

# Sicherheit vs. Privatheit

Vertrauensfaktoren im Umgang mit Daten  
und Konsequenzen für die digitale Identität

**Abschlussbericht**

## PROJEKTTEAM



Prof. Dr. Miriam Meckel  
MCM - Institute for Media and  
Communications Management  
University of St.Gallen  
Blumenbergplatz 9  
CH-9000 St.Gallen  
Tel.: +41 (0)71 224 27 90  
Fax: +41 (0)71 224 34 54  
[www.mcm.unisg.ch](http://www.mcm.unisg.ch)  
e-Mail: [miriam.meckel@unisg.ch](mailto:miriam.meckel@unisg.ch)



Prof. Dr. Christian P. Hoffmann  
MCM - Institute for Media and  
Communications Management  
University of St.Gallen  
Blumenbergplatz 9  
CH-9000 St.Gallen  
Tel.: +41 (0)71 224 30 24  
Fax: +41 (0)71 224 34 54  
[www.mcm.unisg.ch](http://www.mcm.unisg.ch)  
e-Mail: [christian.hoffmann@unisg.ch](mailto:christian.hoffmann@unisg.ch)



Andrea Chandra von Kaenel  
MCM - Institute for Media and  
Communications Management  
University of St.Gallen  
Blumenbergplatz 9  
CH-9000 St.Gallen  
Tel. +41 (0)71 224 34 74  
Fax +41 (0)71 224 27 71  
[www.mcm.unisg.ch](http://www.mcm.unisg.ch)  
e-Mail: [andrea.vonkaenel@unisg.ch](mailto:andrea.vonkaenel@unisg.ch)

## MANAGEMENT SUMMARY

In den letzten Jahren ist unter Internetnutzern eine stärker werdende Diskrepanz in Bezug auf den Umgang mit persönlichen Daten zu beobachten. Einerseits werden in (vermeintlich) privaten Foren und sozialen Netzwerken freiwillig in fast schon exhibitionistischer Weise persönliche Daten mitgeteilt. Vor allem junge Nutzer stellen enorme Mengen persönlicher Informationen ins Netz, die bislang in die Privatsphäre gehörten. Auf der anderen Seite ist eine grosse Unsicherheit hinsichtlich der Datensicherheit sowie Bedenken bezüglich der Aggregation privater Daten im Internet feststellbar. Die Medien thematisieren regelmässig den Datenschutz und das Recht auf Privatheit im Kontext der Online-Kommunikation.

Warum aber sind Internet-Nutzer bereit, bestimmten Netz-Angeboten ihre persönlichen Daten preiszugeben, anderen hingegen nicht? Welche Implikationen ergeben sich daraus für ein zeitgemässes elektronisches Identitätsmanagement? Fest steht: Im Internet erweist sich das Vertrauen der Nutzer als kritischer Erfolgsfaktor - ein vertrauensvoller Umgang mit persönlichen Daten kann als Basis für ökonomische Wertschöpfung im Internet betrachtet werden. Vor diesem Hintergrund hat das *mcm*institute - von ISPRAT gefördert - eine mehrstufige Erhebung unter deutschen Internetnutzern und Anbietern von Online-Applikationen durchgeführt, mit dem Ziel, jene Faktoren zu analysieren, die die Bereitschaft der Internetnutzer fördern, eine Applikation zu nutzen und ihr persönliche Daten zu überlassen.

Basierend auf einer systematischen Analyse bisheriger Forschungsergebnisse und einer fundierten empirischen Erhebung konnten so insbesondere sieben Faktoren identifiziert werden, die das Vertrauen in Internet-Angebote erhöhen: Reziprozität, Marke & Design, Kundenservice, Nutzerkontrolle, Third Party Endorsements, Realweltbezug und technische Zuverlässigkeit. Auf den folgenden Seiten werden diese Faktoren ebenso ausführlich beschrieben, wie ihre Implikationen für die Einführung und Vermittlung moderner Angebote des elektronischen Identitätsmanagements.

# INHALTSVERZEICHNIS

<b><u>I. EINLEITUNG</u></b>	<b>1</b>
THEMENSTELLUNG	1
ZIELE DES FORSCHUNGSPROJEKTS	3
AUFBAU DER STUDIE	4
EINBETTUNG IN DAS ISPRAT FORSCHUNGSPORTFOLIO	6
<b><u>II. SICHERHEIT, PRIVATHEIT UND VERTRAUEN</u></b>	<b>7</b>
PERSÖNLICHE DATEN: DIE WÄHRUNG DES INTERNETZEITALTERS	7
SICHERHEIT UND PRIVATHEIT	12
VERTRAUEN IM NETZ	14
ZUSAMMENFASSUNG	16
<b><u>III. VORGEHEN UND FORSCHUNGSMETHODEN</u></b>	<b>18</b>
PHASE 1: QUALITATIVE ANBIETER-INTERVIEWS	18
PHASE 2: QUALITATIVE NUTZER-INTERVIEWS	22
PHASE 3: QUANTITATIVE NUTZER-BEFragung	25
ZUSAMMENFASSUNG	31
<b><u>IV. RESULTATE: TREIBER DES NUTZERVERTRAUENS</u></b>	<b>32</b>
EINFLUSSFAKTOREN IM ÜBERBLICK	32
REZIPROZITÄT: VERTRAUEN ALS NUTZENABWÄGUNG	33
MARKE & DESIGN: BIG IS BEAUTIFUL	36
KUNDENSERVICE: AUSWAHL HILFT	39
NUTZERKONTROLLE: ANGST VOR DRITTPARTEIEN	41
THIRD PARTY ENDORSEMENTS: FREUNDE UND GOOGLE	44
REALWELTBEZUG: AUCH BILDER WIRKEN	47
TECHNISCHE ZUVERLÄSSIGKEIT: EIN HYGIENEFAKTOR	48
ZUSAMMENFASSUNG	49
<b><u>V. IMPLIKATIONEN FÜR DAS IDENTITÄTSMANAGEMENT</u></b>	<b>52</b>
REZIPROZITÄT	52
MARKE & DESIGN	53
KUNDENSERVICE	54
NUTZERKONTROLLE	55
THIRD PARTY ENDORSEMENTS	56

REALWELTBEZUG	57
TECHNISCHE ZUVERLÄSSIGKEIT	58
FAZIT	59
<b><u>VI. VERÖFFENTLICHUNGEN</u></b>	<b>61</b>
<b><u>VII. LITERATUR- UND QUELLENVERZEICHNIS</u></b>	<b>62</b>
<b><u>ANHANG</u></b>	<b>72</b>
A: LEITFADEN ANBIETER-BEFragung	72
B: LEITFADEN NUTZER-BEFragung	73
C: FRAGEBOGEN DER ONLINE-UMFRAGE	74
DAS INSTITUT FÜR MEDIEN- UND KOMMUNIKATIONS MANAGEMENT (MCM), UNIVERSITÄT ST. GALLEN	81

# ABBILDUNGSVERZEICHNIS

Abbildung 1: Protest gegen die Vorratsdatenspeicherung, sowie Protestmarsch in Berlin.....	3
Abbildung 2: Projektverlauf "Sicherheit vs. Privatheit" .....	4
Abbildung 3: Zeitplan und Ergebnisse des Forschungsprojekts.....	5
Abbildung 4: n:n-Kommunikation.....	8
Abbildung 5: Selbstdarstellung im Netz.....	10
Abbildung 6: Abwägung von Vertrauen und Sorgen .....	12
Abbildung 7: Sicher im Netz?.....	13
Abbildung 8: Einflussfaktoren des Nutzervertrauens .....	16
Abbildung 9: Kodierung der transkribierten Interviews .....	21
Abbildung 10: Vertrauensfaktoren aus Sicht der Anbieter.....	22
Abbildung 11: Vertrauensfaktoren aus Sicht der Nutzer .....	25
Abbildung 12: Aufbau der Online-Befragung.....	26
Abbildung 13: Durch Umfrage identifizierte Vertrauensfaktoren .....	32
Abbildung 14: Zusatzinformationen sind erwünscht.....	35
Abbildung 15: Mögliche Third Party Endorsements .....	46
Abbildung 16: Das Team des Lehrstuhls MCM2 .....	81

# TABELLENVERZEICHNIS

Tabelle 1: Anbieterinterviews nach Geschäftsmodell .....	20
Tabelle 2: Demographische Daten der Nutzerinterviews.....	23
Tabelle 3: Anzahl Nutzer pro Geschäftsmodell.....	26
Tabelle 4: Zusammensetzung der Stichprobe der Online-Umfrage (n=1294) .....	27
Tabelle 5: KMO und Bartlett's Test .....	29
Tabelle 6: Explorative Faktorenanalyse .....	30
Tabelle 7: Korrelation Faktoren und Vertrauen.....	30
Tabelle 8: Faktorladungen Reziprozität .....	33
Tabelle 9: Faktorladungen Marke & Design.....	37
Tabelle 10: Faktorladungen Kundenservice.....	40
Tabelle 11: Faktorladungen Nutzerkontrolle.....	42
Tabelle 12: Faktorladungen Third Party Endorsement .....	45
Tabelle 13: Faktorladungen Realweltbezug.....	47
Tabelle 14: Faktorladungen Technische Zuverlässigkeit.....	49

# I. EINLEITUNG

## THEMENSTELLUNG

Das populäre Online-Netzwerk „SchülerVZ“ für Schüler ab 12 Jahren zählt heute über 5,5 Millionen Mitglieder. Die Plattform ermöglicht ihren Mitgliedern das Einrichten eines Profils, welches Fotos ebenso wie persönliche Angaben enthält. Auf Grundlage eines solchen Profils vernetzen sich die Mitglieder untereinander, bilden Gruppen und kommunizieren über persönliche Nachrichten oder öffentliche Mitteilungen. Im Mittelpunkt steht also die Kommunikation mit Freunden und Klassenkameraden. Ende 2009 erfuhr die Öffentlichkeit, dass eine Million Datensätze solcher persönlicher Profile kopiert und damit der Kontrolle des Betreibers entzogen worden waren. Zu den kopierten Daten zählten Angaben zu Schule, Namen, Geschlecht und Alter der Nutzer sowie Profilfotos. Die Betreiber des Netzwerks wurden daraufhin von einem Unbekannten kontaktiert, der 20'000 Euro für die Rückgabe der Datensätze forderte, verbunden mit der Drohung, diese andernfalls ins Ausland zu verkaufen. Kurze Zeit später wurde diese Auslösesumme auf 80'000 Euro erhöht. Nachdem sich das betroffene Unternehmen an die zuständigen Behörden wandte, wurde schon sehr bald ein polizeibekannter 20-jähriger Schüler aus Erlangen verhaftet. Die Staatsanwaltschaft warf ihm versuchte Erpressung vor. Der Fall nahm schliesslich eine tragische Wendung, als nur wenige Tage später der Verdächtige tot in seiner Zelle der Jugendstrafanstalt Plötzensee aufgefunden wurde – offenbar hatte er sich in der Verzweiflung seiner Situation das Leben genommen (Augsburger Allgemeine, 2009; Greif, 2009; Spiegel Online, 2010; Seidler, 2009).

Das Vertrauen der Bürger ist heute einer der bedeutendsten Erfolgsfaktoren internetbasierter Geschäftsmodelle. Die Bereitschaft eines Nutzers, einem Interaktionspartner persönliche Daten zur Verfügung zu stellen, ist eine notwendige Voraussetzung für unterschiedlichste soziale und ökonomische Transaktionen (Culnan & Armstrong, 1999; Milne & Boza, 1999; Hoffman, Novak & Peralta, 1999b; Eastlick, Lotz & Warrington, 2006). Jüngste Entwicklungen machen deutlich, dass das Vertrauen der Nutzer und ihr Umgang mit persönlichen Daten noch weiter an Bedeutung gewinnen: Soziale Medien, das so genannte Web 2.0, verstärkt die personalisierte Präsenz der Bürger in webbasierten Kommunikationsnetzwerken - sei es in Social Networks oder auf Plattformen wie Blogs, Twitter und Youtube. Verbunden mit der Online-Präsenz auf solchen Kommunikationsplattformen ist unvermeidlich eine zunehmende Bereitstellung persönlicher Daten und Informationen.

Gleichzeitig kommt es immer wieder zu Erschütterungen des Nutzervertrauens gegenüber bedeutenden Interaktionspartnern, etwa aufgrund von Verfehlungen einzelner Anbieter. In

den vergangenen Monaten wurde eine Reihe prominenter Unternehmen von Datenschutzskandalen heimgesucht, welche breite öffentliche und mediale Aufmerksamkeit fanden. Es kann daher nicht davon ausgegangen werden, dass Internetnutzer Online-Anbietern und ihren Plattformen stets bereitwillig Vertrauen entgegen bringen (McKnight, Choudhury & Kacmar, 2002; Jarvenpaa, Tractinsky & Vitale, 2000; Urban, Amyx & Lorenzon, 2009). Um Neukunden anzuziehen und Kundenbindungen zu vertiefen, ist es für Online-Anbieter daher immer wieder notwendig, das Vertrauen ihrer Nutzer zu gewinnen und bestärken - eine Beobachtung, die ebenso für Angebote der öffentlichen Hand, also eGovernment-Applikationen gilt (Hoffman, Novak & Peralta, 1999a; Sheehan & Hoy, 1999; Rust, Kannan & Peng, 2002; Corbitt, Thanasankit & Yi, 2003).

Internetnutzer zeigen regelmässig ein erstaunlich ambivalentes Verhältnis zu ihren persönlichen Daten: Einerseits werden in fast schon exhibitionistischer Weise sensible Daten in vermeintlich privaten Foren und sozialen Netzwerken publiziert und getauscht - von Angaben über Schulnoten, politische oder sexuelle Präferenzen, religiöse Überzeugungen, bis hin zu inkriminierenden Fotodokumentationen alkoholbasierter Freizeitgestaltung. Andererseits regt sich massiver Widerstand, wenn staatliche Ansätze des Identitätsmanagements den Eindruck erwecken, einen Zugriff auf persönliche Daten zu ermöglichen. Diese Verhaltensweisen, in Verbindung mit dem rasanten Wachstum vielfältiger Online-Geschäftsmodelle (Timmers, 1998) in den vergangenen Jahren, rückten Fragen in Bezug auf Sicherheit und Privatheit im Netz in den Mittelpunkt der gesellschaftlichen Debatte.

Schon seit einigen Jahren befassen sich öffentliche Stellen sehr intensiv mit der Herausforderung eines zeitgemässen Identitätsmanagements in Online-Medien. Zunehmend ist die öffentliche Hand in der Lage, konkrete Applikationen und Lösungen für einen sicheren Umgang mit persönlichen Daten im Netz anzubieten; zuletzt fanden etwa die De-Mail sowie der elektronische Personalausweis öffentliche Aufmerksamkeit. Immer wieder muss dabei allerdings festgestellt werden, dass öffentliche Angebote des Identitätsmanagements in der Öffentlichkeit auf Skepsis, Sorgen und Ablehnung treffen - bis hin zu Protesten. Die Kritik der Bürger und verschiedener Organisationen richtet sich insbesondere auf Aspekte des Datenschutzes und der Datensicherheit, wie die Debatte um die Vorratsdatenspeicherung gezeigt hat (Albrecht, 2007).

Bürgerinnen, Datenschützer, Verfassungsrechtlerinnen, Politiker und Vertreter verschiedener Berufsgruppen kritisierten diese Massnahme als bedenklichen Schritt in Richtung eines "Überwachungsstaats". Debattiert wurde, ob mehr Sicherheit für die Bürger auf Kosten der Grundrechte zu rechtfertigen sei (Albrecht, 2007). Interessensgemeinschaften organisierten Widerstand nicht nur in Form traditioneller Unterschriftensammlungen - insbesondere in den Sozialen Medien wurde der Protest interessierter Kreise organisiert. So entstanden Wikis ([www.wiki.vorratsdatenspeicherung.de](http://www.wiki.vorratsdatenspeicherung.de)), etliche Websites und Blogs mit entsprechenden Diskussionsbeiträgen und -foren. Facebook-Gruppen wie etwa "Stop Vorratsda-

tenspeicherung!" organisierten Aktionen ihrer Mitglieder von Demonstrationen bis Flashmobs (Fiala, 2011; Heise, 2011 - s. Abbildung 1).



