fraglich, ob die durch Gesetze und andere Vorgaben entstehenden Kosten durch die Vorteile des Cloud-Computing ausgeglichen werden können (vgl. Duisberg 2011, 60).

Aus technischer Sicht steht der Anwender auf eine Stufe mit dem Angreifer: Beide greifen von außen auf Dienste und Daten zu. Da beide über das selbe physikalische Medium (Internet) zugreifen (vgl. Schwenk 2011, 74), ergibt sich ein Problem für traditionelle Sicherheitsmechanismen: Firewalls müssen jetzt zwischen Angreifer und Nutzer unterscheiden können und nicht lediglich Systeme abschotten. Daher kommt dem Identitätsmanagement die wichtigste Rolle bei der Informationssicherheit im Cloud-Computing zu (Abbildung 4-26 auf Seite 58).

VPNs zur virtuellen Integration der Cloud-Dienste in die Unternehmensnetze werden ebenfalls als sehr wichtig eingeschätzt (ebd.). Durch die Übernahme von Sicherheitsaufgaben durch den Dienstleister werden klare Strukturen und Alarm- und Eskalationssysteme sowie Intrusion-Detection- und -Preventionsysteme erforderlich (Frage 28, Abbildungen 4-17 auf Seite 48 und 4-26 auf Seite 58). Backups spielen auch nach wie vor eine wichtige Rolle (ebd. und Frage 33, Abbildung 4-19 auf Seite 50), obwohl eine Cloud-Infrastruktur dies hätte erübrigen können.

Modell zur Informationssicherheit im Cloud-Computing Um die angesprochenen Probleme zu katalogisieren und geeignete Maßnahmen zur Bewältigung zu finden, wurde ein hypothetisches Modell entwickelt (Abbildung 3.3 auf Seite 31). Die Entwicklung erfolgte über das häufig eingesetzte Modell zum Erfolg von Informationssystemen von DeLone/McLean (1992, 2003) und dem daraus abgeleiteten Qualitätsmodell von Rodríguez/Casanovas (2010). Mit Hilfe der Studienergebnisse wurde das resultierende Modell überprüft und verfeinert (Abbildung 4-41 auf Seite 80). Das Modell besteht aus sechs Qualitätskomponenten, die miteinander interagieren. Sie wirken sich direkt oder indirekt auf die Informationssicherheit im Cloud-Computing aus. Mit den vorliegenden Daten konnten nicht alle Gütekriterien, die ein gutes „Model-Fit“ attestieren würden, deutlich erfüllt werden. Das muss allerdings nicht bedeuten, dass dieses Modell falsch ist. Der Pfad Servicequalität → Qualität der Informationssicherheit konnte nicht bestätigt werden, da er einen negativen Einfluss auf die Informationssicherheit zu haben scheint. Ein Grund könnte die falsche Zuordnung der Indikatorvariablen sein oder eine Fehlerhaftigkeit der erhobenen Daten. Dass es hier in der Realität einen negativen Zusammenhang gibt, erscheint fragwürdig. Eine nachfolgende Untersuchung mit speziell auf dieses Modell abgestimmten Indikatorvariablen könnte hier Klarheit schaffen.

Weitere Forschungsansätze Die größten Herausforderungen zur Bewältigung der Informationssicherheit im Cloud-Computing können in drei Klassen eingeteilt werden.

1. Standards und Prozeduren sollten angepasst oder geschaffen werden, damit die gesetzlichen und unternehmerischen Anforderungen an die Informationssicher-

heit gewährleistet werden können. Durch die speziellen Strukturen im Cloud-Computing kommt dem gegenseitigen Vertrauen eine besondere Bedeutung zu. Dieses kann vor allem durch Transparenz aufgebaut werden. Hier fehlen geeignete Prozeduren, die die nötige Transparenz gewährleisten können. Offene Standards zur einfachen Übertragung von Cloud-Instanzen über Anbietergrenzen hinweg bedürfen ebenfalls der Weiterentwicklung um die versprochene Flexibilität zu gewährleisten und Anbieterabhängigkeiten zu reduzieren.

2. Das Bewusstsein für effektive Verschlüsselung muss gestärkt werden, wie in Kapitel 2.2.3 erwähnt bestehen Defizite bei der Umsetzung; die Implementierungen einiger Anbieter sind unbrauchbar. Eine mögliche Umgehung vieler Probleme würde die vollhomomorphe Verschlüsselung bieten. Eine solche wird in den nächsten Jahre für den produktiven Einsatz noch nicht zur Verfügung stehen.

3. Gesetze könnten den besonderen Bedingungen des Cloud-Computings angepasst werden. Insbesondere sollten Lösungen für länderübergreifende Gesetzeskonflikte gefunden werden.

In erster Linie kann empfohlen werden, zu prüfen ob eine Private- oder eine Community-Cloud in Frage kommt, da hier die Auflagen und Risiken wesentlich einfacher zu handhaben sind, als in der Public-Cloud. Vor einer Nutzung von Public-Cloud-Lösungen muss geprüft werden, wie kritisch die zu verarbeitenden Daten einzustufen sind und ob durch die Nutzung Normen verletzt werden. Oft können nur innereuropäische Cloud-Dienstleister zuverlässige Garantien für den Verbleib von Daten geben. Weiterhin ist die sichere Ausgestaltung von SLAs ein wichtiger Aspekt. Wichtig ist die Entwicklung von Kennzahlen, um Sicherheit im Cloud-Computing messen zu können. Dies wäre ein erster Schritt auf dem Weg zum Controlling von Informationssicherheit im Cloud-Computing.

6 Anhang

Fragebogen

Fragebogen zur Informationssicherheit im Cloud Computing

— Im Rahmen der Diplomarbeit von Atman Sense – Telefon: 0551 9950864 – atman.sense@stud.uni-goettingen.de —
— Betreuung: Dipl.-Wirt.-Inf. Tobias F. Langkau – Telefon: 0551 399736 – tobias.langkau@wiwi.uni-goettingen.de —

Rücksendeadresse: Professur für Informationsmanagement · Platz der Göttinger Sieben 5 · 37073 Göttingen
Tel.: 0551 394440 · Fax: 0551 399735

Ich wünsche eine Zusendung der Ergebnisse per E-Mail an: _____

☐: Mehrfachnennung; ○: Einfachnennung; k.A.: keine Antwort

Allgemeine Fragen zum Unternehmen und dem IT-Bereich

01. Wie viele Mitarbeiter sind in Ihrem Unternehmen beschäftigt (FTE)? ○<100 ○<500 ○<1000 ○<5000 ○≥5000

02. In welcher Branche ist Ihr Unternehmen aktiv? ☐ Information und Telekommunikation ☐ Handel, Verkehr ☐ Baugewerbe ☐ produzierendes Gewerbe ☐ Finanzen ☐ Andere: _____

03. Wie hoch war der Jahresumsatz Ihres Unternehmens im Jahr 2010 in Mio. €? ○<5 ○<10 ○<50 ○<500 ○≥500

04. Welche Normen oder Compliance-Anforderungen finden bei Ihnen Berücksichtigung? ☐ Basel II/Solvency II ☐ Bundesdatenschutzgesetz (BDSG) ☐ Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) ☐ Telemediengesetz (TMG) ☐ Signaturgesetz/Signaturverordnung (SigG/SigV) ☐ Sarbanes Oxley Act (SOX) ☐ Telekommunikationsgesetz/Telekommunikations-Überwachungsverordnung (TKG/TKÜV) ☐ Zugangskontrolldiensteschutz-Gesetz (ZKDSG) ☐ Andere: _____

05. Welche Standards und Frameworks werden bei Ihnen angewandt? ☐ CobiT ☐ ITIL ☐ ISO 2700x (bzw. BS 7799) ☐ BSI IT-Grundschutz ☐ ISO 13335 ☐ Common Criteria (ISO 15408 bzw. ITSEC) ☐ OCTAVE ☐ MEHARI ☐ NIST SP 800 ☐ FIRM ☐ Keine ☐ Andere: _____

06. Findet ein Controlling der Informationssicherheit statt bzw. sind Effizienz und Reifegrad im Blickfeld? ☐ ISO 27004 ☐ NIST SP 800-55 ☐ CISWG Best Practices ☐ FIRM Scorecards ☐ Nein ☐ Andere: _____

Allgemeine Fragen zur Nutzung von Cloud Computing

07. Nutzt Ihr Unternehmen Cloud Computing? ☐ Private Cloud ☐ Public Cloud ☐ Hybrid Cloud ☐ Nein

08. Wenn ja, seit wann? _____

09. Welche Nutzungsformen setzen Sie vorwiegend ein? ☐ IaaS ☐ PaaS ☐ SaaS ☐ Keine

10. Warum nutzt Ihr Unternehmen Cloud Computing? ☐ Kosten ☐ Informationssicherheit ☐ Flexibilität ☐ Image ☐ Verfügbarkeit ☐ Effizienz ☐ Andere: _____

11. Was hält Ihr Unternehmen von der Nutzung von Cloud Computing ab? ☐ fehlende Standards ☐ Image-Verlust ☐ Inkonsistenz der Gesetze über Ländergrenzen hinweg ☐ unsichere Schnittstellen/APIs ☐ Abhängigkeit vom Anbieter ☐ schlechte Verfügbarkeit ☐ unsichere Cloud-Infrastruktur (Hypervisor etc.) ☐ mangelndes Vertrauen ☐ Migrationskosten/-probleme ☐ Kontrollverlust ☐ Datenschutzgesetze ☐ Andere: _____

12. Welche Daten verarbeiten Sie in der Public/Hybrid Cloud? ☐ keine vertraulichen Daten ☐ personenbezogene Daten ☐ unternehmenskritische Daten ☐ k.A. ☐ Andere: _____

13. Erwägen Sie Cloud Computing wegen anhaltender Probleme nicht mehr zu nutzen? ○ Ja ○ Nein ○ k.A. ○ Andere: _____

Kriterien für die Anbieterauswahl	unwichtig				wichtig	k. A.
14. Transparenz des Anbieters	○	○	○	○	○	○
15. Zertifizierungen/externe Audits des Anbieters	○	○	○	○	○	○
16. Mehrstufige Authentifizierungen	○	○	○	○	○	○
17. Wie und welche Mitarbeiter der Anbieter einstellt	○	○	○	○	○	○
18. Überprüfung der physischen Sicherheit des Anbieters (Zugangs- und Katastrophenschutz)	○	○	○	○	○	○
19. Regelungen, wie bei Auflösung/Übernahme des Anbieters zu verfahren ist	○	○	○	○	○	○
20. Der Anbieter sollte Daten auf verschiedenen Sites vorhalten (Vorbeugung vor Datenverlust, Erhöhung der Verfügbarkeit)	○	○	○	○	○	○
21. Kontrollpflichten des Anbieters (z.B. über SLAs)	○	○	○	○	○	○
22. Prüfungsrechte des Kunden (z.B. über SLAs)	○	○	○	○	○	○
23. Dritte dürfen keinen Zugang zur Infrastruktur/Datenhaltung des Anbieters haben	○	○	○	○	○	○
24. Festlegung von Verantwortlichkeiten und Haftungen bei Sicherheitsvorfällen (z.B. über SLAs)	○	○	○	○	○	○
25. Konsequente Verschlüsselung von Daten, sodass nur sich in Bearbeitung befindliche Daten unverschlüsselt vorliegen	○	○	○	○	○	○
26. Reporting des Anbieters über Sicherheitsvorfälle (Informationspflicht nach § 42a BDSG)	○	○	○	○	○	○
27. Vom Anbieter versprochene Sicherheit muss nachvollziehbar sein	○	○	○	○	○	○
28. Vereinbarung klarer Prozesse im Fall von Datenverlusten	○	○	○	○	○	○
29. Physikalische Aufbewahrung der Daten ausschließlich innerhalb der EU	○	○	○	○	○	○

30. Wie stellen Sie das Vertrauen zum Anbieter sicher? ☐ SLAs (z.B. Vertragsstrafen) ☐ Audits ☐ gar nicht ☐ Andere: _____

bitte wenden

Abbildung 6-1: Fragebogen Seite 1

Kriterien für die Nutzung von Cloud Computing (bezogen auf Informationssicherheit)	unwichtig				wichtig	k. A.
31. Berücksichtigung des Browsers (als Universalclient mit vielen Angriffspunkten)	○	○	○	○	○	○
32. Klassifikation von Daten mit Richtlinien zur Weitergabe/Löschung	○	○	○	○	○	○
33. Backups außerhalb des Cloud-Dienstleisters	○	○	○	○	○	○
34. Ausschließlich verschlüsselte Daten in die Public/Hybrid Cloud auslagern	○	○	○	○	○	○
35. Schulung der Mitarbeiter im Umgang mit Cloud Computing und dessen Sicherheitsaspekten	○	○	○	○	○	○
36. Regelung möglichst aller Schadensszenarien (z.B. durch SLAs)	○	○	○	○	○	○
37. Um die Browsersicherheit zu erhöhen, werden folgende Maßnahmen ergriffen ☐ Browservorgabe ☐ Verbote für Erweiterungen ☐ Hardcodierte Sperren im Browser ☐ Keine ☐ Andere: _____						
38. Personenbezogene Daten können in einer Public/Hybrid Cloud ungewollt in ein unsicheres Drittland übermittelt werden. Wie gehen sie mit der Anforderung um, dass diese Daten nicht übermittelt werden dürfen (§ 4b BDSG)? ☐ solche Daten werden nicht ausgelagert ☐ Einwilligung wird eingeholt ☐ wird ignoriert ☐ nur verschlüsselte Speicherung ☐ Vereinbarung über Verbleib der Daten innerhalb der EU/EWR/safe harbor ☐ Andere: _____						

Fragen zu konkreten Auswirkungen in Ihrem Unternehmen	trifft nicht zu				trifft voll zu	k.A.
39. Auslagern von Sicherheitsmaßnahmen in Form von Security-as-a-Service ist sinnvoll und sicher (Proxy, Spam- und Virenschutz)	○	○	○	○	○	○
40. Datenschutzsensible Standardanwendungen auszulagern, ist sinnvoll und sicher (Mail, Office, Anwendungsentwicklung)	○	○	○	○	○	○
41. Die neuen Gefahren des Cloud Computing sind durch bestehende Standards und Sicherheits-Frameworks ausreichend abgedeckt	○	○	○	○	○	○
42. Das Konzept Ihres Unternehmens zum Informationssicherheitsmanagement im Cloud Computing ist gut	○	○	○	○	○	○
43. Die Ausgaben für die Informationssicherheit sind gestiegen	○	○	○	○	○	○
44. Der Wechsel zu Cloud Computing hat sich aus finanzieller Sicht gelohnt	○	○	○	○	○	○
45. Eine Private Cloud verspricht weniger Sicherheitsrisiken bei verringerter Vorteilhaftigkeit; sie ist dennoch vorteilhaft gegenüber traditioneller IT-Landschaft	○	○	○	○	○	○
46. Nicht-EU-Anbietern mit „safe harbor"-Abkommen kann man nicht vertrauen	○	○	○	○	○	○
47. Die Gefährdung durch unbemerkte staatliche Eingriffe bei Nicht-EU-Anbietern (z.B. durch „national security letters"), auch wenn die Datenhaltung in der EU garantiert wird bzw. das „safe harbor"-Abkommen unterzeichnet wurde, ist hoch	○	○	○	○	○	○
48. Effizienz im Informationssicherheitsmanagement lässt sich bei Cloud Computing leichter erreichen	○	○	○	○	○	○
49. Schadenssummen bei Vorfällen mit Cloud Computing sind gestiegen	○	○	○	○	○	○

Fragen zu Sicherheitsvorfällen im Cloud Computing

50. Welche Sicherheitsvorfälle traten in der Vergangenheit auf, die im Zusammenhang mit Cloud Computing standen?
51. Welche Vorfälle, die ohne Cloud Computing auftraten, treten mit Cloud Computing vermindert auf?
52. Welche Vorfälle treten seit Nutzung von Cloud Computing vermehrt auf?

50. 51. 52.		50. 51. 52.	
☐ ☐ ☐	Manipulation mit dem Ziel der Bereicherung	☐ ☐ ☐	Sabotage
☐ ☐ ☐	Nachlässigkeit und Irrtum der eigenen Mitarbeiter	☐ ☐ ☐	Softwareseitige Mängel und Defekte
☐ ☐ ☐	Unbeabsichtigte Fehler von Externen	☐ ☐ ☐	Hardwareseitige Mängel und Defekte
☐ ☐ ☐	Dokumentationsseitige Mängel und Defekte	☐ ☐ ☐	Malware (Würmer, Viren, Trojaner)
☐ ☐ ☐	Höhere Gewalt (Feuer, Erdbeben, Sturm, Wasser, etc.)	☐ ☐ ☐	Unsichere Mandantentrennung
☐ ☐ ☐	Unzureichende Löschung nach Abschluss einer Session	☐ ☐ ☐	Ausbruch aus dem virtuellen System
☐ ☐ ☐	Informationsdiebstahl, Spionage, unbefugte Kenntnisnahme	☐ ☐ ☐	Hacking, Vandalismus, Missbrauch

☐ ☐ ☐ Andere Gefahrenbereiche: _____

53. Welche Ziele der Informationssicherheit wurden dadurch verletzt?
54. Welche Ziele der Informationssicherheit haben besondere Priorität?