*Abbildung 1: Links: Protest gegen die Vorratsdatenspeicherung (Vorratsdatenspeicherung, 2011) und Rechts: Protestmarsch in Berlin (Heise, 2011)*

Auch nach einem ablehnenden Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung hält die Frage des staatlichen Zugriffs auf persönliche Daten sowie eines hinreichenden Schutzes der Privatsphäre das politische System in Atem (Spiegel Online Thema, 2011). Sicherheit und Privatheit sowie ein zeitgemäßes Identitätsmanagement bleiben zentrale Herausforderungen einer zunehmend internetbasierten Wissensgesellschaft. Angesichts des häufig ambivalenten Verhaltens der Nutzer stellt sich dabei insbesondere auch die Frage nach dem Vertrauen, der Vertrauensbereitschaft der Bürger im Rahmen von Online-Transaktionen. Welche Angebote im Netz treffen auf Akzeptanz, welche auf Ablehnung, und warum? Diesen Fragen sollte die Studie des Instituts für Medien- und Kommunikationsmanagement an der Universität St. Gallen, "Sicherheit vs. Privatheit: Vertrauensfaktoren im Umgang mit Daten und Konsequenzen für die digitale Identität", nachgehen. Der vorliegende Bericht wird deren Ergebnisse beschreiben, welche insbesondere wesentliche Treiber des Nutzervertrauens im Netz und sinnvolle Kommunikationsmassnahmen im Rahmen des Vertrauensmanagement identifizieren.

## ZIELE DES FORSCHUNGSPROJEKTS

Im Vordergrund der Studie steht die Frage nach den Einflussfaktoren, welche eine Akzeptanz spezifischer Online-Angebote und -Applikationen fördern, indem sie Vertrauen unter Internetnutzern erzeugen. Die Kenntnis dieser "Vertrauensfaktoren" soll es ermöglichen, Empfehlungen für die Implementation und Kommunikation eines professionellen Identitätsmanagements abzuleiten. Wie das Beispiel des neuen Personalausweises verdeutlicht, bewegt sich das Identitätsmanagement dabei in einem Spannungsverhältnis von Sicherheit und Privatheit, da Applikationen zur Garantie einer dieser Zielgrößen regelmässig Sorgen in Hinblick auf die andere nach sich zieht. Bislang ist jedoch nur wenig darüber bekannt,

wie sich Bürger bzw. Nutzer mit den gewandelten Anforderungen im Umgang mit Daten und neuen Formen des digitalen Identitätsmanagements auseinandersetzen, wie und auf welcher Basis sie ihren Umgang mit sensiblen Daten reflektieren, und wie die kommunikativen Grundlagen für eine optimale Operationalisierung eines professionellen Identitätsmanagements aussehen könnten.

Durch die Identifikation der vertrauensfördernden Faktoren wird es möglich, praxisgerechte Massnahmen des Vertrauensmanagement für Anbieter von Online-Geschäftsmodellen abzuleiten. Gleichzeitig wird dabei das Verständnis vertieft, welche Rolle öffentliche Angebote des Identitätsmanagements spielen können und sollen, sowie welche Massnahmen der Kommunikation und Implementation dieser Angebote als vielversprechend betrachtet werden dürfen.

## AUFBAU DER STUDIE

Das Projekt "Sicherheit vs. Privatheit" untersuchte anhand umfassender Befragungen der relevanten Zielgruppen deren Wahrnehmungen und Abwägungen im Umgang mit sensiblen Daten bei der Nutzung digitaler Applikationen. Im Rahmen von vertiefenden qualitativen Interviews sollten insbesondere jene Faktoren identifiziert werden, welche vertrauensbildend auf die Nutzer wirken und der Besorgnis um einen möglichen Missbrauch sensibler Daten entgegenwirken. Dabei sollten auch solche Personen Berücksichtigung finden, welche digitalen Applikationen ablehnend gegenüber stehen.

Das Forschungsprojekt war in vier aufeinander aufbauende Phasen gegliedert, die sich über einen Gesamtzeitraum von zwei Jahren erstreckten.

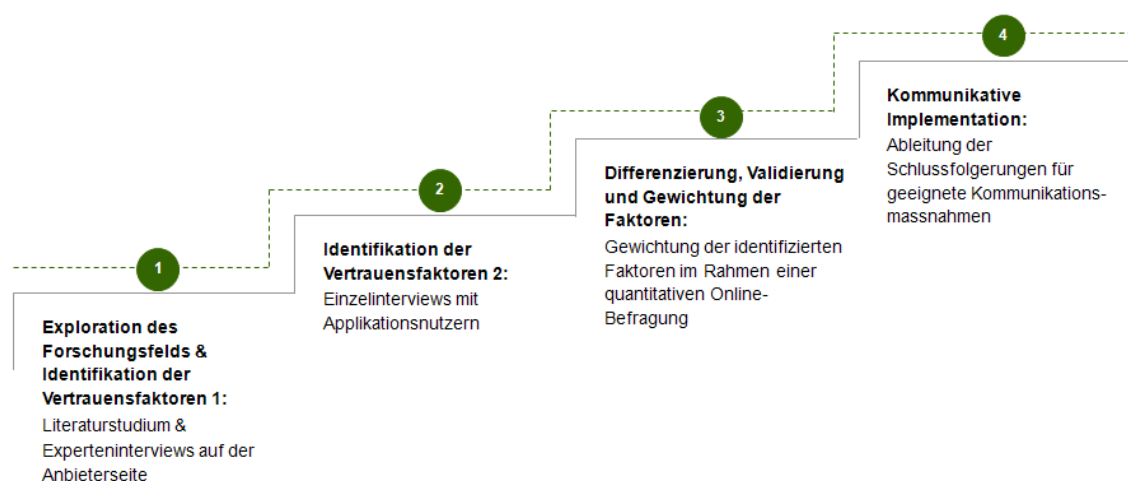
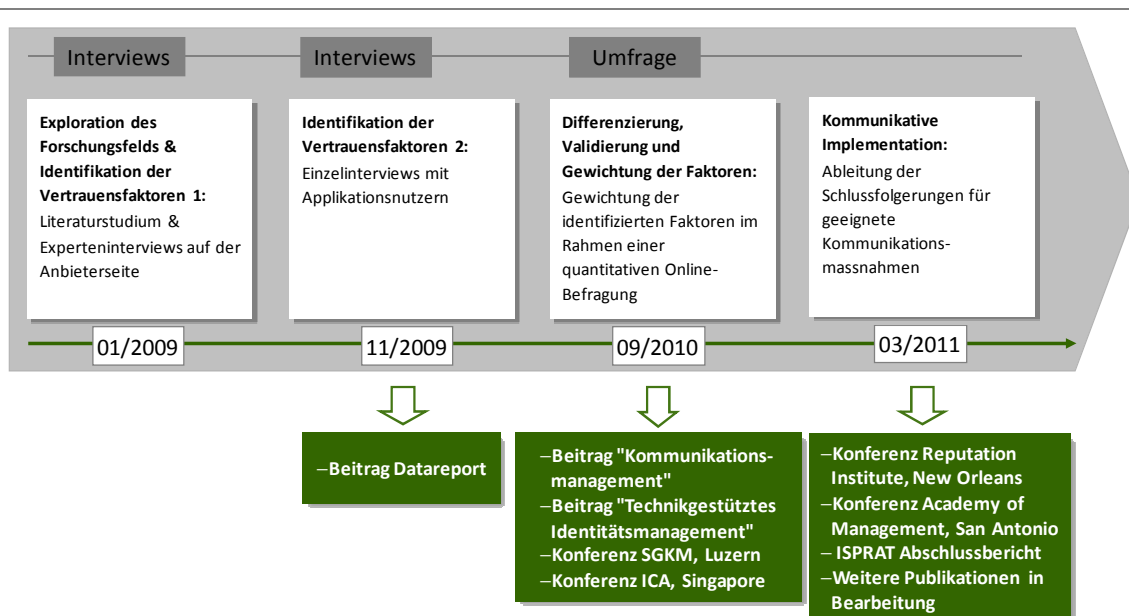


Abbildung 2: Projektverlauf "Sicherheit vs. Privatheit"

Die beschriebene Identifikation relevanter Vertrauensfaktoren im Zuge der **ersten Phase** des Projekts basierte neben einer intensiven Exploration des Forschungsfelds auch auf einer Untersuchung der Praxis-Perspektive: Im Rahmen von interdisziplinären Experteninterviews sollten vor allem die Anforderungen an und der Umgang mit Nutzerdaten auf Seiten der Applikationsanbieter erörtert werden. Darauf aufbauend wurde eine Systematik zur gezielten Befragung der Nutzergruppen hergeleitet.

In der **zweiten Phase** wurden Internetnutzer in qualitativen Einzelinterviews und Gruppendiskussionen nach ihrem Nutzungsverhalten, ihren Perspektiven und Abwägungen befragt, um so die zentralen Vertrauensfaktoren des Identitätsmanagements und der Online-Kommunikation zu identifizieren.

Die **dritte Phase** diente der Differenzierung, Validierung und Gewichtung der identifizierten Faktoren auf Basis einer quantitativen Online-Befragung. Begleitend umfasste die **vierte Projektphase** die Auswertung und Kommunikation der relevanten Erkenntnisse.



*Abbildung 3: Zeitplan und Ergebnisse des Forschungsprojekts*

Das Forschungsprojekt war insgesamt auf eine zweijährige Laufzeit ausgelegt. Die Ergebnisse jeder einzelnen Befragungsphase wurden aggregiert, als Teilergebnisse der Studie aufgearbeitet und im Rahmen der wissenschaftlichen Community sowie in Form gezielter Medienbeiträge auch öffentlich reflektiert. Details zu den Projektveröffentlichungen sind im Kapitel VI aufgeführt.

## **EINBETTUNG IN DAS ISPRAT FORSCHUNGSPORTFOLIO**

Das Projekt "Sicherheit vs. Privatheit" fügt sich ein in eine Reihe von Forschungsprojekten und Stellungnahmen seitens ISPRAT e.V. zu den aktuellen Herausforderungen des digitalen Identitätsmanagement, wie etwa das Whitepaper "Elektronisches Identitätsmanagement" oder die Forschungsprojekte "Bürgerfreundliches Identitätsmanagement" oder "Technikgestütztes Identitätsmanagement". Es deckt mit seinem breiten, explorativen Ansatz insbesondere den Aspekt der „Vertrauensbildung“ ab, und bietet Ansatzpunkte für die Analyse relevanter digitaler Geschäftsmodelle. Darüber hinaus hilft es, im Sinne der Ursachenforschung und sozialen Analyse, die Kommunikations- und Verhaltensmotive der Bürgerinnen und Bürger im Themenfeld „digitale Identität“ zu verstehen, und so ein wissenschaftlich fundiertes Verständnis in die Umsetzung und Kommunikation von Massnahmen im Rahmen des elektronischen Identitätsmanagement einzubringen.

## II. SICHERHEIT, PRIVATHEIT UND VERTRAUEN

*"Ihr habt heute keinerlei  
Privatsphäre mehr.  
Gewöhnt euch daran!"*

Scott McNealy

### PERSÖNLICHE DATEN: DIE WÄHRUNG DES INTERNET- ZEITALTERS

#### AUF DER BÜHNE DES WEB 2.0

Das neue Internet ist zu einem sozialen Katalysator von zunehmend spürbarer Bedeutung geworden, umschreibt der Begriff 'Web 2.0', obwohl er zunächst technische Assoziationen wecken mag, doch in erster Linie weitreichende gesellschaftliche und ökonomische Dynamiken, die durch das Internet in Bewegung gesetzt werden. Seit der Technologie-Guru Tim O'Reilly (2006) im Jahr 2004 die Bezeichnung für neu entstehende Formen der Zusammenarbeit und des Datenaustauschs prägte, hat sich Web 2.0 zu einem Oberbegriff für grundlegende Wandlungsprozesse in der digitalen Gesellschaft entwickelt. Massenkollaboration, kollektive Intelligenz, Wissensaustausch, grenzenlose Demokratie und die Eingliederung von Nischenangeboten und entlegener Regionen prägten immer schon die Grundzüge des WWW, allerdings auf Basis gut vernetzter Veröffentlichungsplattformen des Web 1.0. Das Web 2.0 ermöglicht nun darüber hinaus die selbstorganisierte Interaktion und Kommunikation der Nutzer durch Herstellung, Tausch und Weiterverarbeitung von Inhalten über Weblogs, Wikis und Social Networks. Neue soziale und wirtschaftliche Phänomene erwachsen aus dem schier unerschöpflichen Potential der Beteiligung des Einzelnen an digital vermittelten Prozessen sowie der gemeinsamen Nutzung und Herstellung von Inhalten.

Die Sozialen Medien werden häufig gepriesen für ihren Beitrag zu einer erleichterten, flächendeckenden Kommunikation und Vernetzung sowie für eine Erhöhung der gesellschaftlichen Transparenz. Die damit verbundenen sozialen Veränderungen, also Verände-

runge n im Verhalten und in der Interaktion der Bürger, stellen Wirtschaft, Politik und Gesellschaft vor erhebliche Herausforderungen (Ruisinger, 2007). Das soziale Netz bezieht seine Nutzer aktiv in lebendige Wertschöpfungsprozesse ein – sei es durch die erleichterte Produktion eigener Inhalte, Kommentare, Tags oder auch nur durch die virtuelle Präsenz in Austauschbeziehungen (Kilian, Hass & Walsh, 2007). Das Web 2.0 erlaubt es einem zuvor auf passiven Konsum beschränkten Publikum, zum Schöpfer vielfältiger multimedialer Inhalte zu werden – und stellt die Plattformen wie beispielsweise Blogs, Wikis und soziale Netzwerke für deren Verbreitung zur Verfügung. Bastionen der Meinungshoheit werden dadurch ebenso geschliffen, wie etablierte mediale Geschäftsmodelle (Bucher, Fieseler & von Kaenel, 2009). Je mehr soziale Interaktionen und ökonomische Transaktionen im Netz abgewickelt werden, desto mehr steigen jedoch auch die mit dem Datenaustausch verbundenen Herausforderungen und Risiken für die Nutzer.

Soziale Medien erfordern die Präsenz und Teilnahme ihrer Nutzer. Im Gegensatz zu den Massenmedien steht nicht mehr nur die Dissemination von Daten und Informationen im Vordergrund: die Teilnehmer der Sozialen Medien gestalten Beziehungsnetzwerke, die darin verbreiteten Informationen erfüllen nicht zuletzt auch den Zweck der Beziehungspflege. Lange Zeit war die gesellschaftliche Kommunikation geprägt von zwei Formen der Interaktion: Der 1:1- und der 1:n-Kommunikation (Göldi, 2008). Während die 1:1-Kommunikation auf der zwischenindividuellen Ebene stattfindet, steht im Rahmen der 1:n-Kommunikation ein Sender einer Vielzahl von Empfängern gegenüber. Frühe Websites folgten meist auch noch dem 1:n-Paradigma und waren in Hinblick auf ihre Kommunikationslogik damit *«alter Wein in neuen Schläuchen»*.

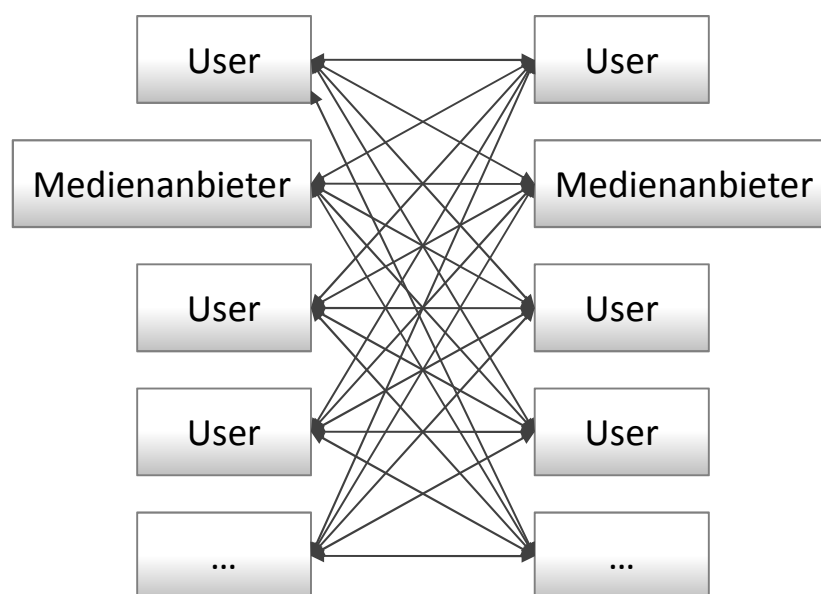


Abbildung 4: n:n-Kommunikation

Die heutigen Social Media Plattformen basieren im Kontrast dazu auf einem offenen und wechselseitigen Austausch von Informationen, Meinungen und Erfahrungen. Plattformen wie Weblogs, Wikis, «Youtube» oder «Facebook» stellen n:n-Medien dar – im Rahmen eines Netzwerks ist jeder Sender zugleich auch Empfänger (und umgekehrt). Wichtig ist dabei vor allem: Die Vielzahl der Sender verbindet sich mit einer Vielzahl von Empfängern, und dies öffentlich. Köhler (2008) nennt das die «Theatralität» der n:n-Kommunikation. «Im Unterschied zu klassischen Dialogmedien wie dem Telefon finden hier die Gespräche auf einer Art Bühne statt, die von anderen Personen beobachtbar ist. Im Social Web wird der dialogische Austausch sendefähig und kann ein quasi-massenmediales Publikum erreichen» (Köhler, 2008, Paragraph 4).