53. 54.		53. 54.		53. 54.		53. 54.	
☐ ☐	Revisionsfähigkeit	☐ ☐	Verfügbarkeit	☐ ☐	Integrität (Unversehrtheit, Verlässlichkeit)	☐ ☐	Authentizität (Echtheit, Zurechenbarkeit)
☐ ☐	Vertraulichkeit	☐ ☐	Nichtabstreitbarkeit, Verbindlichkeit				

55. Welche Konsequenzen hatten die Vorfälle? ☐ Imageschaden ☐ Kunden/Aufträge verloren ☐ Abmahnung, Versetzung, Entlassung von Mitarbeitern ☐ Strafanzeige gegen Verursacher ☐ Informationen wurden missbräuchlich durch Dritte verwendet ☐ Strafen gegenüber Ihrer Firma oder Mitarbeitern ☐ Andere: _____
56. Welche Bausteine eines Informationssicherheitsmanagements sind Ihrer Meinung nach bzgl. Cloud Computing besonders relevant? ☐ Benutzerverwaltung/Identity Management ☐ VPN ☐ Alarm- und Eskalationssystem ☐ Intrusion Detection/Prevention ☐ Backup ☐ Firewalls ☐ Virenschutz ☐ Spamabwehr ☐ Protokollierung von Zugriffen ☐ Schnittstellenüberwachung ☐ physische Sicherheit ☐ Verschlüsselung ☐ elektronische Signaturen ☐ zentrales Controlling eingesetzter Sicherheitssysteme ☐ Andere: _____

Optionale Anmerkungen

Vielen Dank für Ihre Unterstützung

Abbildung 6-2: Fragebogen Seite 2

Ergebnisse der PLS-Analyse der dritten Modellversion

```
PARTIAL LEAST SQUARES PATH MODELING (PLS-PM)

------------------------------------------------------------
MODEL SPECIFICATION
1   Number of Cases   58
2   Latent Variables   7
3   Manifest Variables   26
4   Scale of Data   Standardized Data
5   Weighting Scheme   centroid
6   Tolerance Crit   1e-05
7   Max Num Iters   100
8   Convergence Iters   48
9   Paths by PLS-R   FALSE
10  Bootstrapping   TRUE
11  Bootstrap samples   100

------------------------------------------------------------
BLOCKS DEFINITION
       Block          Type   NMVs         Mode
1   INFOQUAL     Exogenous      7    Formative
2   PROZQUAL     Exogenous      4   Reflective
3   PERSQUAL     Exogenous      2    Formative
4   ORGAQUAL     Exogenous      4   Reflective
5    SYSQUAL    Endogenous      5    Formative
6   SERVQUAL    Endogenous      3   Reflective
7     ISQUAL    Endogenous      1    Formative

------------------------------------------------------------
BLOCKS UNIDIMENSIONALITY
          Type.measure  MVs  C.alpha  DG.rho  eig.1st  eig.2nd
INFOQUAL     Formative    7    0.000   0.000     2.40    1.460
PROZQUAL    Reflective    4    0.786   0.862     2.44    0.694
PERSQUAL     Formative    2    0.000   0.000     1.27    0.733
ORGAQUAL    Reflective    4    0.535   0.742     1.71    0.993
SYSQUAL      Formative    5    0.000   0.000     1.68    1.364
SERVQUAL    Reflective    3    0.440   0.727     1.42    0.881
ISQUAL       Formative    1    1.000   1.000     1.00    0.000

------------------------------------------------------------
OUTER MODEL
          weights  std.loads  communal  redundan
INFOQUAL
  F25      0.4094      0.687    0.4722    0.0000
  F29     -0.6199     -0.274    0.0753    0.0000
  F32      0.7280      0.564    0.3185    0.0000
  F33     -0.3959     -0.140    0.0195    0.0000
  F34      0.1328      0.328    0.1074    0.0000
  F46      0.0919      0.118    0.0139    0.0000
  F47      0.1219      0.231    0.0535    0.0000
PROZQUAL
  F21      0.2304      0.737    0.5427    0.0000
  F22      0.2831      0.759    0.5765    0.0000
  F24      0.3477      0.820    0.6719    0.0000
  F28      0.4212      0.784    0.6147    0.0000
PERSQUAL
```

F17	0.0122	0.278	0.0772	0.0000
F35	0.9967	1.000	0.9999	0.0000
ORGAQUAL				
F14	0.5866	0.722	0.5209	0.0000
F15	-0.4028	-0.200	0.0398	0.0000
F23	0.3674	0.644	0.4142	0.0000
F27	0.4117	0.631	0.3981	0.0000
SYSQUAL				
F16	0.1296	0.469	0.2203	0.0695
F18	-0.1226	-0.188	0.0352	0.0111
F20	0.3450	0.300	0.0899	0.0283
F31	0.8647	0.932	0.8688	0.2740
F43	0.0202	0.329	0.1084	0.0342
SERVQUAL				
F19	0.4386	0.602	0.3627	0.1941
F26	0.3959	0.640	0.4100	0.2194
F36	0.6030	0.800	0.6398	0.3424
ISQUAL				
F42	1.0000	1.000	1.0000	0.3710

CORRELATIONS BETWEEN MVs AND LVs

	INFOQUAL	PROZQUAL	PERSQUAL	ORGAQUAL	SYSQUAL	SERVQUAL	ISQUAL
INFOQUAL							
F25	0.6871	0.0333	0.2404	-0.0201	0.3841	0.2090	0.0261
F29	-0.2743	0.2126	0.2980	0.1561	-0.1555	0.2750	-0.0898
F32	0.5643	0.3658	0.6154	0.4238	0.3161	0.5209	0.1118
F33	-0.1395	0.1407	0.4108	0.0574	-0.0811	0.3267	-0.2205
F34	0.3277	0.1654	0.3873	-0.0181	0.1815	0.4569	-0.1505
F46	0.1180	-0.1360	-0.1151	0.3101	0.0651	0.0435	0.1597
F47	0.2314	0.1608	0.2670	0.2940	0.1280	0.3220	0.0958
PROZQUAL							
F21	-0.0236	0.7367	0.4896	0.3470	-0.0337	0.3613	0.1627
F22	-0.0131	0.7593	0.4039	0.3163	-0.0336	0.4439	0.0239
F24	0.0357	0.8197	0.2663	0.1748	0.0088	0.5451	0.0332
F28	0.2809	0.7840	0.4878	0.3210	0.2127	0.6603	0.1330
PERSQUAL							
F17	0.0136	0.1225	0.2779	0.1465	0.1584	0.1645	-0.0164
F35	0.2733	0.5255	0.9999	0.4711	0.0707	0.5919	0.0834
ORGAQUAL							
F14	0.2089	0.1816	0.2998	0.7217	-0.0630	0.2762	0.3007
F15	0.1348	0.1382	0.1033	-0.1996	0.1071	0.2563	-0.2065
F23	0.2214	0.2437	0.3331	0.6436	0.1039	0.2793	0.1883
F27	0.2261	0.5467	0.5214	0.6309	0.2532	0.5061	0.2111
SYSQUAL							
F16	0.3985	0.0648	0.3366	-0.0046	0.4694	0.2898	0.0237
F18	-0.0907	0.0581	0.0371	0.1388	-0.1877	0.1598	-0.0789
F20	0.1597	0.0897	0.1284	0.2274	0.2998	0.1821	0.1100
F31	0.5073	0.0496	-0.0175	0.0046	0.9321	0.0288	0.3326
F43	0.2474	0.0131	0.2026	-0.1238	0.3293	0.1636	0.0490
SERVQUAL							
F19	0.1431	0.3203	0.3268	-0.0520	0.0132	0.6023	-0.2020
F26	0.2786	0.3772	0.3621	0.2996	0.1343	0.6403	-0.0272
F36	0.1589	0.6414	0.5063	0.4544	0.0831	0.7999	-0.0197
ISQUAL							
F42	0.2413	0.1118	0.0829	0.4157	0.3393	-0.1113	1.0000

```
INNER MODEL
$SYSQUAL
        concept  value
1            R2 0.3153
2     Intercept 0.0000
3 path_INFOQUAL 0.5616

$SERVQUAL
        concept  value
1            R2 0.5351
2     Intercept 0.0000
3 path_PROZQUAL 0.5050
4 path_PERSQUAL 0.3268

$ISQUAL
        concept   value
1            R2  0.3710
2     Intercept  0.0000
3 path_ORGAQUAL  0.5204
4  path_SYSQUAL  0.3441
5 path_SERVQUAL -0.3412

------------------------------------------------------------
CORRELATIONS BETWEEN LVs
          INFOQUAL  PROZQUAL  PERSQUAL  ORGAQUAL  SYSQUAL  SERVQUAL   ISQUAL
INFOQUAL     1.000    0.1216    0.2725    0.2427   0.5616     0.269   0.2413
PROZQUAL     0.122    1.0000    0.5252    0.3655   0.0754     0.677   0.1118
PERSQUAL     0.273    0.5252    1.0000    0.4713   0.0724     0.592   0.0829
ORGAQUAL     0.243    0.3655    0.4713    1.0000   0.0623     0.370   0.4157
SYSQUAL      0.562    0.0754    0.0724    0.0623   1.0000     0.109   0.3393
SERVQUAL     0.269    0.6766    0.5920    0.3698   0.1090     1.000  -0.1113
ISQUAL       0.241    0.1118    0.0829    0.4157   0.3393    -0.111   1.0000

------------------------------------------------------------
SUMMARY INNER MODEL
          LV.Type  Measure  MVs  R.square  Av.Commu  Av.Redun    AVE
INFOQUAL   Exogen    Frmtv    7     0.000     0.151    0.0000  0.000
PROZQUAL   Exogen    Rflct    4     0.000     0.601    0.0000  0.601
PERSQUAL   Exogen    Frmtv    2     0.000     0.538    0.0000  0.000
ORGAQUAL   Exogen    Rflct    4     0.000     0.343    0.0000  0.343
SYSQUAL   Endogen    Frmtv    5     0.315     0.265    0.0834  0.000
SERVQUAL  Endogen    Rflct    3     0.535     0.471    0.2520  0.471
ISQUAL    Endogen    Frmtv    1     0.371     1.000    0.3710  0.000

------------------------------------------------------------
GOODNESS-OF-FIT
         GoF   value
1   Absolute  0.3754
2   Relative  0.8020
3  Outer.mod  0.8997
4  Inner.mod  0.8914

------------------------------------------------------------
TOTAL EFFECTS
         relationships  dir.effects  ind.effects  tot.effects
1   INFOQUAL->PROZQUAL        0.000        0.000        0.000
2   INFOQUAL->PERSQUAL        0.000        0.000        0.000
3   INFOQUAL->ORGAQUAL        0.000        0.000        0.000
```