Das «Soziale» der Sozialen Medien hat somit eine doppelte Bedeutung, es steht zugleich für eine gesellschaftliche als auch für eine gemeinschaftliche Dimension. «Während sich Mitglieder einer Gesellschaft dieser aus rationalen Gründen und Zwecküberlegungen anschliessen, überwiegt bei der Gemeinschaft ein emotionales Moment. Beide können im Social Web gefunden werden» (Ebersbach, Glaser & Heigl, 2008, S. 30). Die Veröffentlichung von Blog- oder Twitter-Beiträgen oder auch nur Statusmeldungen in Sozialen Netzen dient einerseits zweifellos der Information der Interaktionspartner, aber zugleich stets auch der Vergewisserung der geknüpften Beziehungen sowie der eigenen Position innerhalb dieser Netzwerke. Soziale Medien haben darum mehr denn je die Veröffentlichung, das Mitteilen persönlicher Daten zur Folge.

### **SAMMEL- ODER VERÖFFENTLICHUNGSWUT?**

Schon seit Jahren ist das Ausmass der im Netz getauschten und gesammelten Datenmengen enorm (Vidmar & Flaherty, 1985). Zahlreiche Unternehmen pflegen umfangreiche Datenbanken, welche Informationen über das Verhalten ihrer Kunden und Nutzer aggregieren – automatisierte Analyseinstrumente wie Cookies, Click-stream Monitoring und weitere lassen diese Datenbanken beständig anwachsen (Rust et al., 2002; Olivero & Lunt, 2004). Niemals zuvor war es so einfach und billig, grosse Mengen vielfältiger Daten zu sammeln und auszuwerten (Hoffman et al., 1999b; Milne, 2000; Chellappa & Sin, 2005). Diese Entwicklung brachte Scott McNealy, den damaligen CEO von Sun Microsystems, dazu, auszurufen: „Ihr habt heute keinerlei Privatsphäre mehr. Gewöhnt euch daran!“ (Lester, 2001). Immer mehr Dienstleister spezialisieren sich darauf, Nutzerprofile zu erstellen - meist mit der Absicht, die enormen Werbeanstrengungen der Unternehmen in effizientere, zielgenauere Bahnen zu lenken.

Die auch öffentlich regelmässig problematisierte Sammelwut im Internet aktiver Unternehmen steht jedoch eine komplementäre Veröffentlichungswut der Nutzer gegenüber. Hunderte Millionen Menschen veröffentlichen heute in Sozialen Medien regelmässig Details über ihre persönliche Lebensgestaltung - von beruflichen Erlebnissen über Freizeitaktivitäten, politische und religiöse Überzeugungen bis hin zu sexuellen Präferenzen (Stutz-

mann, 2006). Auf der Social Network Site Facebook werden täglich über 60 Mio. Statusmeldungen publiziert, und 3 Milliarden Fotos veröffentlicht (Facebook, 2010). Laut einer BITKOM-Studie (zit. in Eck, 2008, S. 4) geben 49% der nach 1980 Geborenen ("Digital Natives") persönliche Informationen im Web über sich Preis. Die Migration beruflicher und privater Interaktionen ins Netz ist verbunden mit der Notwendigkeit einer gezielten Selbstdarstellung in den gewählten Medien (Jung, Youn & McClung, 2007). Wenn die Sozialen Medien eine Art Bühne darstellen, so wird diese, vor allem durch junge Erwachsene, mit grossem Engagement bespielt (Rifkin, 2010). Kritisch wird hier bereits von einem "Selbstdarstellungskult" gesprochen (Gmür, 2002).



*Abbildung 5: Selbstdarstellung im Netz*

Tatsächlich kann festgestellt werden, dass die durchaus vorhandene Möglichkeit, die Privatsphäre durch eine Limitierung der Zugriffsmöglichkeiten auf persönliche Daten in Sozialen Medien zu schützen, nur selten in Anspruch genommen wird (Peluchette & Karl, 2010; Palfrey & Gasser, 2008, Solove, 2007; Gallant, Boone & Heap, 2007). Ein allzu konsequenter Schutz der Privatsphäre widerspricht schlicht der Absicht einer Selbstdarstellung in ausgesuchten Netzwerken (boyd & Ellison, 2007; Preibusch, Hoser, Gürses & Berendt, 2007). Laut einer OECD Studie sind 41% der Facebook-Nutzer bereit, einem völlig Fremden, sogar frei erfundenen Personen, persönliche Informationen mitzuteilen (OECD, 2007; vgl. Blech et al., 2009). Dabei ist zweifellos auch zu beachten, dass sich der Schutz der Privatsphäre durch eine gezielte Kontrolle unterschiedlichster Filter- und Abschirmungsoptionen durchaus zeitaufwändig und intellektuell anspruchsvoll gestalten kann (Blech et al., 2009; Lischka, 2010; Neubauer, 2010).

Ob nun aber durch einen Anbieter gesammelt oder durch einen Nutzer publiziert, die Bereitschaft der Nutzer, einem Interaktionspartner persönliche Daten zur Verfügung zu stellen, ist eine notwendige Grundlage für jede Art von Online-Transaktion (Culnan & Armstrong, 1999; Milne & Boza, 1999; Eastlick et al., 2006). Diese Feststellung ist von kaum zu überschätzender Bedeutung: Ohne die Bereitschaft zur Mitteilung oder Bekanntgabe per-

sönlicher Daten kommen Online-Transaktionen nicht zustande, entsteht also kein "eBusiness". Nutzer verbringen heute immer mehr Zeit, immer grössere Teile ihres Lebens im Netz – Arbeit, Kommunikation und Freizeit basieren zunehmend auf einer Vielzahl von Online-Applikationen. Durch mobile Endgeräte wird das Internet tatsächlich allgegenwärtig. Eine immer grösser werdende Zahl von Unternehmen stellt Applikationen zur Verfügung, damit Nutzer sich untereinander verbinden und Kooperationen eingehen können (Afuah & Tucci, 2001; Mahadevan, 2000; O'Donnell, 2002; Rust et al., 2002). Jones, Wilikens, Morris und Masera (2000, S. 81) definieren eBusiness als "the carrying out of business activities that lead to an exchange of value, where the parties interact electronically, using network or telecommunications technologies". Folglich umfasst eBusiness nicht nur den Austausch von Gütern und Dienstleistungen, sondern auch den Austausch von Informationen. Persönliche Daten können daher als so etwas wie die Währung des eBusiness verstanden werden. Ähnlich wie Geld, Waren oder Dienstleistungen sind sie ein Tauschgut, das sich vorab im Verfügungsbereich eines Tauschpartners befindet und im Rahmen der Transaktion gegen einen subjektiven Nutzen eingetauscht wird.

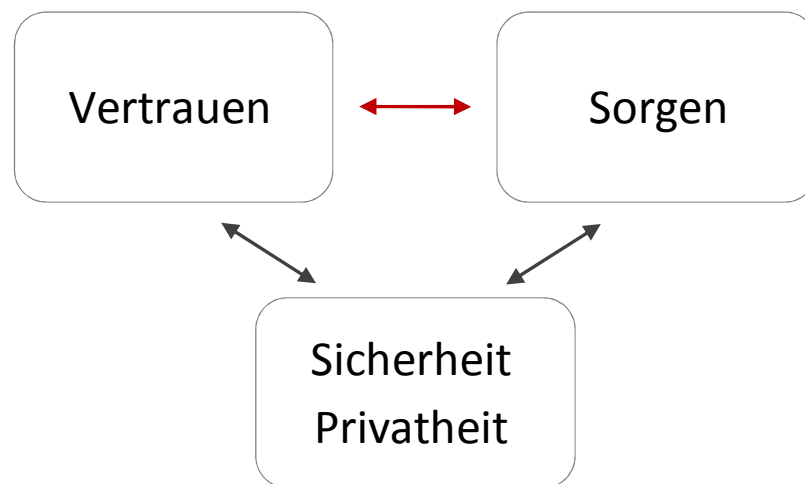
Es besteht eine grosse Vielzahl Internet-basierter Geschäftsmodelle, welche durch die Verbindung von Anbietern und Nachfragern im weitesten Sinne einen Mehrwert für die Nutzer generieren (Afuah & Tucci, 2001; Timmers, 1998; Mahadevan, 2000; O'Donnell, 2002). Zahlreiche dieser Geschäftsmodelle greifen ineinander, etwa wenn Informationsdienste die Grundlage für den Austausch in Sozialen Netzen sind, oder Finanzdienstleistungen eCommerce-Angebote ermöglichen. Auch die Angebote der öffentlichen Hand, also eGovernment-Applikationen, können sowohl im direkten Austausch mit den Nutzern stehen, oder den Austausch der Nutzer mit privatwirtschaftlichen Akteuren unterstützen. Das Gesamtvolumen der online generierten Wertschöpfung zu schätzen, unterliegt gewissen methodischen Schwierigkeiten. Feststellen lässt sich jedoch, dass allein der deutsche eCommerce-Umsatz bis 2010 auf über 20 Mrd. Euro geklettert ist, das Werbevolumen im Netz soll schon bald jenes der Rundfunkmedien überschreiten (Statista, 2011).

Die Bereitschaft der Nutzer, Transaktionen durch die Bereitstellung einer notwendigen Datenbasis zu ermöglichen, ist jedoch alles andere als eine Selbstverständlichkeit. Mangelndes Vertrauen wurde daher immer wieder als wesentliches Hindernis für das weitere Wachstum des eBusiness genannt (Hoffman et al., 1999a; McKnight et al., 2002; Urban et al., 2009). Mit der Ausbreitung des Web 2.0 und der damit verbundenen Kommunikations- und Kooperationsformen steigt entsprechend das Bedürfnis nach einem wirksamen Schutz der Sicherheit und Privatheit der Nutzer, also nach einem ebenso effizienten wie effektiven Identitätsmanagement. Ohne die freiwillige Beteiligung der Bürger kann das Netz nicht sein volles Wertschöpfungspotential für Wirtschaft, Kultur und Gesellschaft entfalten. Private wie öffentliche Anbieter von Online-Diensten sehen sich mit der Herausforderung konfrontiert, das Vertrauen ihrer (potentiellen) Nutzer zu gewinnen und pflegen.

## SICHERHEIT UND PRIVATHEIT

Die Einstellung der Nutzer gegenüber Online-Angeboten wird durch eine Vielzahl von Einflussfaktoren determiniert. Wesentliche Elemente dieser Einstellung sind die Sorgen oder Risikowahrnehmungen der Nutzer. Es wird angenommen, dass die Wahrscheinlichkeit der Beteiligung an einer Online-Transaktion abnimmt, je höher die Besorgnis oder die Risikowahrnehmung der Nutzer ausfällt (Sheehan & Hoy, 1999; Phelps, Nowak & Ferrell, 2000; Phelps, D'Souza & Nowak, 2001; Olivero & Lunt, 2004). Umgekehrt gilt: je mehr Vertrauen ein Nutzer aufbringt, desto weniger Sorgen oder Risikowahrnehmung wird gegenüber dem Vertrauensobjekt empfunden - und desto grösser ist die Wahrscheinlichkeit, dass es zu einer Teilnahme an einer Transaktion kommt (Morgan & Hunt, 1994; Culnan & Armstrong, 1999; Milne & Boza, 1999; Hoffman et al., 1999a; Jarvenpaa et al., 2000; Eastlick et al., 2006).

Zwei wesentliche Treiber sowohl des Vertrauens als auch der Risikowahrnehmung im Netz wurden identifiziert: Sicherheit und Privatheit. Urban et al. (2009) stellen fest: "Privacy and security have become the new baseline from which one evaluates an online merchant's trustworthiness."



**Abbildung 6:** Abwägung von Vertrauen und Sorgen

Der Wunsch nach Privatheit wird dabei in der Literatur mit seinem gegensätzlichen Bedürfnis nach Beteiligung kontrastiert (Lanier & Saini, 2008). Als soziale Wesen wünschen sich Menschen im Allgemeinen den Austausch mit Anderen. Gleichzeitig empfinden sie ein Bedürfnis nach Abgeschiedenheit, Autonomie und Selbstkontrolle. Im heutigen technologischen Umfeld impliziert der Wunsch nach Privatheit vor allem die Notwendigkeit, den Fluss und die Verbreitung persönlicher Daten zu kontrollieren, und ihre öffentliche Verfügbarkeit zu begrenzen. Nachdem Online-Transaktionen üblicherweise die Bekanntgabe mehr oder weniger umfangreicher persönlicher Daten erfordert, führen sie regelmässig zu

Bedenken bezüglich des Schutzes der Privatsphäre. Online-Transaktionen sind also mit einer Risikowahrnehmung hinsichtlich der Privatheit verbunden: "In fact, it may be quite impossible for customers to transact business on the Internet without revealing information about themselves that they may be unwilling to share" (Rust et al., 2002, p. 455). Vertrauen reduziert die Risikowahrnehmung in Hinblick auf Gefährdungen der Privatsphäre und erleichtert so Online-Transaktionen (Milne & Boza, 1999; Culnan & Armstrong, 1999; Olivero & Lunt, 2004; Chellappa & Sin, 2005).

Eine weiterer wesentlicher Treiber der Risikowahrnehmung im Netz sind Sorgen hinsichtlich einer unzureichenden Sicherheit (Hoffman et al., 1999b; Jarvenpaa et al., 2000; Jones et al., 2000; Belanger et al., 2002). Dabei bezieht sich das Element der Sicherheit üblicherweise auf die technische Integrität der IT Systeme der Transaktionspartner (Friedman et al., 2000; Nissenbaum, 2001; Urban et al., 2009). Diese Systeme können anfällig für technische Fehler, aber auch absichtliche Eingriffe oder Manipulationen sein. Verletzungen der Sicherheit erhöhen die Gefahr von Betrugs- oder Diebstahlsdelikten im Netz. Aus diesem Grund wird Sicherheitsbedenken in der Regel durch Massnahmen auf der technischen und Verwaltungsebene eines Online-Anbieters begegnet: angemessene Infrastrukturen, Software und Prozesse sollen die Webpräsenz eines Anbieters vor Fehlern oder Angriffen schützen (Nissenbaum, 2001; Belanger et al., 2002). Genau wie im Falle der Sorge um den Schutz der Privatheit reduziert auch die Risikowahrnehmung in Hinblick auf eine unzureichende Sicherheit die Wahrscheinlichkeit des Zustandekommens einer Online-Transaktion - während Vertrauen umgekehrt Sorgen hinsichtlich der Sicherheitsrisiken reduziert und damit Online-Transaktionen erleichtert (Urban et al., 2009).



---

*Abbildung 7: Sicher im Netz?*

---

Zusammenfassend entpuppt sich das Vertrauen der Nutzer als zentraler Erfolgsfaktor vielfältiger Online-Transaktionen. Es steht in einem Wechselverhältnis zur wahrgenommenen Sorge um eine ausreichende Gewährleistung von Sicherheit und Privatheit. Die Erzeugung und Erhaltung von Vertrauen ist damit die notwendige Grundlage für die Realisierung der wirtschaftlichen, kulturellen und sozialen Wertschöpfungspotentiale im Netz - gerade im Zeitalter Sozialer Medien.

## VERTRAUEN IM NETZ

Eine Vielzahl wissenschaftlicher Disziplinen, wie die Psychologie, Soziologie und Wirtschaftswissenschaften, befassen sich mit den Voraussetzungen und Wirkungen menschlichen Vertrauens. Es kann daher nicht überraschen, dass keine generell akzeptierte Definition dieses vielschichtigen Konzepts existiert. Einige Gemeinsamkeiten der verschiedenen Forschungsstränge lassen sich jedoch identifizieren: Regelmässig wird Vertrauen als ein subjektives Konstrukt beschrieben, eine Überzeugung, ein Glaube, ein Gefühl, und damit eine Eigenschaft, welche sowohl kognitive als auch affektive Elemente beinhaltet (Morgan & Hunt, 1994; Belanger et al., 2002; Lee & Turban, 2001). Eine verbreitete Definition beschreibt Vertrauen als "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau, Sitkin, Burt & Camerer, 1998, S. 395). Bart, Shankar, Sultan und Urban (2005) wenden diese Definition auf einen Online-Kontext an und unterstreichen dabei: "Online trust includes consumer perceptions of how the site would deliver on expectations, how believable the site's information is, and how much confidence the site commands."

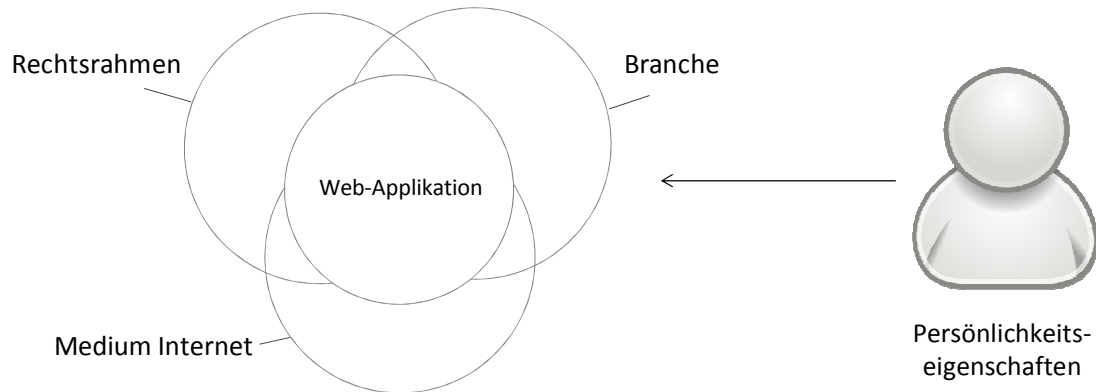
Die Bedeutung des Vertrauens wächst immer dann, wenn soziale Situationen durch Risiko, Unsicherheit und gegenseitige Abhängigkeit gekennzeichnet sind (McKnight & Chervany, 2002). Morgan und Hunt (1994) betonen, dass Vertrauen, verstanden als die Bereitschaft, eine Verwundbarkeit zu riskieren, Transaktionen erleichtert und stabile Geschäftsbeziehungen ermöglicht. Konsumenten müssen hinsichtlich der Integrität, der Kompetenz sowie auch des Wohlwollens der Geschäftspartner ein gewisses Vertrauensniveau erreichen, um sich an einer Transaktion zu beteiligen (Gefen, 2000; Bhattacharjee, 2002). Diese generellen Beobachtungen können auch auf Online-Transaktionen übertragen werden.

Das Online-Vertrauen unterscheidet sich von weiteren Verständnissen dieses Konstrukts somit vor allem darin, dass das Vertrauensobjekt eine Website darstellt - im Gegensatz zu Individuen, Gruppen, physischen Produkten oder Objekten, etc. (Nissenbaum, 2001). In einer Online-Umwelt sind alle Interaktionen computergestützt oder -mediert. Dies schränkt die Qualität und Quantität jener Hinweise ein, welche dem Konsumenten zur Beurteilung der Vertrauenswürdigkeit des Transaktionspartners zur Verfügung stehen (Friedman et al., 2000; Jarvenpaa et al., 2000; Yoon, 2002; Wang, Beatty & Foxx, 2004). Onli-

ne-Vertrauen wird immer dann generiert, wenn der Konsument positive Eindrücke der Webpräsenz eines Transaktionspartners gesammelt hat und deshalb bereit ist, ein bestimmtes Mass möglicher Enttäuschungen in der Interaktion mit dem Geschäftspartner zu akzeptieren (Urban et al., 2009). Ein ganz wesentliches Element des Online-Vertrauens ist die Bereitschaft, persönliche Daten mitzuteilen. Eine solche Mitteilung setzt den Nutzer einer gewissen Verwundbarkeit, einem Risiko aus. Zugleich ist sie jedoch eine notwendige Voraussetzung für die Durchführung einer Online-Transaktion (Scheonbachler & Gordon, 2002).

Wenn Nutzer vor der Entscheidung stehen, eine Online-Transaktion durchzuführen, haben sie daher eine Abwägung zu treffen: Ist man bereit, die geforderten Daten preiszugeben, um dafür den erwarteten Nutzen in Empfang nehmen zu können? Damit wird ein wesentliches Phänomen des Nutzerumgangs mit persönlichen Daten ersichtlich: Die Entscheidung über die Preisgabe persönlicher Daten fällt vor dem Hintergrund einer Abwägung des Umfangs erforderlicher Daten einerseits, und erwarteter Nutzengewinne andererseits (Phelps et al., 2000). Wenn der erwartete Nutzen einer Transaktion das empfundene Risiko durch die notwendige Preisgabe persönlicher Daten überschreitet, wird sie eingegangen werden (Sheehan & Hoy, 2000; Olivero & Lunt, 2004). Diese Feststellung erleichtert die Interpretation des beschriebenen Phänomens der Selbstdarstellung in sozialen Netzwerken: Die jungen Mitglieder einer Plattform wie Facebook sind offensichtlich bereit, Details über das (bisweilen intimste) Privatleben zu offenbaren, um auf dieser Grundlage Freundschaften pflegen oder Kontakte knüpfen zu können - ein offenbar höchst bedeutsamer Nutzen.

Noch nicht beantwortet ist damit jedoch die Frage, auf welcher Basis Nutzer eben diese Abwägung vornehmen, welche Einflussfaktoren jeweils das Risiko oder den Nutzen als grösser erscheinen lassen und somit zur Ablehnung oder Akzeptanz einer Online-Transaktion führen. Zahlreiche Studien haben den Versuch unternommen, jene Einflussfaktoren zu identifizieren, die Vertrauen erzeugen, bzw. Risikowahrnehmungen reduzieren. Die Forschung hat gezeigt, dass die Anzahl der das Nutzervertrauen beeinflussenden Elemente enorm hoch ist, da nicht nur der Auftritt und die Vermittlung der Webpräsenz eines Anbieters einen Einfluss entfaltet: Einerseits wird das Nutzervertrauen auch durch individuelle Persönlichkeitsfaktoren geprägt, wie etwa die Risikoneigung oder soziodemographische Faktoren. Andererseits entwickeln Nutzer auch Vertrauen gegenüber gewissen grundlegenden Institutionen, wie etwa dem Rechtsrahmen oder dem Medium Internet (Milne & Boza, 1999; Hoffman et al., 1999a; Walczuch & Lundgren, 2004; Olivero & Lunt, 2004; Ashworth & Free, 2006; Lanier & Saini, 2008). Vertrauensfaktoren sind also auf einer Mikroebene abhängig von Eigenschaften des jeweiligen Individuums, auf einer Mesoebene von Eigenschaften des Interaktionspartners und schliesslich auf einer Makroebene von Eigenschaften des kulturellen und institutionellen Kontextes (s. Abb. 8).



*Abbildung 8: Einflussfaktoren des Nutzervertrauens*

Die vorliegende Studie konzentriert sich in diesem Spannungsfeld auf die Mesoebene, also jene des Transaktionspartners. Sie soll die Frage beantworten, welche Eigenschaften eines Online-Angebots, bzw. der Darstellung dieses Angebots, das wahrgenommene Vertrauen der Nutzer erhöht - und damit das wahrgenommene Risiko reduziert - und so die Wahrscheinlichkeit des Zustandekommens einer Transaktion erhöht. Durchgeführt wurde die Studie auf dem deutschen Markt, die hier präsentierten Ergebnisse sind also stets im Kontext jener kulturellen und institutionellen Einflussfaktoren zu interpretieren, welche charakteristisch für die Bundesrepublik Deutschland sind.

## ZUSAMMENFASSUNG

Das Internet ist heute die Basis unzähliger privater und geschäftlicher Transaktionen, es prägt die ökonomische, politische und kulturelle Entwicklung einer Gesellschaft. Dies gilt insbesondere für das Zeitalter des "Web 2.0", in welchem neue Applikationen jedem Nutzer die Möglichkeit geben, Informationen und digitale Inhalte auf einfache Weise zu erstellen, gestalten, teilen und publizieren. Diese neuen Potentiale der vierteiligen, non-zentralen Kommunikation und des Austausches sind unweigerlich verbunden mit der Übermittlung persönlicher Daten in einem bisher ungeahnten Ausmass. Während schon das "Web 1.0" den Austausch von Daten zur Voraussetzung für das Zustandekommen elektronisch vermittelter Wertschöpfungsprozesse machte, und so die Sammlung und Auswertung enormer Datenmengen auf Seiten der Anbieter nach sich zog, erfordern die Sozialen Medien darüber hinaus eine Positionierung der Teilnehmer innerhalb ihrer Gemeinschaften und Netzwerke. Das elektronische Aufbauen, Pflegen und Nutzen persönlicher Beziehungsnetze - wie sie zentrale Eigenschaft des Web 2.0 sind - ist unweigerlich mit der Mitteilung und Verbreitung zahlreicher persönlicher Daten verbunden. Das Web 2.0 bereitet die Bühne, auf der wir Nutzer unsere Rollen einnehmen und ausleben. Umso bedeutender sind zeitgemässe Ansätze des elektronischen Identitätsmanagements.

Das Zustandekommen von Transaktionen im Netz setzt das Vertrauen der Interaktionspartner voraus. Vertrauen bedeutet dabei die Bereitschaft, ein gewisses Risiko einzugehen, in der Erwartung, dass ein potentieller Nutzen dieses überwiegt. Im Kontext der Internetwirtschaft beziehen sich Risikowahrnehmung oder Sorgen insbesondere auf der Gewährleistung der Sicherheit sowie der Privatsphäre der Nutzer. Bevor also ein Nutzer einem Interaktionspartner seine persönlichen Daten zur Verfügung stellt, hat er mögliche Risiken in Hinblick auf seine Sicherheit und Privatheit gegen den erhofften Nutzen abzuwägen. Im Rahmen dieser Abwägung spielen neben den Persönlichkeitseigenschaften der Nutzer sowie institutionelle Einflussfaktoren vor allem die wahrgenommenen Eigenschaften des Transaktionspartners eine Rolle. Diese können als "Vertrauensfaktoren" bezeichnet werden. Die vorliegende Studie hatte zum Ziel, die zentralen Vertrauensfaktoren im Rahmen von Online-Transaktionen für den deutschen Markt zu identifizieren und differenzieren, um so eine nutzergerechte Ausrichtung und Vermittlung des elektronischen Identitätsmanagement zu ermöglichen.



## VORGEHEN UND FORSCHUNGSMETHODEN

Um die definierten Forschungsfragen zu beantworten, und vertiefte Einblicke in die Wahrnehmungen der betroffenen Anbieter und der Nutzer erlangen zu können, entschied sich das Forschungsteam für einen interpretativen Forschungsansatz (Denzin, 1983). In einem ersten Schritt wurden mittels explorativer Erhebungen - in Verbindung mit einer gründlichen Analyse vorliegender Forschungsergebnisse - mögliche Einflussfaktoren auf das Vertrauen der Internetnutzer identifiziert. In einem zweiten Schritt wurden diese Faktoren auf Basis einer breit angelegten quantitativen Erhebung differenziert und validiert. Dieses Vorgehen sollte sicherstellen, dass ein umfassender, fundierter Einblick in die komplexen Konstrukte des Forschungsgegenstandes sichergestellt werden kann.

### PHASE 1: QUALITATIVE ANBIETER-INTERVIEWS

#### ***Datenerhebung: Leitfadenbasierte Interviews***

Der erste empirische Schritt der Studie stellte eine Expertenbefragung dar, mit dem Ziel, einen durch Erfahrung substantiierten Überblick über die relevanten Einflussfaktoren des Forschungsfeldes zu gewinnen. Unter "Experten" werden dabei Personen verstanden, die über besonderes Wissen verfügen, das sie auf Anfrage weitergeben oder für die Lösung besonderer Probleme einsetzen können (Mehrmann, 1995). Im vorliegenden Kontext entschied sich das Forschungsteam, die Kommunikationsverantwortlichen einer Reihe von Anbietern von Online-Applikationen auf dem deutschen Markt zu untersuchen. Mitarbeiter der Kommunikationsabteilungen wurden ausgewählt, da diese sich berufsmässig mit der Wahrnehmung des Anbieters durch zahlreiche Zielgruppen befassen, und insbesondere auch mit den (positiven wie negativen) Wahrnehmungen seiner Nutzer konfrontiert sind (Grunig & Hunt, 1984; Dozier & Ehling, 1992; Grunig, 1993; van Riel, 1992). Experteninterviews sind erfahrungsgemäss besonders geeignet für Untersuchungen, in deren Rahmen soziale Situationen oder Prozesse rekonstruiert werden sollen, und dienen dazu, eine sozialwissenschaftliche Erklärung für diese zu finden (Gläser & Laudel, 2006.).

Im Zeitraum von März bis Oktober 2009 wurden 23 Kommunikationsverantwortliche von 21 Internetanbietern befragt, welche auf dem deutschen Markt tätig sind. Dabei folgten die Autoren einem explorativen Grounded Theory Ansatz (Glaser & Strauss, 1967). Die Erhebung, und damit verbunden auch das Sampling, einer solchen Studie zielen nicht auf die Hypothesen-Prüfung ab, sondern auf die Theoriegenese (Strübing, 2004). Umfang und Zusammensetzung der Stichprobe orientieren sich daher an der Zielvorgabe der theoretischen Sättigung (Glaser & Strauss, 1967). Glaser (1992) beschreibt theoretisches Sampling als ei-

nen Prozess, in dessen Rahmen Personen und Gruppen dem Sample hinzugefügt werden, sofern diese weitere Aufschlüsse über das untersuchte Phänomen oder dessen Kontext versprechen. So wurde auch in diesem Fall die Stichprobe schrittweise um Interviewpartner unterschiedlicher Eigenschaften erweitert, bis die parallel stattfindende Auswertung einen hinreichenden Grad theoretischer Sättigung erreichte, die Resultate also begannen, massgebliche Redundanzen aufzuweisen. Bei der Erweiterung der Stichprobe wurde insbesondere darauf geachtet, zahlreiche unterschiedliche Online-Geschäftsmodelle zu berücksichtigen. Die Differenzierung der Geschäftsmodelle wurde dabei auf Basis der Taxonomie von Timmers (1998) vorgenommen, da diese als theoretisch etabliert betrachtet werden kann und darüber hinaus Geschäftsmodelle nach Nutzererfahrungen differenziert, was für den vorliegenden Kontext besonders angebracht ist (Afuah & Tucci, 2001; Lambert, 2006). Timmers differenziert insbesondere die folgenden hier relevanten Business-to-Consumer (B2C) Geschäftsmodelle: e-shops (aufgrund grosser Überschneidungen wurden hier die Kategorien e-malls und third party marketplaces eingeschlossen), e-auctions, virtual communities, collaboration platforms, information brokers, and value chain service providers. Neben der Eigenschaft unterschiedlicher Geschäftsmodelle wurde auch auf eine Differenzierung der Grösse, Bekanntheit und des Alters der Anbieter geachtet - in der Stichprobe finden sich bekannte, etablierte Anbieter, wie etwa Google, eBay und XING, aber auch kleinere Anbieter und Start-ups wie Experteer, Mitfahrzentrale oder Wunderloop. Börsennotierte Unternehmen sind ebenso vertreten, wie private.