4	INFOQUAL->SYSQUAL	0.562	0.000	0.562
5	INFOQUAL->SERVQUAL	0.000	0.000	0.000
6	INFOQUAL->ISQUAL	0.000	0.193	0.193
7	PROZQUAL->PERSQUAL	0.000	0.000	0.000
8	PROZQUAL->ORGAQUAL	0.000	0.000	0.000
9	PROZQUAL->SYSQUAL	0.000	0.000	0.000
10	PROZQUAL->SERVQUAL	0.505	0.000	0.505
11	PROZQUAL->ISQUAL	0.000	-0.172	-0.172
12	PERSQUAL->ORGAQUAL	0.000	0.000	0.000
13	PERSQUAL->SYSQUAL	0.000	0.000	0.000
14	PERSQUAL->SERVQUAL	0.327	0.000	0.327
15	PERSQUAL->ISQUAL	0.000	-0.112	-0.112
16	ORGAQUAL->SYSQUAL	0.000	0.000	0.000
17	ORGAQUAL->SERVQUAL	0.000	0.000	0.000
18	ORGAQUAL->ISQUAL	0.520	0.000	0.520
19	SYSQUAL->SERVQUAL	0.000	0.000	0.000
20	SYSQUAL->ISQUAL	0.344	0.000	0.344
21	SERVQUAL->ISQUAL	-0.341	0.000	-0.341

BOOTSTRAP VALIDATION

weights

	Original	Mean.Boot	Std.Error	perc.05	perc.95
F25	0.4094	0.09875	3.80e-01	-0.52816	0.617
F29	-0.6199	-0.33628	3.14e-01	-0.73684	0.198
F32	0.7280	0.45656	3.58e-01	-0.14755	0.955
F33	-0.3959	-0.10556	5.00e-01	-0.76428	0.763
F34	0.1328	0.00935	3.19e-01	-0.53085	0.562
F46	0.0919	0.14234	3.37e-01	-0.33336	0.721
F47	0.1219	-0.01654	2.77e-01	-0.43776	0.451
F21	0.2304	0.22527	7.21e-02	0.09949	0.311
F22	0.2831	0.28841	4.95e-02	0.22280	0.368
F24	0.3477	0.33136	5.72e-02	0.23476	0.408
F28	0.4212	0.43690	1.26e-01	0.29219	0.656
F17	0.0122	0.00102	2.26e-01	-0.36575	0.333
F35	0.9967	0.97277	8.06e-02	0.85004	1.065
F14	0.5866	0.53177	2.20e-01	0.24727	0.764
F15	-0.4028	-0.33539	3.40e-01	-0.73396	0.153
F23	0.3674	0.31790	1.73e-01	0.03820	0.527
F27	0.4117	0.35821	1.65e-01	0.00748	0.586
F16	0.1296	-0.08836	5.39e-01	-0.84369	0.785
F18	-0.1226	0.01890	3.05e-01	-0.43368	0.557
F20	0.3450	0.25376	2.29e-01	-0.05442	0.594
F31	0.8647	0.53289	4.51e-01	-0.49541	1.035
F43	0.0202	0.09039	3.20e-01	-0.48174	0.570
F19	0.4386	0.38617	1.57e-01	0.03155	0.558
F26	0.3959	0.39814	1.27e-01	0.20395	0.584
F36	0.6030	0.59750	9.17e-02	0.47058	0.766
F42	1.0000	1.00000	1.28e-16	1.00000	1.000

loadings

	Original	Mean.Boot	Std.Error	perc.05	perc.95
F25	0.687	0.2176	4.69e-01	-0.6137	0.814
F29	-0.274	-0.1573	3.51e-01	-0.6694	0.467
F32	0.564	0.2926	3.90e-01	-0.4880	0.739
F33	-0.140	-0.0563	5.18e-01	-0.7587	0.772
F34	0.328	0.0799	5.43e-01	-0.7569	0.793
F46	0.118	0.1128	3.10e-01	-0.4168	0.546

```
F47     0.231     0.0732   3.85e-01  -0.5268    0.634
F21     0.737     0.7042   1.63e-01   0.4145    0.883
F22     0.759     0.7433   1.15e-01   0.5072    0.881
F24     0.820     0.7930   8.45e-02   0.5965    0.896
F28     0.784     0.7932   6.64e-02   0.6831    0.889
F17     0.278     0.2615   2.57e-01  -0.1875    0.626
F35     1.000     0.9762   3.69e-02   0.9076    1.000
F14     0.722     0.6560   2.20e-01   0.2961    0.878
F15    -0.200    -0.1596   3.71e-01  -0.6299    0.511
F23     0.644     0.5498   2.25e-01   0.1110    0.771
F27     0.631     0.5628   2.30e-01   0.0889    0.842
F16     0.469     0.1657   5.12e-01  -0.6457    0.838
F18    -0.188    -0.0236   3.98e-01  -0.6044    0.692
F20     0.300     0.2417   3.04e-01  -0.3074    0.706
F31     0.932     0.5417   3.53e-01  -0.2598    0.937
F43     0.329     0.2323   3.87e-01  -0.4591    0.779
F19     0.602     0.5516   2.26e-01   0.0722    0.814
F26     0.640     0.6290   1.73e-01   0.3860    0.850
F36     0.800     0.8075   7.50e-02   0.6548    0.896
F42     1.000     1.0000   7.73e-17   1.0000    1.000

paths
                    Original  Mean.Boot  Std.Error  perc.05  perc.95
INFOQUAL->SYSQUAL      0.562      0.703     0.1577    0.614   0.8108
PROZQUAL->SERVQUAL     0.505      0.516     0.0907    0.352   0.6424
PERSQUAL->SERVQUAL     0.327      0.340     0.1034    0.177   0.5187
ORGAQUAL->ISQUAL       0.520      0.471     0.1921    0.305   0.6823
SYSQUAL->ISQUAL        0.344      0.283     0.2108   -0.222   0.5700
SERVQUAL->ISQUAL      -0.341     -0.266     0.1425   -0.514  -0.0230

rsq
          Original  Mean.Boot  Std.Error  perc.05  perc.95
SYSQUAL      0.315      0.519     0.0947    0.381    0.657
SERVQUAL     0.535      0.577     0.0952    0.411    0.702
ISQUAL       0.371      0.406     0.1015    0.241    0.574

total.efs
                    Original  Mean.Boot  Std.Error  perc.05   perc.95
INFOQUAL->PROZQUAL     0.000     0.0000     0.0000    0.000   0.00000
INFOQUAL->PERSQUAL     0.000     0.0000     0.0000    0.000   0.00000
INFOQUAL->ORGAQUAL     0.000     0.0000     0.0000    0.000   0.00000
INFOQUAL->SYSQUAL      0.562     0.7033     0.1577    0.614   0.81076
INFOQUAL->SERVQUAL     0.000     0.0000     0.0000    0.000   0.00000
INFOQUAL->ISQUAL       0.193     0.1952     0.1531   -0.167   0.38916
PROZQUAL->PERSQUAL     0.000     0.0000     0.0000    0.000   0.00000
PROZQUAL->ORGAQUAL     0.000     0.0000     0.0000    0.000   0.00000
PROZQUAL->SYSQUAL      0.000     0.0000     0.0000    0.000   0.00000
PROZQUAL->SERVQUAL     0.505     0.5156     0.0907    0.352   0.64245
PROZQUAL->ISQUAL      -0.172    -0.1358     0.0769   -0.252  -0.01432
PERSQUAL->ORGAQUAL     0.000     0.0000     0.0000    0.000   0.00000
PERSQUAL->SYSQUAL      0.000     0.0000     0.0000    0.000   0.00000
PERSQUAL->SERVQUAL     0.327     0.3400     0.1034    0.177   0.51873
PERSQUAL->ISQUAL      -0.112    -0.0912     0.0590   -0.191  -0.00529
ORGAQUAL->SYSQUAL      0.000     0.0000     0.0000    0.000   0.00000
ORGAQUAL->SERVQUAL     0.000     0.0000     0.0000    0.000   0.00000
ORGAQUAL->ISQUAL       0.520     0.4711     0.1921    0.305   0.68231
SYSQUAL->SERVQUAL      0.000     0.0000     0.0000    0.000   0.00000
SYSQUAL->ISQUAL        0.344     0.2826     0.2108   -0.222   0.57000
```

```
SERVQUAL->ISQUAL      -0.341    -0.2664     0.1425   -0.514  -0.02302
```

Eingesetzte Software zur Erstellung dieser Arbeit

Diese Arbeit wurde mit LyX auf Basis von TeX Live in den Schriftarten Linux Libertine und Biolinum erstellt. Die Literaturverwaltung erfolgte mit Hilfe von Biblatex und JabRef. Die Graphiken wurden mit Inkscape und R erzeugt.

Literatur

Amberg, M., Wiener, M., „IT-Offshoring: Management internationaler IT-Outsourcing-Projekte“, Physica-Verl., Heidelberg 2006

Amberg, M., Mossanen, K., Kramolisch, W., Biermann, S., Lehr, L., „Compliance im IT-Outsourcing“, Techn. Ber., Lehrstuhl für Wirtschaftsinformatik III, Friedrich-Alexander-Universität Erlangen-Nürnberg und Accenture GmbH 2009, URL: http://www.accenture.com/SiteCollectionDocuments/Local_Germany/PDF/ComplianceimITOutsourcing.pdf

Annuscheit, R., „Erfüllung von Compliance-Aufgaben“, 27. 11. 2006, URL: http://www.compliance-magazin.de/compliancefachbeitraege/management/ca271106.html, 6, 17. 10. 2011

Armbrust, M. et al., „Above the Clouds: A Berkeley View of Cloud Computing“, Techn. Ber., EECS Department, University of California, Berkeley 2009, URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Bagozzi, R. P., Yi, Y., „Advanced topics in structural equation models“, in: Bagozzi, R. P. (Hrsg.): *Advanced methods of marketing research*, Blackwell Business, Cambridge, Mass 1994

Bagozzi, R. P., „Causal models in marketing“, Wiley, New York, NY 1980

Bailey, J. E., Pearson, S. W., „Development of a Tool for Measuring and Analyzing Computer User Satisfaction“, in: *Management Science* 29 (1983) 5, 530–545

Baumgartner, H., Homburg, C., „Applications of structural equation modeling in marketing and consumer research: a review“, in: *International Journal of Research in Marketing* 13 (1996) 2, 139–161

Baun, C., Kunze, M., Nimis, J., Tai, S., „Cloud Computing: Web-basierte dynamische IT-Services“, Günther, O., Karl, W., Lienhart, R., Zeppenfeld, K. (Hrsg.): Informatik im Fokus, Springer, Berlin et al. 2010

Bernd-Striebeck, U., „Trust — Herausforderungen für die IT-Versorgung heute und morgen“, in: Picot, A., Hertz, U., Götz, T. (Hrsg.): *Trust in IT: wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?*, Springer, Berlin 2011, 5–21

BITKOM, „Sicherheit für Systeme und Netze in Unternehmen“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2003, URL: http://www.bitkom.org/60376.aspx?url=ACF897.pdf, 64, 10. 05. 2011

– „Übermittlung personenenbezogener Daten“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2008, URL: http://www.bitkom.org/files/documents/20060418_Band__2_Auslandsgeschaeft_Uebermittlung_personenbezogener_Daten.pdf, 44, 17. 10. 2011

– „Cloud Computing - Evolution in der Technik, Revolution im Business - BITKOM-Leitfaden“, Bundesverband Informationswirtschaft, Telekommunikation und neue

Medien e. V., 10/2009, URL: http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf, 87, 01. 03. 2011

BITKOM, „Cloud Computing – Was Entscheider wissen müssen“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2010, URL: http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf, 116, 17. 10. 2011

– „Cloud Computing wächst zweistellig“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 28. 02. 2011, URL: http://www.bitkom.org/files/documents/BITKOM_PK_Cloud_Computing_CeBIT_28_02_2010(1).pdf, 3, 01. 03. 2011

Blattmann, O., Grüter, M., von Burg, S., Myrach, T., „e-Success — Ein Instrument zur Messung des Erfolgs von Web-Seiten — getestet bei Schweizer Winzern“, in: Schumann, M., Kolbe, L. M., Breitner, M. H., Frerichs, A. (Hrsg.): *Multikonferenz Wirtschaftsinformatik 2010*, Universitäts-Verlag, Göttingen 2010, 2163–2180

Bortz, J., Döring, N., „Forschungsmethoden und Evaluation: für Human- und Sozialwissenschaftler“, 4., überarb. Aufl., Nachdr., Springer-Medizin-Verl., Heidelberg 2009

Brotby, W. K., „Information security management metrics: a definitive guide to effective security monitoring and measurement“, Auerbach Publications/CRC Press, Boca Raton, Fla. et al. 2009

BSI, „BSI-Standard 100-1 — Managementsysteme für Informationssicherheit“, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2008a

– „BSI-Standard 100-2 — IT-Grundschutz-Vorgehensweise“, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2008b

– „IT-Grundschutz-Kataloge“, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2009

Budszus, J., Heibey, H.-W., Hillenbrand-Beck, R., Polenz, S., Seifert, M., Thiermann, M., „Orientierungshilfe – Cloud Computing“, Techn. Ber. Version 1.0, 2011: Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Buxmann, P., Lehmann, S., Hess, T., „Software as a Service“, in: *Wirtschaftsinformatik* 50 (2008) 6, 500–503

Böhmer, W., „Managementsysteme sind Balance-Systeme — Diskussion relevanter Kennzahlen eines ISMS gemäß ISO/IEC 27001:2005“, in: Schumann, M., Kolbe, L. M., Breitner, M. H., Frerichs, A. (Hrsg.): *Multikonferenz Wirtschaftsinformatik 2010*, Universitäts-Verlag, Göttingen 2010, 2163–2180

Cameron, K., „The Laws of Identity“, 05/2005, URL: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, 24. 10. 2010

Chin, W., „Issues and Opinion on Structural Equation Modeling“, in: *MIS Quarterly* 22 (1998) 1, vii–xvi

Chin, W. W., Newsted, P. R., „Structural equation modeling analysis with small samples using partial least squares“, in: Hoyle, R. H. (Hrsg.): *Statistical strategies for small sample research*, Thousand Oaks et al., Calif. 1999, S. 307 ff.