Die Teilnehmer wurden per eMail kontaktiert und über das Projektvorhaben informiert sowie um ein Telefongespräch gebeten. Die Datenerhebung folgte dem Muster eines problemzentrierten Interviews, welches gekennzeichnet ist durch „eine sehr lockere Bindung an einen knappen, der thematischen Orientierung dienenden Leitfaden“ mit der Absicht, „den Befragten sehr weitgehende Artikulationschancen einzuräumen und zu freien Erzählungen anzuregen“ (Witzel 1982, zit. in Hopf, 1991, S. 178). Der Interviewleitfaden basierte auf den aus der Literatur generierten Erkenntnissen; die Teilnehmer wurden jeweils in etwa halbstündigen Telefoninterviews nach dem Stellenwert des Nutzervertrauens in der Unternehmenspraxis befragt, nach Einflussfaktoren der Vertrauenswürdigkeit des eigenen Angebots sowie der Rolle des Datenschutzes, der Datensicherheit und des Identitätsmanagements. Dabei wurde auch der vielschichtige Umgang der Bürger mit den eigenen Daten im Austausch mit Privatunternehmen und dem Staat thematisiert. Der Interviewleitfaden findet sich im Anhang unter "A: Leitfaden Anbieter-Befragung". Tabelle 1 bietet einen Überblick über die Interviewpartner.

Nr.	Name	Geschäftsmodell	Gründungs- jahr	Rechts- form	Bör- sen- notiert	Umsatz 2008 (Mio. EUR)	Mitar- beiter	Interview Datum
1	Google	Information Broker	1998	AG	Ja	15'039	19'665	16.04.2009
2	Geschenke.de	e-Shop / e-Mall	2007	GmbH	Nein	3	35	19.03.2009
3	Gamesload**	e-Shop / e-Mall	2005	AG	Ja	61'700	260'000	06.04.2009
4	eBay	e-Auction	1995	AG	Ja	5'893	16'000	05.03.2009
5	DAB	e-Shop / e-Mall	1994	AG	Ja	137	693	20.03.2009
6	Cortal Consors	e-Shop / e-Mall	1994	AG	Nein	200*	1'500	19.02.2009
7	Buch.de	e-Shop / e-Mall	1998	AG	Ja	70	105	04.03.2009
8	Xing	Virtual Community	2003	AG	Ja	35	239	23.03.2009
9	Wunderloop	Information Broker	1999	GmbH	Nein	n/a	55	26.03.2009
10	Paypal	Value Chain Service Provider	1998	GmbH	Nein	n/a	2'000	09.03.2009
11	Mitfahrzentrale	Collaboration Plat- form	1998	GmbH	Nein	n/a	15	20.04.2009
12	Parship	Virtual Community	2000	GmbH	Nein	46*	190	12.03.2009
13	Postbank	e-Shop / e-Mall	1989	AG	Ja	9'930	21'130	19.03.2009
14	Atizo	Collaboration Plat- form	2008	GmbH	Nein	n/a	9	01.09.2009
15	Doodle	Collaboration Plat- form	2003	AG	Ja	n/a	9	04.08.2009
16	Guenstiger.de	Information Broker	1999	GmbH	Nein	n/a	n/a	22.09.2009
17	Auxion	e-Auction	1999	GmbH	Nein	n/a	n/a	17.09.2009
18	Wordpress	Collaboration Plat- form	2004	GmbH	Nein	n/a	40	13.10.2009
19	Experteer	Information Broker	2005	GmbH	Nein	n/a	n/a	28.09.2009
20	Deutsche Post	Value Chain Service Provider	1995	AG	Ja	54'190	456'716	26.10.2009
21	Unister GmbH	Virtual Community	2002	GmbH	Nein	n/a	500	01.09.2009

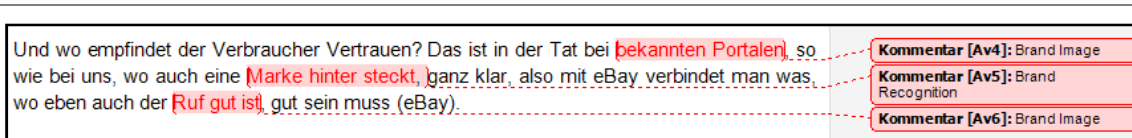
**Table 1:** Anbieterinterviews nach Geschäftsmodell

\*Daten von 2007

\*\*Daten der Muttergesellschaft

### **Datenauswertung: Theoriegenese**

Alle Interviews wurden aufgezeichnet, im Anschluss transkribiert und in einem iterativen Prozess durch mindestens zwei Vertreter des Forschungsteams unabhängig von einander ausgewertet. Auch die Datenauswertung folgte der Methode der Grounded Theory nach Glaser und Strauss (1967). Diese eignet sich besonders für die Konstruktbildung im Rahmen der Datenerhebung, da es sich um eine Methode induktiver Theoriegenerierung aus qualitativen, empirischen Daten handelt (Strauss & Corbin, 1998; Mayring, 2002). "The grounded theory approach is a general methodology of analysis linked with data collection that uses a systematically applied set of methods to generate an inductive theory about a substantive area" (Glaser, 1992, S. 16).



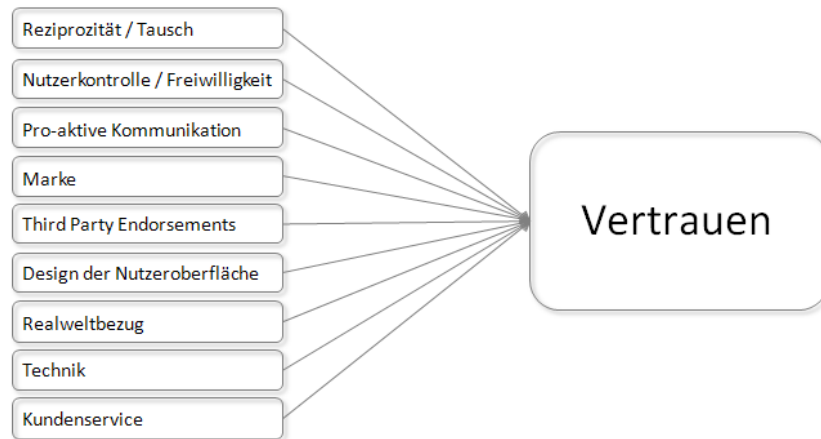
**Abbildung 9:** Kodierung der transkribierten Interviews

Aussagen, Sätze und Satzfragmente, welche bezug auf Bestimmungsfaktoren des Nutzervertrauens nahmen, wurden codiert und zu Kategorien zusammengefasst (Strauss & Corbin, 1998 - s. Abb. 5). Im Rahmen des selektiven Kodierens wurden erste, so genannte "Core Categories" herausgearbeitet (Strauss & Corbin, 1997). Anschliessend wurde geprüft, ob und in welcher Art Kategorien und Schlüsselkategorien zueinander im Verhältnis stehen. Der Vergleich der Daten auf Übereinstimmungen oder Unterschiede hilft dabei, angemessene Namen (Codes) für die zu beschreibenden Begebenheiten zu finden (Locke, 2001). Durch den Einbezug weiterer Interviews konnten die identifizierten Kategorien schrittweise erweitert und angepasst werden. Auf diese Weise wurden 60 vertrauensfördernde Faktoren aus den Gesprächen mit Anbietern von Online-Geschäftsmodellen abgeleitet. Diese Faktoren wurden vorerst zu neun Schlüsselkategorien zusammengefasst.

### **Überblick über Ergebnisse**

Das so entstandene erste Modell relevanter Vertrauensfaktoren aus Anbietersicht (s. Abbildung 10) verbindet Erkenntnisse unterschiedlicher Forschungsdisziplinen in einer integrierten Perspektive. Wie in der Literatur beschrieben, werden Nutzerdaten durch Online-Anbieter als Besitz ihrer Transaktionspartner betrachtet - Unternehmen müssen sich entsprechend bemühen, eine Bereitstellung dieser Daten durch das Angebot eines angemessenen Nutzens zu kompensieren (Das & Teng, 1998; Lanier & Saini, 2008; Chellappa & Sin, 2005; Ashworth & Free, 2006).

Dabei ist von besonderer Bedeutung, dass die Nutzer eine weitgehende Kontrolle über die eigene Datenbereitstellung behalten (Culnan & Armstrong, 1999; Milne & Boza, 1999; Phelps et al., 2001). Die pro-aktive Kommunikation der geplanten Datennutzung wird als vertrauenssteigernde Massnahme betrachtet (Chadwick, 2001; Geyskens, Steenkamp & Kumar, 1998; Lewicki & Bunker, 1995; Morgan & Hunt, 1994; Speier, Harbey & Palmer, 1998), wenngleich eine solche Kommunikationspolitik durch eine Steigerung der Aufmerksamkeit für mögliche Risiken auch Vorbehalte und Sorgen auf Nutzerseite erhöhen kann (Milne & Boza, 1999; Sheehan & Hoy, 1999).



**Abbildung 10:** Vertrauensfaktoren aus Sicht der Anbieter

Nutzervertrauen basiert aus Praxissicht vor allem auf einem entsprechenden Reputationsvorsprung des Anbieters, eine bekannte und sympathische Marke vermittelt diese Positionierung (Corbitt et al., 2003; Ha & Perks, 2005; Jevons & Gabbott, 2000; Walczuch & Lundgren, 2004; Eastlick et al., 2006; Milne & Boza, 1999). Wo eine solche Reputation noch nicht etabliert werden konnte, empfiehlt sich die Kooperation mit etablierten Anbietern und dritten Parteien (Corbitt et al., 2003; Kovar, Burke & Kovar, 2000; Luo & Cook, 2007-2008; Shneiderman, 2000). Darüber hinaus konnte die Erhebung zeigen, dass die Gestaltung der Benutzeroberflächen (Egger, 2000; Chau, Au & Tam, 2000; Shneiderman, 2000) sowie die Zuverlässigkeit der technischen Infrastruktur (Bhatnagar, Misra & Rao, 2000; Lee & Turban, 2001; Nielsen, 1999) als bedeutende Vertrauensstreiber betrachtet werden. Nicht zuletzt sollen auch die Erreichbarkeit des Anbieters und ein hilfsbereiter und freundlicher Kundenservice das Nutzervertrauen fördern (Brinkmann & Seifert, 2001; Lee & Turban, 2001; McAllister, 1995; Olivero & Lunt, 2004). Das so beschriebene Modell - bzw. die darin enthaltenen Faktoren - wurden in einem zweiten explorativen Schritt durch eine Analyse der Wahrnehmung der betroffenen Nutzer ergänzt und validiert.

## PHASE 2: QUALITATIVE NUTZER-INTERVIEWS

### ***Datenerhebung und -Auswertung: Leitfadensbasierte Interviews***

Zwischen Februar und April 2010 wurden in zwei süddeutschen Städten insgesamt 43 Personen im Rahmen von Strasseninterviews zu ihrer Internetnutzung befragt. Die Teilnehmer wurden durch Mitglieder des Forschungsteams angesprochen und für die Teilnahme an bis zu 30 minütigen Gesprächen gewonnen. 63% der Befragten waren weiblich, 37% männlich. Besonders jüngere Nutzer konnten für die Befragung gewonnen werden, 30% der Teilnehmer waren unter 25 Jahre alt, 50% zwischen 26 und 35, 20% waren älter als 36 Jahre. Eine Zusammenstellung der Teilnehmer findet sich in Tabelle 2.

Geschlecht	Alter	Beruf	Branche	Bildungsabschluss	Interview Datum
w	26-35	Assistentin	Dienstleistung	Diplom	23.02.2010
m	26-35	Sachbearbeiter	Dienstleistung	M.A.	02.03.2010
m	26-35	wiss. Mitarbeiter	Forschung	Diplom	03.03.2010
w	36-45	Projektleiter	Dienstleistung	Doktorat	03.03.2010
w	46-55	Marketingleiter	Dienstleistung	Doktorat	04.03.2010
m	26-35	Schauspieler	Kultur	Diplom	04.03.2010
w	26-35	Kaufmännische Angestellte	Elektroindustrie	Berufslehre	05.03.2010
m	26-35	Ingenieur	Energie	Doktorat	05.03.2010
m	26-35	Ingenieur	Energie	Diplom	05.03.2010
m	46-55	Maschinenbau-Ing.	Industriegüter	Diplomingenieur FH	05.03.2010
w	26-35	wiss. Mitarbeiterin	Forschung	Magister	08.03.2010
m	26-35	Ingenieur	Energie	Diplom	08.03.2010
w	26-35	Studentin (auf Stellensuche)	---	M.A.	09.03.2010
w	26-35	wiss. Mitarbeiterin	Forschung	Diplom	11.03.2010
m	56-65	Arzt	Medizin	Doktorat	11.03.2010
m	26-35	Sachbearbeiter	Dienstleistung	Diplom	15.03.2010
w	26-35	Bankkauffrau	Finanzdienstleistung	Mittlere Reife	16.03.2010
w	26-35	Assistentin	Dienstleistung	Diplom	16.03.2010
w	26-35	Assistentin	Dienstleistung	Diplom	16.03.2010
w	56-65	Praxisassistentin	Medizin	Diplom	16.03.2010
w	< 25	Studentin	in Ausbildung	Abitur	17.03.2010
m	26-35	Ingenieur	Rohstoffe	Diplom	17.03.2010
w	26-35	wiss. Mitarbeiterin	Forschung	Diplom	23.03.2010
w	< 25	Studentin	in Ausbildung	Diplom	24.03.2010
w	26-35	Schulpsychologin	Medizin	Doktorat	09.04.2010
m	66 +	Rentner	---	Berufslehre	15.04.2010
w	26-35	Journalistin	Medien	Abitur	26.04.2010
w	26-35	Assistenz	Medizin	Staatsexamen	27.04.2010
w	26-35	Assistenz	Medizin	Staatsexamen	27.04.2010
m	36-45	Abteilungsleiter	Forschung	Doktorat	27.04.2010
w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
w	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
w	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
w	26-35	Sozialpädagogin	Dienstleistung	Erlebnispädagogin	27.04.2010
m	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
m	< 25	Maschinenbauingenieur	in Ausbildung	Diplom	27.04.2010
m	56-65	Freischaffend	Automobilindustrie	Abitur	27.04.2010
w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
w	< 25	Kellnerin	in Ausbildung	Abitur	27.04.2010
m	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010

*Tabelle 2: Demographische Daten der Nutzerinterviews*

Die Befragung wurde mit allgemeinen Fragen zur Internetnutzung eingeleitet, im Anschluss wurden spezifische Fragen in Hinblick auf Anmeldeprozesse im Internet gestellt sowie die Bereitschaft, persönliche Daten zur Verfügung zu stellen. Anhand des jüngsten beschriebenen Anmeldeprozesses wurde vertieft erfragt, welche Elemente oder Faktoren

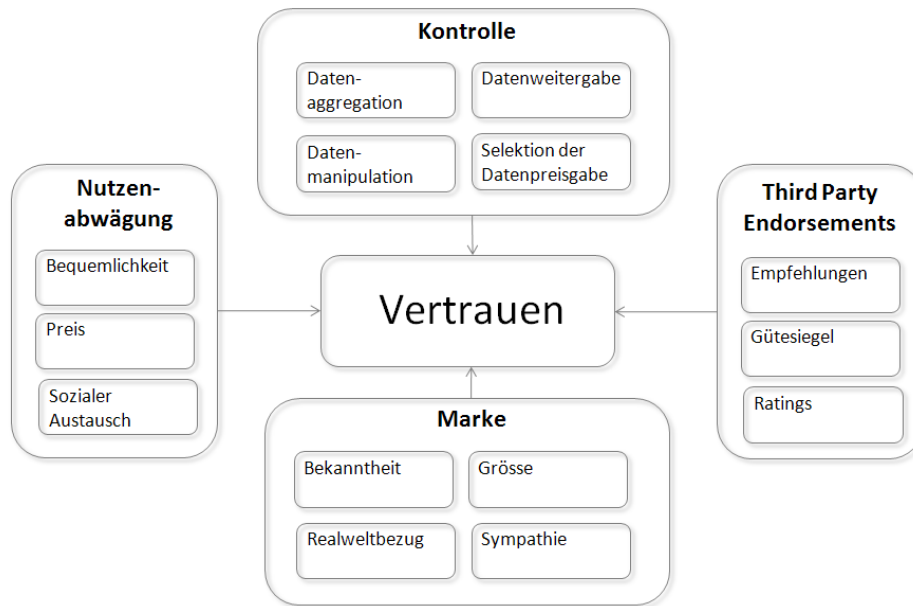
die Entscheidungsfindung der Betroffenen positiv oder negativ beeinflussten. Dabei wurde auch auf mögliche Unterschiede zwischen privaten und öffentlichen Online-Angeboten eingegangen. Der Leitfaden findet sich im Anhang unter "B: Leitfaden Nutzer-Befragung".