Chin, W. W., Dibbern, J., „An Introduction to a Permutation Based Procedure for Multi-Group PLS Analysis: Results of Tests of Differences on Simulated Data and a Cross Cultural Analysis of the Sourcing of Information System Services Between Germany and the USA“, in: Vinzi, V. E., Chin, W. W., Henseler, J., Wang, H. (Hrsg.): *Handbook of partial least squares: concepts, methods and applications*, Springer, Berlin et al. 2010, 171–193

Chongsuvivatwong, V., „Analysis of epidemiological data using R and Epicalc“, McNeil, E. (Hrsg.): Epidemiology Unit - Prince of Songkla University - Thailand, 2007

Chung, L., „Dealing with security requirements during the development of information systems“, in: Rolland, C., Bodart, F., Cauvet, C. (Hrsg.): *Advanced Information Systems Engineering*, Bd. 685, Springer Berlin / Heidelberg, 1993, 234–251

Chutimaskul, W., Funilkul, S., Chongsuphajaisiddhi, V., „The quality framework of e-government development“, in: *Proceedings of the 2nd international conference on Theory and practice of electronic governance*, ACM, Cairo, Egypt 2008, 105–109

CMMI-DEV, „CMMI for Development“, Software Engineering Institute, 2006

Cronbach, L. J., „Coefficient alpha and the internal structure of tests“, in: *Psychometrika* 16 (1951) 3, 297–334

DeLone, W. H., McLean, E. R., „Information systems success: The quest for the dependent variable.“, in: *Information Systems Research* 3 (1992) 1, 60–95

– „The DeLone and McLean Model of Information Systems Success: A Ten-Year Update“, in: *Journal of management information systems* 19 (2003) 4, 9–30

Deograt-Lumy, G., Naldo, R., „Insight into Intrusion Prevention Systems“, in: Tipton, H. F., Krause, M. (Hrsg.): *Information security management handbook*, CRC Press, Auerbach, Boca Raton, FL 2007, 993–1004

Deussen, P. H., Strick, L., Peters, J., „Cloud-Computing für die öffentliche Verwaltung“, Techn. Ber., Fraunhofer-Institut für Offene Kommunikationssysteme 2010, URL: `http://www.fokus.fraunhofer.de/de/elan/_docs/isprat_cloud_studie_20110106.pdf`

Deutsche Messe AG, „Top-Thema der CeBIT 2011 "Work and Life with the Cloud"“, 24. 02. 2011, URL: `http://www.cebit.de/de/ueber-die-messe/themen-und-trends/top-themen/cloud-computing`, 1, 28. 02. 2011

Dijkstra, T. K., „Latent Variables and Indices: Herman Wold's Basic Design and Partial Least Squares“, in: *Handbook of Partial Least Squares*, Springer, Heidelberg u. a. 2010, 23–46

Dillon, W. R., Goldstein, M., „Multivariate analysis : methods and applications“, Wiley, New York [u.a.] 1984

Dropbox, „How secure is Dropbox?“, 08. 08. 2011, URL: http://www.dropbox.com/help/27, 1, 03. 10. 2011

Duisberg, A., „Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing“, in: Picot, A., Hertz, U., Götz, T. (Hrsg.): *Trust in IT : wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?*, Springer, Berlin 2011, 49–70

Duller, C., „Einführung in die Statistik mit EXCEL und SPSS: ein anwendungsorientiertes Lehr- und Arbeitsbuch“, 2., überarb. Aufl., Physica-Verl., Heidelberg 2007

Eberl, M., „Formative und reflektive Indikatoren im Forschungsprozess: Entscheidungsregeln und die Dominanz des reflektiven Modells“, Schriften zur empirischen Forschung und quantitativen Unternehmensplanung; H. 19, Inst. für Organisation, Seminar für Empirische Forschung und Quantitative Unternehmensplanung, München 2004

Eberl, M., Schwaiger, M., „Die wahrgenommene Übernahme gesellschaftlicher Verantwortung als Determinante unternehmerischer Einstellungsziele: ein internationaler kausalanalytischer Modellvergleich“, Schriften zur empirischen Forschung und quantitativen Unternehmensplanung; H. 20, Inst. für Organisation, Seminar für Empirische Forschung und Quantitative Unternehmensplanung, München 2004

Eckert, C., „IT-Sicherheit: Konzepte – Verfahren – Protokolle“, 5., überarb. Aufl., Oldenbourg, München [u.a.] 2008

Eckstein, P. P., „Statistik für Wirtschaftswissenschaftler: eine realdatenbasierte Einführung mit SPSS“, 2., aktualisierte und erw. Aufl., Gabler, Wiesbaden 2010

Egle, U., „IT-Kostenmanagement: Studie zum Kostenmanagement und zur IT bei Schweizer Unternehmen“, Diss., GRIN-Verl., München et al. 2008

Eikenberg, R., „Tool soll SSL-Cookies in zehn Minuten knacken“, 20. 09. 2011, URL: http://www.heise.de/security/meldung/Tool-soll-SSL-Cookies-in-zehn-Minuten-knacken-1346257.html, 1, 02. 10. 2011

ENISA, „Cloud Computing – Benefits, risks and recommendations for information security“, Techn. Ber., European Network und Information Security Agency (ENISA), URL: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Ferguson, J. M., Zawacki, R. A., „Service Quality: A Critical Success Factor for IS Organizations“, in: *Information Strategy: The Executive's Journal* 9 (1993) 2, 24–30

Fitzgerald, T., „Information Security Governance“, in: Tipton, H. F., Krause, M. (Hrsg.): *Information security management handbook*, 6th ed, CRC Press, Auerbach, Boca Raton, Fla. et al. 2007

Foster, I., Zhao, Y., Raicu, I., Lu, S., „Cloud Computing and Grid Computing 360-Degree Compared“, in: *2008 Grid Computing Environments Workshop*, IEEE Service Center, Piscataway, NJ 2008, 60–69

Franch, X., Carvallo, J., „Using quality models in software package selection“, in: *Software, IEEE* 20 (2003) 1, 34 –41

Frentrup, M., Theuvsen, L., „Transparency in supply chains: is trust a limiting factor?“, in: *Trust and risk in business networks*, 2006, 65–74

FU Berlin, „Neuere Entwicklungen in der Partial Least Squares (PLS)-Pfadmodellierung“, Freie Universität Berlin, 21. 01. 2008, URL: http://www.wiwiss.fu-berlin.de/veranstaltungen/vhb-2008/workshops/Workshop_PLS.pdf, 2, 25. 06. 2011

Garson, G. D., „Path Analysis“, 03. 03. 2011, URL: http://faculty.chass.ncsu.edu/garson/PA765/path.htm, 12, 10. 10. 2011

Google, 23. 06. 2011, URL: http://code.google.com/intl/de-DE/appengine/docs/whatisgoogleappengine.html, 5, 2011

Grimpe, C., „Post Merger Integration der Forschung und Entwicklung“, Deutscher Universitäts-Verlag, Wiesbaden 2005

Gronau, N., Lindemann, M., „Einführung in das Informationsmanagement“, Gito, Berlin 2010

Groß, J., „Grundlegende Statistik mit R: eine anwendungsorientierte Einführung in die Verwendung der Statistik Software R“, 1. Aufl., Vieweg + Teubner, Wiesbaden 2010

Gruschka, N., Iacono, L., „Vulnerable Cloud: SOAP Message Security Validation Revisited“, in: Damiani, E. (Hrsg.): *2009 IEEE International Conference on Web Services*, IEEE, Piscataway, NJ 2009, 625 –631

Görtz, H., Stolp, J., „Informationssicherheit in Unternehmen: Sicherheitskonzepte und -lösungen in der Praxis“, 1. Aufl, Addison-Wesley-Longman, Bonn et al. 1999

Haenlein, M., Kaplan, A., „A beginner's guide to partial least squares analysis“, in: *Understanding statistics* 3 (2004) 4, 283–297

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., „Multivariate data analysis“, 7. ed, Pearson Prentice Hall, Upper Saddle River, NJ et al. 2010

Hansen, M., „Cloud Computing – Neue Herausforderungen für den (betrieblichen) Datenschutz?“, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 14. 05. 2009, URL: https://tepin.aiki.de/blog/uploads/20090514-hansen-hattingen-cloud-computing.pdf, 21, 02. 10. 2011

Hansmann, K.-W., Ringle, C. M., „Erfolgsfaktoren Virtueller Unternehmen“, in: Brüggemann, W., Jahnke, H. (Hrsg.): *Betriebswirtschaftslehre und betriebliche Praxis: Festschrift für Horst Seelbach zum 65. Geburtstag*, 1. Aufl, Dt. Univ.-Verl., Wiesbaden 2003

Haupt, J., „Wolkenbruch bei Amazon: Datenverlust in der Cloud“, 28. 04. 2011, URL: http://www.heise.de/newsticker/meldung/Wolkenbruch-bei-Amazon-Datenverlust-in-der-Cloud-1234444.html, 1, 03. 10. 2011

Heinrich, L. J., „Wirtschaftsinformatik: Einführung und Grundlegung“, Oldenbourg, München et al. 1993

Heinrich, L. J., Lehner, F., „Informationsmanagement: Planung, Überwachung und Steuerung der Informationsinfrastruktur“, 8., vollst. überarb. und erg. Aufl., Oldenbourg, München et al. 2005

Herrmann, W., „Experten warnen vor Sicherheitsrisiken in der Cloud“, 08. 02. 2010, URL: http://www.computerwoche.de/subnet/hp-intel/1929023/, 2, 06. 03. 2011

Hildebrandt, L., „Kausalanalytische Validierung in der Marketingforschung“, in: Hildebrandt, L., Homburg, C. (Hrsg.): *Die Kausalanalyse: ein Instrument der empirischen betriebswirtschaftlichen Forschung*, Schäffer-Poeschel, Stuttgart 1998

Ho, R., „Handbook of univariate and multivariate data analysis and interpretation with SPSS“, Chapman & Hall/CRC, Boca Raton, Fla. et al. 2006

Hofstede, G., „Transparency in Netchains“, in: Harnos, Z. (Hrsg.): *Information technology for a better agri-food sector, environment and rural living*, European Federation for Information Technology in Agriculture, Food und the Environment, Debrecen 2003, 17–29

Holthaus, M., „Management der Informationssicherheit in Unternehmen“, Diss., Universität Zürich 2000, URL: http://www.ifi.uzh.ch/archive/diss/Jahr_2000/thesis_holthaus.pdf

Homburg, C., Hildebrandt, L., „Die Kausalanalyse: Bestandsaufnahme, Entwicklungsrichtungen, Problemfelder“, in: Hildebrandt, L., Homburg, C. (Hrsg.): *Die Kausalanalyse : ein Instrument der empirischen betriebswirtschaftlichen Forschung*, Schäffer-Poeschel, Stuttgart 1998

Homburg, C., Pflesser, C., „Strukturgleichungsmodelle mit latenten Variablen: Kausalanalyse“, in: Herrmann, A., Homburg, C. (Hrsg.): *Marktforschung: Methoden, Anwendungen, Praxisbeispiele*, Wiesbaden 2000, 633–659

Hoppe, G., Prieß, A., „Sicherheit von Informationssystemen: Gefahren, Maßnahmen und Management im IT-Bereich“, Verl. Neue Wirtschafts-Briefe, Herne et al. 2003

Huber, F., Herrmann, A., Meyer, F., Vogel, J., Vollhardt, K., „Kausalmodellierung mit Partial Least Squares: eine anwendungsorientierte Einführung“, 1. Aufl., Gabler, Wiesbaden 2007

Husson, F., „Exploratory multivariate analysis by example using R“, CRC Press, Boca Raton et al. 2011

Ihlenfeld, J., „Fehlerhaftes Softwareupdate hat E-Mail-Löschung verursacht“, 01. 03. 2011, URL: http://www.golem.de/print.php?a=81781, 1, 03. 10. 2011

ISI, „ISI Citation Databases Help“, Institute for Scientific Information, 06. 10. 2000, URL: http://wos.isitrial.com/help/helpdefs.html, 9, 31. 05. 2011

ISO, „ISO/IEC 27000 - Informationtechnology – Security techniques – Information security management systems – Overview and vocabulary“, International Standardisation Organisation, 2009, URL: http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip

Jaquith, A., „Security metrics: replacing fear, uncertainty, and doubt“, Addison-Wesley, Upper Saddle River, NJ et al. 2007

Kampffmeyer, U., „Compliance: Rechtliche Anforderungen an die elektronische Dokumentation“, 2006, URL: http://www.project-consult.net/Files/Ingram_Compliance.pdf, 10, 02. 10. 2011

Kirsch, C., „IT-Unternehmen rufen nach Rechtssicherheit für Cloud-Daten“, 15. 07. 2011a, URL: http://www.heise.de/newsticker/meldung/IT-Unternehmen-rufen-nach-Rechtssicherheit-fuer-Cloud-Daten-1278767.html, 1, 13. 10. 2011

– „US-Behörden dürfen auf europäische Cloud-Daten zugreifen“, 30. 06. 2011b, URL: http://www.heise.de/newsticker/meldung/US-Behoerden-duerfen-auf-europaeische-Cloud-Daten-zugreifen-1270455.html, 02. 10. 2011

Klempt, P., Paar, C., Rüdiger, K., Wegener, C., Wolf, C., Düsenberg, P., Lindert, R., „IT-Sicherheit in NRW“, Techn. Ber., Horst-Görtz Institut für IT-Sicherheit 2007, URL: http://www.hgi.rub.de/media/hgi/files/weitere/itSicherheitsstudieNRW2007.pdf

Kolbe, L. M., „Management der Informationswirtschaft“, Vorlesung, 2008

Krcmar, H., „Informationsmanagement“, 4., überarb. und erw. Aufl., Springer, Berlin [u.a.] 2005

– „Informationsmanagement“, 5., Aufl., Springer, Berlin et al. 2010

Krutz, R. L., Vines, R. D., „Cloud security: a comprehensive guide to secure cloud computing“, Wiley, Indianapolis, Ind. 2010

Kuhlen, R., „Informationsmarkt: Chancen und Risiken der Kommerzialisierung von Wissen“, UVK, Univ.-Verl., Konstanz 1995

Kuri, J., „Siemens-Manager: Fundamente der IT-Sicherheit am Wanken“, 14. 09. 2011, URL: http://www.heise.de/security/meldung/Siemens-Manager-Fundamente-der-IT-Sicherheit-am-Wanken-1343442.html, 2, 02. 10. 2011

Langer, W., „Methoden V: Konfirmatorische Faktorenanalyse“, URL: http://www.soziologie.uni-halle.de/langer/lisrel/skripten/lisrelmodelle.pdf, 22. 09. 2011

Lederer, B., „Safe-Harbor-Abkommen in der Kritik“, 14. 04. 2011, URL: http://www.lto.de/de/html/nachrichten/2345/den-sicheren-hafen-gibt-es-nicht-safe-harbor-abkommen-in-der-kritik/, 2, 13. 10. 2011

Lippert, R., Kirsch, C., „Amazon rüstet Verschlüsselung für Cloud-Speicher nach“, 05. 10. 2011, URL: http://www.heise.de/ix/meldung/Amazon-ruestet-Verschluesselung-fuer-Cloud-Speicher-nach-1355308.html?view=print, 1, 15. 10. 2011

Long, J. O., „ITIL version 3 at a glance: information quick reference“, 1. ed., Springer, New York, NY 2008

Mason, R. O., „Measuring information output: a communication systems approach“, in: *Information and Management* 1 (1978) 4, 219–234

Mather, T., Kumaraswamy, S., Latif, S., „Cloud security and privacy: an enterprise perspective on risks and compliance“, 1. ed., O'Reilly, Sebastopol, Calif. et al. 2009

McIntosh, M., Austel, P., „XML signature element wrapping attacks and countermeasures“, in: *Proceedings of the 2005 workshop on Secure web services*, ACM, Fairfax, VA 2005, 20–27

McMillan, R., „Cisco CEO: Cloud Computing a 'Security Nightmare'“, 23. 04. 2009, URL: http://www.csoonline.com/article/490368/cisco-ceo-cloud-computing-a-security-nightmare-, 5, 24. 06. 2011

Misrahi, J., „Validating Your Business Partners“, in: Tipton, H. F., Krause, M. (Hrsg.): *Information security management handbook*, 6th ed, CRC Press, Auerbach, Boca Raton, Fla. et al. 2007

Mosler, K., Schmid, F., „Wahrscheinlichkeitsrechnung und schließende Statistik“, 2., verb. Aufl, Springer, Berlin et al. 2006

Mosler, K. C., Schmid, F., „Beschreibende Statistik und Wirtschaftsstatistik“, 2., verb. Aufl., Springer, Berlin [u.a.] 2005

Neumann, M., Sprenger, J., Gemlik, A., Breitner, M. H., „Untersuchung der praktischen Anwendbarkeit des IS-Erfolgsmodells von DeLone und McLean“, in: *Wirtschaftinformatik Proceedings 2011*, 2011, 486–496

NIST, „Special Publication 800-55 Revision 1 - Performance Measurement Guide for Information Security“, National Institute of Standards und Technology, 07/2008, URL: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Oppl, S., „Unterstützung expliziter Articulation Work“, Diss., Technische Universität Wien 2010, URL: http://www.comprehand.net/intern/dokumente/files/Diss.pdf

o.V., „Google hat gegen das Safe Harbor-Abkommen verstoßen, muss Datenschutz-Audits über sich ergehen lassen“, 31. 03. 2011, URL: http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-abkommen-verstossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html, 2, 13. 10. 2011

P-CMM, „People Capability Maturity Model“, Software Engineering Institute, 2001

Pakalski, I., „Serverausfall: Daten von Sidekick-Nutzern gelöscht“, 2009, URL: http://www.golem.de/print.php?a=70401, 2, 03. 10. 2011

Pandya, P., „Local Area Network Security“, in: Vacca, J. R. (Hrsg.): *Computer and information security handbook*, Elsevier/Morgan Kaufmann, Amsterdam et al. 2009, 149–167

Parasuraman, A., Zeithaml, V., Berry, L., „SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perception of Service Quality“, in: *Journal of Retailing* 64 (1988) 1, 12–40

Peltier, T. R., „Information Security Policies and Procedures – A Practitioner's Reference", Second Edition, Auerbach Publications, Boca Raton et al. 2004

Pichler, M., „Nachhaltige IT im Rechenzentrum: Entwicklung und Darstellung eines Modells zur Messbarkeit von Effizienz im Rechenzentrum", Diplomica Verl., Hamburg 2009