Alle Interviews wurden wiederum aufgezeichnet und transkribiert. Die Auswertung der Texte basierte auf oben beschriebenem Grounded Theory-Ansatz und wurde von mindestens zwei Mitgliedern des Forschungsteams unabhängig von einander vorgenommen. Erneut wurden auf diese Weise mögliche Vertrauensfaktoren identifiziert, zu Kategorien verdichtet und in einem zweiten Modell zusammengefasst (s. Abb. 11).

### ***Überblick über Ergebnisse***

Das aus den Nutzerinterviews generierte Modell erwies sich als weitgehend Deckungsgleich mit jenem der Anbieterseite, jedoch als weniger differenziert. Genauer konnten auf Nutzerseite Kategorien gebildet werden, welche auch im ersten beschriebenen Modell enthalten sind - teilweise sogar durch eine grössere Anzahl Faktoren unterlegt -, das Anbietermodell enthält jedoch darüber hinaus weitere Kategorien. Diese teilweise Überschneidung wurde vor allem auf die Erhebungsmethode sowie die unterschiedliche Kategorisierung der Interviewpartner zurückgeführt: Die Vertreter der Anbieterseite verfügten aufgrund der schriftlichen Einladung über mehr Zeit zur Reflektion des Befragungsgegenstandes in Vorbereitung des Interviews. In ihrer Rolle als Experten sind sie, beruflich bedingt, darüber hinaus auch im Alltag zu einer vertieften Auseinandersetzung mit dem Befragungsgegenstand angehalten. Die qualitativen Nutzerinterviews konnten dagegen vor allem jene Faktoren identifizieren, die in der bewussten Wahrnehmung der Nutzer von grösster Signifikanz sind.

Zusammenfassend beschreibt das zweite Modell relevanter Vertrauensfaktoren eine Konzentration auf wenige zentrale Elemente: Die Abwägung des Nutzens, Empfehlungen, die Bekanntheit und Sympathie der Marke sowie die Abwägung eines möglichen Kontrollverlusts über persönliche Daten. Das anbieterseitige Modell (Abbildung 10) berücksichtigt darüber hinaus eine Reihe weiterer Kategorien, wie Design, Kundenservice und Technik sowie Pro-aktive Kommunikation. Diese mögen durchaus einen Einfluss auf die Wahrnehmung der Nutzer entfalten, gehören jedoch nicht zu den bewusst als am signifikantesten empfundenen. Die Kategorie "Nutzenabwägung" des zweiten Modells entspricht weitgehend dem der "Reziprozität" im ersten, wobei die Anbieter stärker darauf hinwiesen, dass der Nutzen in Relation zu einem Risiko abgewogen wird. Der Faktor der "Third Party Endorsements" wurde auf Nutzerseite differenzierter betrachtet, indem hier neben Gütesiegeln vor allem auch Empfehlungen oder Ratings von anderen Nutzern oder Freunden und Bekannten genannt wurden.



**Abbildung 11:** Vertrauensfaktoren aus Sicht der Nutzer

Gemeinsam bieten die beschriebenen explorativen Phasen einen umfassenden und theoretisch fundierten Überblick über mögliche Einflussfaktoren des Nutzervertrauens, sie ermöglichen jedoch nicht die relative Gewichtung dieser Faktoren. Notwendig war daher in einem abschliessenden empirischen Schritt eine nach Möglichkeit repräsentative Erhebung unter deutschen Internet-Nutzern, welche eine Validierung und Differenzierung der Faktoren bzw. Kategorien ermöglichen sollte.

## PHASE 3: QUANTITATIVE NUTZER-BEFragung

### **Datenerhebung: Online-Befragung**

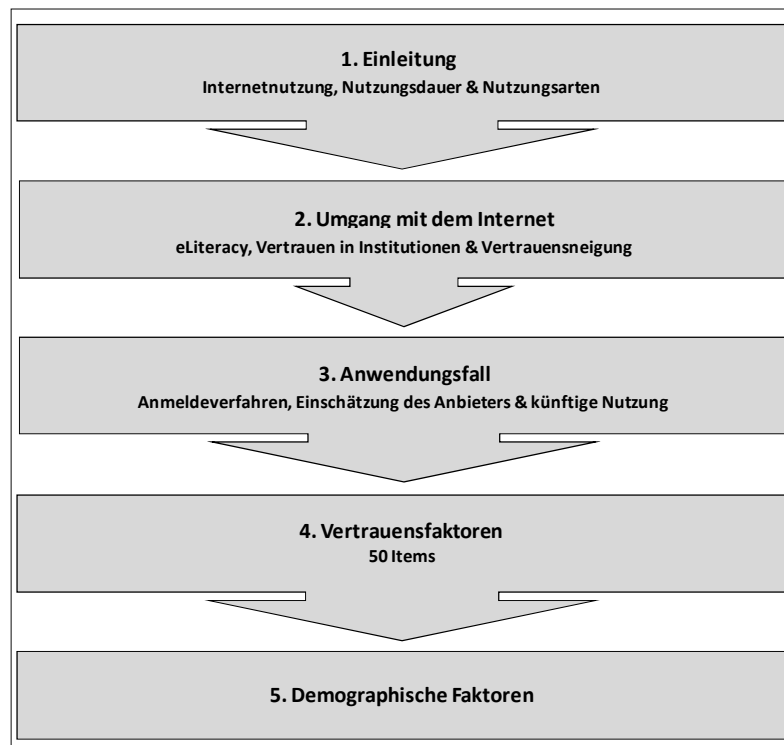
Auf Basis der erhobenen Daten der qualitativen Phasen sowie einer umfassenden Literatur-Analyse wurde eine Liste möglicher Einflussfaktoren auf das Nutzervertrauen erstellt, welche 50 Items enthielt. Diese wurden in den Fragebogen integriert, welche der quantitativen Umfrage zugrunde lag (s. Anhang C: Fragebogen der Online-Umfrage). Der Fragebogen beginnt mit einführenden Fragen, welche die Internet-Nutzungsgewohnheiten der Teilnehmer erkunden, etwa die Nutzungsdauer und -art (beruflich oder privat). Ein zweiter Abschnitt des Fragebogens befasst sich mit der Nutzungskompetenz der Teilnehmer, sowie einigen persönlichen und institutionellen Vertrauensfaktoren. Schliesslich wurden die Nutzer gebeten, jenen Online-Anbieter zu nennen, bei dem sie sich zuletzt als Nutzer registriert haben, wobei die Anmeldung die Eingabe einiger persönlicher Daten erforderte. Der betreffende Anbieter sollte auch einem von vier vorgeschlagenen Online-Geschäftsmodellen zugeordnet werden (Online-Shopping, Online-Banking, Online-

Communities und Online-Informationen). Die Kategorisierung orientierte sich erneut an der Taxonomie von Timmers (1998 - s. Tabelle 3). Die Vertrauenswürdigkeit des gewählten Anbieters sollte auf Basis eines etablierten Masses eingeschätzt werden.

Online Business Model	Nutzer	Prozentsatz
Online-Shopping (z.B. Amazon, eBay, Lufthansa)	599	46.29
Online-Banking (z.B. Comdirect, Postbank, PayPal)	204	15.77
Soziale Netzwerke / Online-Community (z.B. Facebook, Xing, Parship)	315	24.34
Online-Information (z.B. Zeitungen, Blogs, eMail)	176	13.60

*Tabelle 3: Anzahl Nutzer pro Geschäftsmodell*

Anschliessend wurden die Teilnehmer gebeten, die 50 Items anhand einer 5-stufigen Likert-Skala in Hinblick auf ihre Bedeutung für den Anmeldeentscheid einzuschätzen. "Nutzervertrauen" wurde also operationalisiert als die Bereitschaft, persönliche Daten bereitzustellen (Scheonbachler & Gordon, 2002; Wang et. al, 2004). Es sollte somit erkundet werden, inwiefern die identifizierten Items in der Wahrnehmung der Betroffenen in einem konkreten, realweltlichen Falle einen Einfluss auf die Entscheidung zu einer Anmeldung entfaltet haben. Abschliessend wurden einige demographische Daten, wie Geschlecht, Alter, Bildungsabschluss, Erwerbstätigkeit und Branche, erfragt. Abbildung 12 zeigt den Aufbau des Online-Fragebogens.



*Abbildung 12: Aufbau der Online-Befragung*

Der Fragebogen wurde einem zweistufigen Pretest unterzogen, in dessen ersten Schritt vier Experten der Medien- und Kommunikationsforschung die Reliabilität und Validität der Items begutachteten. In einem zweiten Schritt füllten 34 Nutzer den Bogen aus und beurteilten insbesondere die Verständlichkeit und Angemessenheit der Formulierungen. Der Pretest führte zu einer geringfügigen Anpassung der Fragenreihenfolge zu sowie der Korrektur weniger Item-Formulierungen.

	Item	Prozentsatz
Geschlecht	Weiblich	50.5
	Männlich	49.5
Alter	bis 15	10.1
	16 - 25	11.8
	26 - 45	26.2
	46 - 65	26.4
	66 +	19.6
	keine Angabe	5.8
	Höchster Bildungsabschluss	Hauptschulabschluss
	Realschulabschluss	16.9
	Berufslehre	20.2
	Abitur / Fachabitur	17.7
	Fachhochschule / Studium	25.0
	noch in schulischer Ausbildung	12.5
	Sonstige	1.5
Erwerbstätigkeit	Angestellt (Vollzeit / Teilzeit)	38.7
	Selbständig erwerbstätig	9.5
	Arbeitssuchend	3.6
	in Ausbildung / Lehre	12.2
	in Rente	24.5
	Hausfrau / Hausmann	4.4
	keine Angabe	7.1
Internetnutzung	täglich	92.6
	mehrmals pro Woche	7.4
	weniger als einmal pro Woche	0.1
Jahre der Internetnutzung	< 1 Jahren	0.2
	seit 1 Jahren	0.5
	seit 2 Jahren	1.4
	seit 3 Jahren	4.7
	seit 4 Jahren	5.6
	seit 5 Jahren	10.5
	seit 6 Jahren	7.5
	seit 7 Jahren	5.4
	seit 8 Jahren	7.7
	> 8 Jahren	54.9
	keine Antwort	1.6
Art der Internetnutzung	ausschliesslich beruflich	0.1
	überwiegend beruflich	1.2
	sowohl beruflich als auch privat	48.0
	überwiegend privat	23.8
	ausschliesslich privat	26.9

**Tabelle 4:** Zusammensetzung der Stichprobe der Online-Umfrage (n=1294)

Die Teilnehmer der Online-Umfrage wurden durch Vermittlung eines deutschen Marktforschungsinstituts gewonnen, welches den Zugang zu einem für die Bundesrepublik Deutschland bevölkerungsrepräsentativen Panel ermöglichte. Die Stichprobe war dabei nach Geschlecht und Alter quotiert. Im Dezember 2010 wurden insgesamt 11'846 Internetnutzer per eMail zur Umfrage eingeladen. Als Motivation diente ein kleiner Geldbetrag, welcher über das Marktforschungsinstitut ausbezahlt wurde. 1'502 Teilnehmer nahmen an der Umfrage teil, was einer Rücklaufquote von ca. 13% entspricht. 1'294 vollständig ausgefüllte Bogen flossen in die anschliessende Analyse ein. Die Zusammensetzung der Stichprobe kann Tabelle 4 entnommen werden.

Die Stichprobe weist eine Übervertretung regelmässiger Internetnutzer auf: 92% der Teilnehmer nutzen das Internet täglich, während 2009 in Deutschland nur 67% das Internet zumindest gelegentlich benutzen (van Eimeren & Frees, 2009). Nur 1% der Befragten nutzt das Internet ausschliesslich zu beruflichen Zwecken. Diese Verzerrung kann durch die Rekrutierungsmethode erklärt werden, da die Probanden per eMail zur Umfrage eingeladen wurden. Nicht-Internet-Nutzer, dies sind in Deutschland 25% der männlichen und 40% der weiblichen Bevölkerung, wurden von der quantitativen Erhebung gänzlich ausgeschlossen. 2009 betrug in Deutschland der Anteil der Internetnutzer 98% unter den 14 bis 19-jährigen, 98% unter den Personen in Ausbildung, 82% unter Angestellten und 34% unter Personen im Ruhestand (van Eimeren & Frees, 2009).

### ***Datenauswertung: Explorative Faktorenanalyse***

Um abschliessend Einflussfaktoren des Nutzervertrauens zu identifizieren und differenzieren, wurden die gewonnenen Daten einer explorativen Faktorenanalyse unterzogen. Die Faktorenanalyse eignet sich besonders, eine Vielzahl von Variablen (wie sie eine Itembatterie darstellt) auf zugrundeliegende Phänomene zu reduzieren (Arminger, 1979; Überla, 1977). Sie zeigt, welche Items miteinander besonders hoch korrelieren (Korrelation  $> 0.5$ ) und sich daher zu einem (zugrundeliegenden) Faktor zusammenfassen lassen. Die Faktorladung zeigt dabei, wie stark ein Item mit dem Faktor verbunden ist (Geider, Rogge & Schaaf, 1982). Ziel der Faktorenanalyse ist es, die Beziehungen einer Variablengruppe auf einige wenige Faktoren zu konzentrieren, um dadurch den Sachverhalt vereinfacht darstellen zu können (Backhaus, Erichson, Plinke & Weiber, 2011; Geider et al., 1982). Die explorative Faktorenanalyse findet dabei insbesondere Anwendung, wenn die Faktoren nicht theoriegeleitet definiert sondern aus den Ladungsmatrizen extrapoliert werden (Arminger, 1979).

Damit eine Faktorenanalyse vorgenommen werden kann, müssen die Variablen auf eine Normalverteilung (NV) angepasst werden. Bei den betrachteten Variablen lagen entweder normale oder rechtsschiefe Verteilungen vor. Eine rechtsschiefe Verteilung kann im vorliegenden Kontext als Hinweis auf Anspruchsinflation gedeutet und somit als eine "Überschätzung" des entsprechenden Items interpretiert werden. Die Anpassung der rechtsschie-

fen Variablen an die NV wurde entweder mittels Transformation oder Skalenverkürzung vorgenommen. Im Falle der Transformation wurden die Ursprungsdaten potenziert ( $x^{3-5}$ ). Im Rahmen der Skalenverkürzung wurden die Skalenwerte 4 und 5 zusammengefasst, so dass sich im Ergebnis eine 4er-Likertskala ergab. Dieses Vorgehen ist damit zu begründen, dass bei einer starken Überschätzung des Items die Kategorien "wenig beachtet" und "nicht beachtet" nahezu bedeutungsgleich werden.

Die Berechnung der explorativen Faktorenanalyse erfolgte auf Basis der normalverteilten Items. Die Datenanalyse wurde auf Basis des Programms PASW Statistics 18 durchgeführt. Die Eignung des Datensatzes wurde mit der Anwendung des Kaiser-Meyer-Olkin-Kriteriums (KMO) sowie des Bartlett-Test (s. Tabelle 5) geprüft. Um die Anzahl der Faktoren zu bestimmen, wurde das Eigenwert-Kriterium angewandt (Eigenwert nicht kleiner als 1) (Tabachnick, 2007). Im Anschluss an die Bestimmung der Faktoren-Anzahl wurde die Faktorladungsmatrix nach Varimaxverfahren rotiert.

Kaiser-Meyer-Olkin Kriterium		.969
Bartlett-Test auf Sphärität	Approx. Chi-Square	40097.829
	df	1225
	Sig.	.000

*Tabelle 5: KMO und Bartlett's Test*

Die Hauptkomponentenanalyse extrahierte sieben Faktoren - Tabelle 6 zeigt die Eigenwerte und den Anteil erklärter Varianz jedes Faktors. Drei der 50 analysierten Items wurden ausgeschlossen, da ihre Faktorladungen und Extraktionswerte unter dem Grenzwert lagen. Die rotierten Faktorladungen und Extraktionswerte werden im folgenden Kapitel beschrieben. Cronbachs Alpha wurde für jeden Faktor berechnet um die Zuverlässigkeit der Messung festzustellen - dieser Wert liegt für alle Faktoren über dem Grenzwert. Offenbar trug der explorative Forschungsansatz, welcher qualitative Interviews zugrunde legte, zur Validität der Erhebung bei und führte zu einer hohen Massqualität. Auffällig ist der hohe Anteil erklärter Varianz des Faktors Reziprozität, welcher etwa 35% beträgt, während alle anderen Faktoren gemeinsam lediglich 27% der Varianz erklären.

Bei der Analyse wurde deutlich, dass die Items des Faktors "Technische Zuverlässigkeit" nur schlecht extrahiert werden konnten (Extraction < 0.5). Als Konsequenz musste "Technische Zuverlässigkeit" daher aus den folgenden Berechnungen ausgeschlossen werden. Alle anderen Faktoren wiesen hohe Ladungen auf (Ladungen > 0.5). Es konnten zudem keinerlei Kreuzladungen zwischen den Items der Einflussfaktoren festgestellt werden.

Faktoren	Interpretation	Eigenwert	Anteil erklärter Varianz
Faktor 1	Reziprozität	17.679	35.358
Faktor 2	Marke & Design	4.018	8.037
Faktor 3	Nutzerkontrolle	3.163	6.326
Faktor 4	Kundenservice	2.353	4.706
Faktor 5	Realweltbezug	1.491	2.981
Faktor 6	Technische Zuverlässigkeit	1.153	2.305
Faktor 7	Third Party Endorsements	1.072	2.144
	Kumulativ		61.858

*Tabelle 6: Explorative Faktorenanalyse*

### **Datenauswertung: Korrelationsanalyse der Faktoren**

Teil der Erhebung war auch eine Einschätzung der Vertrauenswürdigkeit des gewählten Anbieters durch die Teilnehmer. In einem letzten analytischen Schritt sollte daher untersucht werden, inwiefern die identifizierten Vertrauensfaktoren tatsächlich mit dem Vertrauensmass korrelieren. Die Berechnung des Pearson-Korrelations-Koeffizienten setzt normalverteilte Variablen voraus. Da alle Faktorenwerte automatisch aufgrund des Berechnungsalgorithmus z-transformiert (d.h. Mittelwert = 0 und S.D. = ca. 1) sind, ist die Anwendung hier möglich. Alle Einflussfaktoren korrelieren höchst signifikant mit dem Vertrauensmass (\*\*  $p < 0.001$ ). Die stärkste Korrelation besteht zwischen "Reziprozität" und "Vertrauen", doch auch "Marke & Design" sowie "Kundenservice" entpuppen sich als massgebliche Einflussfaktoren. Tabelle 7 zeigt die Korrelationen sortiert nach deren Stärke:

Faktor	Korrelation zu "Trust"
Reziprozität	.502**
Marke & Design	.481**
Kundenservice	.464**
Nutzerkontrolle	.280**
Third Party Endorsements	.245**
Realweltbezug	.202**

*Tabelle 7: Korrelation Faktoren und Vertrauen*

## ZUSAMMENFASSUNG

Unsere Studie, basierend auf zwei explorativen, qualitativen Erhebungen sowie einer quantitativen Umfrage, konnte 47 Items identifizieren, welche die Bereitschaft der Nutzer, im Rahmen einer Online-Transaktion persönliche Daten zur Verfügung zu stellen, beeinflussen. Diese Items können zusammenfassend auf 7 zugrunde liegende Vertrauensfaktoren reduziert werden. Sechs dieser Faktoren korrelieren in unterschiedlichem Masse mit der aggregierten Vertrauenswahrnehmung der Nutzer. Das folgende Kapitel wird die identifizierten Faktoren ausführlich beschreiben, einschliesslich einiger illustrativer Kommentare der befragten Praktiker und Nutzer.

# IV. RESULTATE: TREIBER DES NUTZERVERTRAUENS

## EINFLUSSFAKTOREN IM ÜBERBLICK

Nutzer bilden sich ein Urteil über die Vertrauenswürdigkeit eines Online-Angebots, indem sie entsprechende Hinweise und Signale sammeln und zu einem konsistenten Bild zusammenfügen. Es handelt sich dabei vor allem um Eigenschaften oder Elemente der Web-Präsenz, also der Homepage eines Anbieters (Friedman et al., 2000; Jarvenpaa et al., 2000). Wie bereits festgestellt, sind es jedoch nicht Eigenschaften des Transaktionspartners alleine, die zur Entstehung von Vertrauen beitragen. Vielmehr existieren daneben eine Reihe bedeutsamer individueller wie institutioneller Faktoren, die in der Vertrauensbildung eine Rolle spielen: Individuen sind je nach persönlichen Charakterzügen, demographischen Variablen oder psychologischen Merkmalen, wie Extrovertiertheit oder Gewissenhaftigkeit, mehr oder weniger empfänglich für Vertrauen. Das Vertrauen in einen Transaktionspartner ist darüber hinaus immer auch getragen vom Vertrauen in zugrundeliegende Institutionen, wie etwa das Medium Internet oder die relevanten rechtlichen Rahmenbedingungen (Sheehan & Hoy, 2000; Lee & Turban, 2001; Walczuch & Lundgren, 2004; Lanier & Saini, 2008).

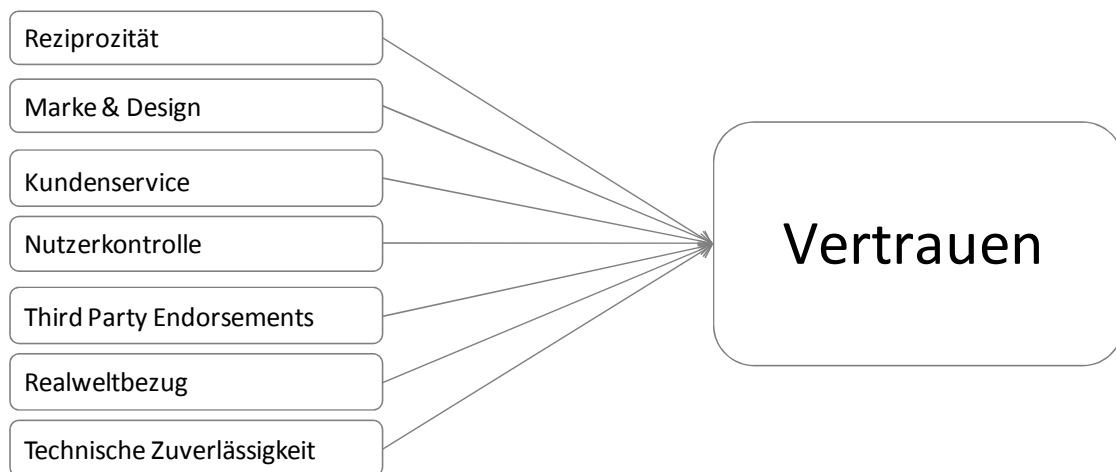


Abbildung 13: Durch Umfrage identifizierte Vertrauensfaktoren

An dieser Stelle sollen jedoch insbesondere jene Vertrauensfaktoren beleuchtet werden, die tatsächlich durch einen Online-Anbieter beeinflusst werden können. Unsere Analyse ergab sieben solcher Faktoren: Reziprozität, Marke & Design, Kundenservice, Nutzerkontrolle, Third Party Endorsements, Realweltbezug und Technische Zuverlässigkeit (s. Abb. 13).

Diese werden im Folgenden detailliert vorgestellt und beschrieben. Dabei werden illustrierend einzelne Zitate aus den geführten Interviews mit Anbietern (A) und Nutzern (N) eingebunden.

## REZIPROZITÄT: VERTRAUEN ALS NUTZENABWÄGUNG

Persönliche Daten können als eine Art Währung des Internet-Zeitalters betrachtet werden. Online-Transaktionen berühren regelmässig die Privatsphäre der beteiligten Nutzer: “In fact, it may be quite impossible for customers to transact business on the Internet without revealing information about themselves that they may be unwilling to share” (Rust et al., 2002, S. 455). Eine Betrachtung persönlicher Daten als Tauschmittel impliziert jedoch auch, dass diese in einen Tauschprozess eingebracht werden, in welchem Gewinne und Verluste kalkuliert werden. Und tatsächlich: Wenn Nutzer vor der Entscheidung stehen, eine Online-Transaktion durchzuführen, haben sie eine Abwägung zu treffen. Im Zentrum steht dabei die Frage, welcher Nutzen durch die Bereitstellung der geforderten Daten gewonnen werden kann, und welches Risiko, also welche möglichen Verluste, dem gegenüber steht.

Factor 1	Loading	Extraction
i 1.1) Die Datenschutzbestimmungen sind leicht verständlich.	.814	.769
i 1.2) Die Allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	.786	.709
i 1.3) Die Datenschutzbestimmungen sind leicht zu finden.	.753	.707
i 1.4) Die Allgemeinen Geschäftsbedingungen sind leicht zu finden.	.739	.683
i 1.5) Der Anbieter verfügt über strikte Datenschutzrichtlinien.	.691	.662
i 1.6) Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z.B. Garantien, Rückgaberecht).	.651	.650
i 1.7) Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	.648	.606
i 1.8) Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	.646	.629
i 1.9) Der Anbieter bietet viele Informationen über das eigene Unternehmen.	.612	.593
i 1.10) Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.	.525	.658
i 1.11) Der Umfang der abgefragten Daten steht in einem passenden Verhältnis zum Nutzen, den mir der Dienst bietet.	.504	.612
i 1.12) Es ist gut erkennbar, welche Pflichten ich eingehe (z.B. Kosten).	.482	.585
Cronbach's Alpha = 0.937		

*Tabelle 8: Faktorladungen Reziprozität*

Der Wunsch nach Sicherheit und Privatheit ist daher nicht absolut, sondern relativ. Der Nutzer kann einmal das mögliche Risiko höher einschätzen, und von der Transaktion ab-

sehen. Ein anderes Mal kann dagegen der Nutzen verlockender erscheinen, und die Transaktion daher eingegangen werden (Phelps et al., 2000). Vertrauen, die Bereitschaft, persönliche Daten zur Verfügung zu stellen, wird dann aufgebracht, wenn der wahrgenommene Nutzen überwiegt (Olivero & Lunt, 2004). Online-Transaktionen müssen sich somit durch einen als "fair" empfundenen Grad an Reziprozität auszeichnen. So sollte beispielsweise der Kauf eines Buches nicht die Angabe religiöser Überzeugungen erfordern. Diese Kalkulation setzt jedoch voraus, dass der Nutzer die zu erwartenden Nutzen und Risiken tatsächlich abschätzen kann: Welche Daten hat der Nutzer bereitzustellen, um welchen Nutzen dadurch gewinnen zu können? Diesen Zusammenhang beschreibt der Vertrauensfaktor "Reziprozität" (s. Tabelle 8).

"Fair Information Practices" wurden in der Literatur verschiedentlich als eine Voraussetzung der Vertrauensbildung bezeichnet (Ashworth & Free, 2006). Anbieter sollten deutlich kommunizieren, welche Daten sie zu welchem Zweck benötigen (i. 1.7) und auf welche Weise diese Daten verwendet werden sollen (i. 1.8). Vertrauenserweckend wirkt, wenn sichtbar nur jene Daten erfragt werden, die für die Abwicklung des Angebots notwendig sind (i. 1.10 - s. Abb. 14).

*"Das heisst, dass der Kunde immer das Gefühl hat, zu wissen, was er jetzt zu tun hat, und dass an den Kunden auch sehr klar kommuniziert wird, welche Daten benötigt werden, und zwar zu welchem Zweck." (A3\_06.04.2009)*

*"(...) wo das Individuum etwas will, ist er auch bereit, etwas einzutragen. Also, wenn der Kunde ein Produkt kaufen will, sei das eine CD, ein Buch oder ein Bankprodukt, so schreibt er auch keine 'Mickey Mouse'-Daten in die Felder rein, das tut er nicht. Ich glaube, bei so Themen, wo er das Gefühl hat, dass es möglicherweise sensibel sein kann, überprüft er manchmal die Sinnhaftigkeit." (A5\_20.03.2009)*

*"Auf der anderen Seite funktioniert es ja sonst nicht, weil sie müssen es mir ja zuschicken und wenn sie nun keine Adresse und keinen Namen haben, können sie es mir ja nicht zuschicken." (N13\_09.03.2010)*

*"Und wenn die Datenfrage zu gross wird, das hatte ich auch schon, also wenn ich wirklich merke, die wollen wirklich alles wissen und Unternehmen und Fax-Nummer, dann breche ich auch ab. Und dann sage ich, okay, dann nicht." (N27\_26.04.2010)*

The image shows a contact information form titled "Contact Information" with a "\* required" label. The form includes fields for:
 

- Gender:  Mr  Mrs  Dr  Ms  Miss
- \* First name, Middle name, \* Last name, Suffix (dropdown)
- \* Email
- \* Address,  Home  Business
- \* City, State/province (required for USA), \* Zip/postal code (required for USA)
- \* Country (dropdown showing USA)
- Phone,  Home  Business  Mobile

 A blue link "Why provide my phone number?" is at the bottom left. A callout box on the right, titled "Why Provide my Phone Number?", contains the text:
 

is committed to providing you with personalized service. Having your phone number is another way for us to instantly identify you as a valued member when you call us. Please rest assured that your phone number or other contact information will never be shared with a third party.

 An arrow points from the link in the form to the callout box.

Abbildung 14: Zusatzinformationen sind erwünscht

Um die Reziprozität einer Transaktion jedoch abschätzen zu können, sind Informationen notwendig - zu den möglichen Risiken einer Transaktion, zu den Verpflichtungen, die der Nutzer eingeht, aber auch zu den Rechten, die ihm zugesichert werden. Hierzu gehören leicht auffindbare (i 1.3 & i 1.4) sowie verständliche (i 1.1 & i 1.2) Angaben zu den Datenschutzbestimmungen eines Anbieters sowie den Allgemeinen Geschäftsbedingungen. Auch Garantien oder Rückgaberechte fließen in diese Betrachtung ein (i 1.6). Informationen zum Geschäftsgebaren des Anbieters im Allgemeinen werden gerne gesehen (i 1.9).

*"Es bringt ja nichts, weil es ist ja irgend so eine juristische Formsache und ist alles dann immer mehr oder weniger also dasselbe, also, was soll man da noch seitenlang lesen."*  
(N39\_27.04.10)

*"Sicherlich hat es auch damit zu tun, dass eine Seite, die übersichtlich gestaltet ist, mit vielen Infoseiten zum Beispiel, wo der User darauf hingewiesen wird unter anderem, was mit seinen Daten geschieht oder grundsätzliche Informationen über den Service, grundsätzliche Informationen zum Anbieter. Das sind ja Massnahmen, die das Vertrauen steigern."*  
(A11\_20.04.2009)

Der Nutzer möchte also verstehen, welche Verpflichtungen er einem Anbieter gegenüber eingeht (i 1.12) und welche Ansprüche oder Rechte er dadurch erlangt (i 1.6). Die geforderten Daten müssen in einem angemessenen Verhältnis zum erwarteten Nutzen stehen (i 1.11). Damit wird jedoch auch deutlich: neben Rechten oder Risiken sollten Anbieter auch den Nutzen kommunizieren, den sie ihren Transaktionspartnern bieten. In der beschriebenen Abwägung spielt dieser eine entscheidende Rolle, denn nur angesichts des gebotenen Nutzens kann die Verhältnismässigkeit der erforderlichen Datensammlung beurteilt werden.

*„Und bin dann also wieder zu [Anbieter X] zurückgekehrt, natürlich in dem Bewusstsein, dass die vielleicht auch Daten von mir weitergeben, benutzen und machen und tun, aber was ich von denen will, war oder ist für mich einfach, steht an erster Stelle, nämlich, dass ich Informationen bekomme.“ (N27\_26.04.2010)*

*„(...) Also, dass man ihm nicht mehr die Pistole auf die Brust setzt und sagt, so, willst du eigentlich, dass irgendein Unternehmen weiss, was du vor 10 Jahren gekauft hast? Wahrscheinlich nicht, aber willst du eigentlich, dass es den Dienst gibt, der dir durchaus auch Vorstellungen, Vorschläge machen kann? Da wird er wahrscheinlich eher sagen, ja, warum nicht?“ (A4\_05.03.2009)*

## MARKE & DESIGN: BIG IS BEAUTIFUL

Nachdem Vertrauen als eine subjektive Wahrnehmung, ein Empfinden oder eine Überzeugung beschrieben werden kann, liegt es nahe, Vertrauensbildung als eine eminent kommunikative Aufgabe zu betrachten (Morgan & Hunt, 1994; Bart et al., 2005). Verschiedene Autoren haben betont, dass das Image oder die Reputation eines Anbieters eine starke Wirkung auf das Konsumenten- oder Nutzervertrauen im Netz entfaltet (Jarvenpaa et al., 2000; Walczuch & Lundgren, 2004; Eastlick et al., 2006; Milne & Boza, 1999). Zahlreiche Studien konnten in der Vergangenheit zeigen, dass die Marke eines Anbieters tatsächlich bei der Beurteilung der Vertrauenswürdigkeit eines Online-Anbieters eine wichtige Rolle spielt (Corbitt, Thanasankit & Yi, 2003; Ha & Perks, 2005; Jevons & Gabbott, 2000).