Pitt, L. F., Watson, R. T., Kavan, C. B., „Service Quality: A Measure of Information Systems Effectiveness", English, in: *MIS Quarterly* 19 (1995) 2, 173–187

Pohl, H., „Taxonomie und Modellbildung in der Informationssicherheit", in: *DuD – Datenschutz und Datensicherheit* 28 (2004) 11, 678–685

Ringle, C. M., „Gütemaße für den Partial Least Squares-Ansatz zur Bestimmung von Kausalmodellen", Techn. Ber., Universität Hamburg — Institut für Industriebetriebslehre und Organisation 2004, URL: http://www.ibl-unihh.de/ap16.pdf, 13. 10. 2011

– „Messung von Kausalmodellen: ein Methodenvergleich", Techn. Ber., Hamburg: Universität Hamburg — Institut für Industriebetriebslehre und Organisation 2004, URL: http://www.ibl-unihh.de/ap14.pdf

Ristenpart, T., Tromer, E., Shacham, H., Savage, S., „Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", in: *Proceedings of the 16th ACM conference on Computer and communications security*, ACM, Chicago, Illinois 2009, 199–212

Rodríguez, N., Casanovas, J., „A structural model of information system quality: an empirical research", in: *Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010)*, Lima, Peru 2010

Saaksjarvi, M., Saarinen, T., „Evaluation of service quality of information systems", in: *Proceedings of the Second International Software Metrics Symposium*, 1994, 84–94

Sachs, L., Hedderich, J., „Angewandte Statistik: Methodensammlung mit R", 12., vollst. neu bearb. Aufl., Springer, Berlin et al. 2006

Sanchez, G., „Understanding Partial Least Squares Path Modeling", Techn. Ber., Department of Statistics und Operations Research – Universitat Politécnica de Catalunya, URL: http://www.docstoc.com/docs/5049364/Understanding-PLSPM-with-R, 18. 09. 2011

– „Frequently Asked Questions about PLS Path Modeling", 25. 05. 2010, URL: http://www.docstoc.com/docs/40322021/FAQs-on-PLSPM, 6, 10. 10. 2011

Schulzki-Haddouti, C., Ziegler, P.-M., „Safe-Harbor-Abkommen: Freibrief für amerikanische Datenschutz-Sünder?", 17. 02. 2010, URL: http://www.heise.de/newsticker/meldung/Safe-Harbor-Abkommen-Freibrief-fuer-amerikanische-Datenschutz-Suender-933700.html?view=print, 2, 13. 10. 2011

Schwenk, J., „Technologien & Sicherheitsaspekte in Cloud Computing", in: Picot, A., Hertz, U., Götz, T. (Hrsg.): *Trust in IT : wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?*, Springer, Berlin 2011, 71–93

Schürmann, F., „Cloud Security“, in: Adelsberger, H. H., Drechsler, A. (Hrsg.): *Ausgewählte Aspekte des Cloud-Computing aus einer IT-Management-Perspektive*, Institut für Informatik und Wirtschaftsinformatik (ICB), Universität Duisburg-Essen, Essen 2010, 53–72

Seddon, P., Kiew, M., „A partial test and development of DeLone and McLean's model of IS success“, in: *Australian Journal of Information Systems* 4 (1996) 1, 90–109

Sedera, D., Gable, G., Chan, T., „A factor and structural equation analysis of the enterprise systems success measurement model“, in: *Proceedings of the Twenty-Fifth International Conference on Information Systems*, Association for Information Systems, Washington, DC 2004

Shannon, C. E., Weaver, W., „The mathematical theory of information“, University of Illinois Press, Urbana 1949

Sikora, A., „Security im Überblick (Teil 1) — Einführung in die Kryptographie — Safety und Security“, 07. 01. 2003, URL: http://www.tecchannel.de/sicherheit/management/402017/einfuehrung_in_die_kryptographie/index2.html, 3, 10. 05. 2011

Simonite, T., „Sicheres Computing für die Cloud“, 06/2010, URL: http://www.heise.de/tr/artikel/Sicheres-Computing-fuer-die-Cloud-1021071.html, 3, 03. 10. 2011

Singel, R., „Dropbox Left User Accounts Unlocked for 4 Hours Sunday“, 20. 06. 2011a, URL: http://www.wired.com/threatlevel/2011/06/dropbox/, 15, 03. 10. 2011

– „Dropbox Lied to Users About Data Security, Complaint to FTC Alleges“, 13. 05. 2011b, URL: http://www.wired.com/threatlevel/2011/05/dropbox-ftc/, 19, 03. 10. 2011

Staats, S., „Metriken zur Messung von Effizienz und Effektivität von Konfigurationsmanagement- und Qualitätsmanagementverfahren“, 1. Aufl., Europ. Hochsch.-Verl., Bremen 2009

Stanoevska-Slabeva, K., Wozniak, T., „Cloud Basics - An Introduction to Cloud Computing“, in: Stanoevska-Slabeva, K., Wozniak, T., Ristol, S. (Hrsg.): *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, Springer, Heidelberg et al. 2010

Stölzel, T., „Google-Server in Europa vor US-Regierung nicht sicher“, 2011, URL: http://www.wiwo.de/politik-weltwirtschaft/google-server-in-europa-vor-us-regierung-nicht-sicher-476338/, 1, 02. 10. 2011

Temme, D., Kreis, H., Hildebrandt, L., „PLS path modeling: a software review“, Institute of Marketing, Humboldt University Berlin, 2006

Toval, A., Nicolás, J., Moros, B., García, F., „Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach“, in: *Requirements Engineering* 6 (2002) (4), 205–219

Urbach, N., Smolnik, S., Riempp, G., „A Conceptual Model for Measuring the Effectiveness of Employee Portals“, in: *15th Americas Conference on Information Systems 2009*, Red Hook, NY 2009, Paper 589

Vinzi, V. E., „Model assessment in PLS path modelling“, 08. 09. 2009, URL: http://www.pls09.org/PPT/Model%20Assessment%20in%20PLS%20Path%20Modeling.pdf, 33, 19. 09. 2011

Vinzi, V. E., Trinchera, L., Amato, S., „PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement“, in: Vinzi, V. E., Chin, W. W., Henseler, J., Wang, H. (Hrsg.): *Handbook of Partial Least Squares*, Springer, Heidelberg et al. 2010, 47–82

Waidner, M., „Security and Cloud Computing“, IBM Corporation, 17. 04. 2010, URL: http://www.sit.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_SIT/Presentations/100302a%20Cloud%20Security%20Lecture.pdf, 62, 03. 10. 2011

Wang, M.-H., „Security in Cloud Computing“, 13. 09. 2010, URL: http://www.cse.scu.edu/~mwang2/cloud/Security.pdf, 4, 03. 10. 2011

Werts, C. E., Linn, R. L., Jöreskog, K. G., „Intraclass reliability estimates: Testing structural assumptions“, in: *Educational and Psychological Measurement* 34 (1974) 1, 25–33

West, M., „Preventing System Intrusions“, in: Vacca, J. R. (Hrsg.): *Computer and information security handbook*, Elsevier/Morgan Kaufmann, Amsterdam et al. 2009, 39–51

Williamson, G., Yip, D., Sharoni, I., Spaulding, K., „Identity Management: A Primer“, Mc Press, Lewisville, TX 2009

Windley, P., „Digital Identity“, O'Reilly Media, Inc., Sebastopol, CA 2005

Winkler, T. J., Ernst, P., „Innovationen im Mobile Government Eine Analyse von Dienstattraktivitäten und Motivationen von deutschen Kommunen“, in: Bernstein, A., Schwabe, G. (Hrsg.): *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, Bd. 2, Zürich 2011

XING AG, „XING ist das soziale Netzwerk für berufliche Kontakte“, 2011, URL: http://corporate.xing.com/no_cache/deutsch/unternehmen/xing-ag/, 2, 21. 09. 2011

Zahedi, F., „Reliability of Information Systems Based on the Critical Success Factors - Formulation“, in: *MIS Quarterly* 11 (1987) 2, 187–203

Zapf, S., „Informationssicherheit als Qualitätsmerkmal eines IT-Services nach ITIL“, 2007, URL: http://www.iwi.uni-hannover.de/cms/files/lv/sosem07/seminar/Zapf/Zapf_Seminararbeit_Thema15.pdf

Zinnbauer, M., Eberl, M., „Die Überprüfung von Spezifikation und Güte von Strukturgleichungsmodellen: Verfahren und Anwendung“, Inst. für Organisation, Seminar für Empirische Forschung und Quantitative Unternehmensplanung, München 2004

Versicherung

Ich versichere, dass ich die Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen oder anderen Quellen entnommen sind, sind als solche kenntlich gemacht.