*„Und wo empfindet der Verbraucher Vertrauen? Das ist in der Tat bei bekannten Portalen, so wie bei uns, wo auch eine Marke dahinter steckt (...), wo eben auch der Ruf gut ist, gut sein muss.“ (A4\_05.03.2009)*

Marken können als ein Signal verstanden werden, welches dem Konsumenten funktionelle aber auch emotionale Eigenschaften eines Anbieters vermittelt (Gardner & Levy 1955). Marken bieten Anhaltspunkte für die Qualität der Produkte oder Dienstleistungen eines Unternehmens, schaffen Bekanntheit sowie Loyalität (Aaker, 1995; 2000). Auch im Internet sind Nutzer eher bereit, bekannten Marken ihr Vertrauen zu schenken (Urban, Sultan & Qualls, 2000).

*„(...) in der Finanzkrise, wo wir uns gerade jetzt befinden, ist das Thema Vertrauen und Sicherheit eines der Themen gewesen, und nach wie vor eines der wichtigsten Themen. (...) da ist die Marke definitiv eine grosse Grösse, die dort etwas ausstrahlt in das Thema Sicherheit, Vertrauen hinein.“ (A5\_20.03.2009)*

Factor 2	Loading	Extraction
i 2.1) Es handelt sich um einen bekannten Anbieter.	.808	.695
i 2.2) Der Anbieter hat bereits viele Kunden bzw. Nutzer.	.776	.677
i 2.3) Der Anbieter existiert schon eine Weile.	.768	.666
i 2.4) Die Seite des Anbieters ist einfach und übersichtlich gestaltet.	.744	.680
i 2.5) Der Anbieter ist führend in seinem Bereich.	.712	.612
i 2.6) Das Design des Anbieters wirkt seriös und professionell.	.708	.611
i 2.7) Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.	.707	.603
i 2.8) Ich fühle mich auf der Seite wohl.	.702	.611
i 2.9) Links sind gut kenntlich gemacht.	.694	.595
Cronbach's Alpha = 0.922		

*Tabelle 9: Faktorladungen Marke & Design*

Auch unsere Studie zeigt: Nutzer vertrauen gerne etablierten (i 2.3) und bekannten (i 2.1) Anbietern. Dies stellt selbstverständlich eine Herausforderung für jene Anbieter da, die sich erst noch auf dem Markt etablieren und in den Köpfen der Nutzer verankern müssen. Im Vertrauensmanagement gibt es also durchaus einen Alters- und Grössenvorteil.

*"Also im Prinzip ist der positive Verstärker tatsächlich der (...) Brand, das heisst die Kunden haben zur [Firma X] schon ein sehr grosses Vertrauen. Das haben wir auch im Rahmen von verschiedenen Marktforschungen noch mal bestätigt bekommen, dass der Kunde, wenn auf unserer Seite noch mal das Logo zu sehen ist (...), die Kunden das Gefühl haben, dass wir eben keine kleine Drittseite sind, die die Daten der Kunden eben nicht entsprechend schützt, sondern dass es hier auch eine gewisse Sensibilität gibt." (A3\_06.04.2009)*

*"Also, ich kaufe jetzt nichts bei irgendwelchen Seiten, die mir nichts sagen, das muss schon irgendeine bekannte Marke dann quasi sein." (N17\_16.03.2010)*

Doch nicht nur die Bekanntheit, auch der Erfolg macht im Internet attraktiv: Kunden orientieren sich gerne an Marktführern (i 2.5). Anbieter, die bereits zahlreiche Nutzer für sich gewinnen konnten (i 2.2), sind also deutlich im Vorteil, wenn es um die Erzeugung von Vertrauen geht (Luo & Cook, 2007-2008).

*"Das geht (...) mit einer gewissen Marktführerschaft, einer gewissen Grösse und auch einer gewissen Erfahrung einfach in Jahren los. Also, einem absolut neuen, kleinen, unbekanntem Internetanbieter, würde ich (...) in keiner Form vertrauen (...)." (A10\_09.03.2009)*

*"(...) was wir sagen wollen ist, wir sind seriös, wir sind gross, wir sind für unsere Zielgruppe da, wir sind erfolgreich, das sind die wesentlichen Elemente." (A12\_12.03.2009)*

*“Das heisst, es gibt einfach bestimmte Dienste, bei denen ich angemeldet bin, denen vertraue ich, weil es vielleicht auch einfach etablierte Dienste sind, die eine Nutzerbasis von Hunderttausend, Millionen Leuten haben, wo ich davon ausgehe, dass die sich das gar nicht leisten können, dann fehlerhaft mit meinen Daten umzugehen.” (N3\_03.03.2010)*

Auffällig an den Ergebnissen unserer Erhebung ist, dass Design, die Gestaltung einer Nutzeroberfläche eine zentrale Rolle bei der Beurteilung der Vertrauenswürdigkeit in diesem Kontext spielt. Ein einfacher, sauberer (i 2.4) sowie professionell gestalteter (i 2.6) Auftritt vermittelt Nutzern das Gefühl, einem seriösen Anbieter gegenüber zu stehen.

*“Ja, also wenn ich jetzt sehe, dass die Seite recht unprofessionell aufgebaut ist oder wenn ich sehe, dass da Schreibfehler drin sind, wenn ich sehe, dass da ganz verrückte Farben benutzt werden, also ganz hässliches Blau. [...] Also, so was, wo man wirklich sagt, das sieht aus, als wenn es jemand zu Hause am PC zusammengebastelt hätte, dann kann es vorkommen, dass ich Abstand nehme, dass ich dann denke, nein, das ist mir jetzt hier zu unseriös.” (N27\_26.04.2010)*

*“Das Erscheinungsbild der Seite ist entscheidend. Wenn man das erste Mal eine Seite besucht und sie macht keinen schlechten Eindruck, sondern transportiert Qualität und Seriosität, dann bleibt man eventuell.” (A19\_28.09.2009)*

Shneidermann (2000, S. 59) stellt fest: "good design can inspire trust". Die Qualität der Benutzeroberfläche bietet dem Nutzer massgebliche Hinweise zur Qualität des Angebots (Riegelsberger & Sasse, 2001). Online-Anbieter sollten vor allem Wert auf eine nutzerfreundliche und leistungsfähige Oberfläche legen, welche den Umgang und die Navigation erleichtert (Cheskin/Sapient, 1999). Dabei kann ein Wiedererkennungswert hilfreich sein: entspricht der Aufbau einer Seite einem verbreiteten und bekannten Standard, erkennt der Nutzer also gewisse Abläufe und Prozesse wieder, so wird dies eher vertrauenserweckend wirken (i 2.7). Nutzer haben inzwischen ein klares Verständnis dafür entwickelt, wie die Website eines Online-Händlers, eines sozialen Netzwerks oder einer Online-Bank auszusehen und zu funktionieren hat. Webseiten sollten daher etablierten Schemata folgen und vertraute Elemente und Prozesse integrieren. Auch hier sind etablierte Angebote wieder sichtbar gegenüber neuen im Vorteil. Ein Indikator für die Qualität der Website-Gestaltung ist schliesslich auch, dass die eingebauten Links sinnvoll sind und den Nutzer dorthin führen, wo er hinmöchte (i 2.9).

*“Das ist häufig im Unterhaltungselektronikbereich, da kommt man dann über 3 Suchmaschinen auf diese Seite, die man sonst nie gefunden hätte, und die ist dann also für mich so schlecht gemacht, dass ich von diesem schlechten Aufbau der Seite auch auf einen ansonsten schlechten Service schliesse.” (N15\_15.03.2010)*

*“Wenn wir an einen Dritten verlinken kann das [eine Störung] passieren und das ist sehr schädlich, genau. Das fällt negativ auf die eigene Marke.”(A2\_19.03.2009)*

Neben der Markenstärke spielt auch die Markensympathie eine Rolle. Ein seriös, angenehm und sympathisch wirkender Auftritt steigert das Vertrauen und senkt die Risikowahrnehmung. Nutzer interagieren freier und weniger zurückhaltend, wenn die Marke ihnen sympathisch ist (Bart et al., 2005). Wichtig ist letztlich für den Nutzer, dass er sich auf der Seite des Anbieters wohl fühlt (i 2.8).

*„Ich glaube, dass das Layout und inklusive ein Logo gewisse Befindlichkeiten mittransportieren, so mehr in die Richtung süß/sauer, also so diese Hauptgeschmacksrichtungen transportieren. Ist das jugendlich, ist das altbacken, ist das frisch, ist das nicht lesbar, ist das cool, ist das uncool, so in die Richtung, glaube ich, transportiert Layout sehr, sehr viel. (...) dort wo ich mich wohl fühle, dort wo ich mich aufgehoben fühle, wo es mir auch gefällt, bleibe ich auch gern und vice versa, dort, wo ich es ziemlich komisch finde, gehe ich nicht gerne hin. Also, das trifft definitiv auf Webseiten auch zu.“ (A5\_20.03.2009)*

## KUNDENSERVICE: AUSWAHL HILFT

Urban, Sultan and Qualls (2000) beschreiben den Vollzug, also die Abwicklung eines Online-Angebots als den wichtigsten Vertrauensfaktor. Der Dienst am Kunden, die Erfüllung des gegebenen Leistungsversprechens erhöht die Zuneigung des Kunden innerhalb wie ausserhalb des Internets. Online-Transaktionen basieren jedoch nicht auf der Etablierung zwischenmenschlicher Beziehungen, sondern stellen vielmehr medienvermittelte Austauschprozesse dar. Dies hat zur Folge, dass alle Informationen oder Hinweise bezüglich der Servicequalität eines Anbieters durch eine Website dargestellt werden muss (Culnan & Armstrong, 1999; Harris & Goode, 2004; Shankar, Smith & Rangaswamy, 2003; Yen & Gwinner, 2003; Yoon, 2002). Nicht zuletzt die Sozialen Medien bieten heute zahlreiche Ansätze und Instrumente für die kommunikative Einbindung der Nutzer und ihre pro-aktive Versorgung mit relevanten Informationen. Umgekehrt fällt es natürlich auch den Nutzern immer leichter, ihre Wünsche zu formulieren und gegenüber den Online-Anbietern einzufordern (Hart & Blackshaw, 2005).

*“(...) der Anspruch an das Einkaufen im Internet [ist] deutlich gestiegen (...), dass einfach da ein Service-Level erwartet wird, was so am Anfang natürlich nicht erwartet wurde.“ (A4\_05.03.2009)*

Unsere Studie bestätigt, dass Kundenservice eine bedeutende Rolle bei der Vertrauensbildung spielt. Auch online steht Anbietern eine Reihe von Möglichkeiten offen, die Qualität ihres Kundenservices zu signalisieren.

Factor 3	Loading	Extraction
i 3.1) Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, eMail, Adresse).	.738	.717
i 3.2) Der Kundenservice des Anbieters ist freundlich.	.726	.712
i 3.3) Der Kundendienst ist einfach erreichbar.	.701	.683
i 3.4) Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.	.686	.640
i 3.5) Die Kontaktdaten des Anbieters sind einfach zu finden (z.B. Adresse, Telefonnummer).	.666	.676
i 3.6) Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.	.643	.521
Cronbach's Alpha = 0.896		

*Tabelle 10: Faktorladungen Kundenservice*

In einiger Hinsicht unterscheiden sich die Service-Anforderungen gegenüber einem Online-Angebot nicht von jenen eines Offline-Anbieters. Qualitätskriterien sind hier die Erreichbarkeit des Anbieters (i 3.3), die Reaktionszeit bei Fragen oder Bestellungen (i 3.4) ebenso wie ein hilfreicher und freundlicher Service (i 3.2) (McAllister, 1995; Fang & Salvendy, 2003).

*“Man kann sich an uns wenden, wenn man eine Frage hat, dann gewährleisten wir, dass unser Kundenservice innerhalb von 24 Stunden auch antwortet.” (A8\_23.03.2009)*

*“(…) was ebenfalls absolut zur Vertrauensbildung beiträgt, ist schnelle Antworten auf Emails, da bin ich überzeugt von. (…) manchmal auch über Weihnachten zum Beispiel die Erfahrung, dass wir die Emails der Kunden eben nicht so schnell und so rasch abarbeiten können, wie wir es gerne wollen. Das ist ein ganz, ganz wichtiger Faktor, die Kommunikation mit dem Kunden, wenn die rasch und reibungslos funktioniert, der Kunde auf eine Anfrage sofort eine Antwort bekommt, ist das ein ganz hoher vertrauensstärkender Faktor.” (A7\_04.03.2009)*

Hinzu kommen mögliche Angaben auf einer Website, die einen hochwertigen Kundenservice signalisieren, ohne dass dieser tatsächlich in Anspruch genommen werden muss. Hierzu zählt die Angabe verschiedener Wege oder Möglichkeiten der Kontaktaufnahme (i 3.1) - wie etwa eMail, Telefon, Post, Foren, etc. - und die einfache Auffindbarkeit der Kontaktdaten (i 3.5).

*“Ich gucke eigentlich immer prinzipiell genau, ob es eine Kontaktadresse gibt und solche Sachen und Impressum, wenn es das nicht auf der Seite gibt, würde ich nicht bestellen.” (N12\_08.03.2010)*

*"Ganz, ganz wichtig ist natürlich die ganze Impressumsgeschichte, diese Geschichte, die ja auch gesetzlich vorgeschrieben ist. (...) ich muss den Anbieter als juristische oder natürliche Person identifizieren können mit allen Angaben, die es mir erlauben, dort Kontakt aufzunehmen."* (A7\_04.03.2009)

Nicht zuletzt wird es als ein Qualitätssignal empfunden, wenn ein Anbieter unterschiedliche Zahlungsmethoden zur Verfügung stellt (i 3.6). Üblich sind hier etwa Kreditkartenzahlungen, Bankeinzug, weitere Online-Bezahlservices oder die klassische Rechnungsstellung.

*"(...) mit einem gut gemachten Seitenauftritt, mit Möglichkeit zum Beispiel auch sichere Zahlungsdienste zu verwenden, oder eben Vorkasse auszuschliessen usw., da gibt es natürlich noch diverse Möglichkeiten, Vertrauen einzuflößen."* (A4\_05.03.2009)

## **NUTZERKONTROLLE: ANGST VOR DRITTPARTEIEN**

Haben sich Nutzer einmal entschieden, persönliche Daten in eine Transaktion einzubringen, geben sie damit jedoch subjektiv keineswegs die Kontrolle über diese auf. Nutzer betrachten persönliche Daten letztlich als eine Art Eigentum - dieses wird durch die Teilnahme an einem Online-Austausch nicht völlig abgetreten (Phelps et al., 2000; Olivero & Lunt, 2004). Nutzer erwarten, dass die angegebenen Daten nicht über den von ihnen beabsichtigten Zweck hinaus verwendet werden (Culnan & Armstrong, 1999). Denn die Kehrseite des Nutzervertrauens sind deren Ängste und Sorgen. Je höher das wahrgenommene Risiko einer Transaktion, desto geringer ist deren Vollzugswahrscheinlichkeit. Die Vollzugswahrscheinlichkeit einer Transaktion kann also gesteigert werden, wenn die Risikowahrnehmung der Nutzer gesenkt wird, indem diese etwa die Kontrolle über die zur Verfügung gestellten Daten behalten (Milne & Boza, 1999; Culnan & Armstrong, 1999; Chellappa & Sin, 2005).

Sheehan und Hoy (2000) unterscheiden zwei Dimensionen der Nutzerkontrolle: "Awareness of information collection" bezieht sich auf die Frage, ob dem Nutzer die Sammlung seiner Daten überhaupt bewusst ist, "information usage" bezeichnet dagegen die Kenntnis der Verwendungsarten der gesammelten Informationen. Zahlreiche Autoren weisen darauf hin, dass ein subjektives Kontrollempfinden vertrauensfördernd wirkt (vgl. u.a. Nowak & Phelps, 1995; Hoffman & Novak, 2009; Urban et al., 2009).

Factor 4	Loading	Extraction
i 4.1) Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	.728	.668
i 4.2) Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	.722	.638
i 4.3) Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	.681	.607
i 4.4) Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	.663	.575
i 4.5) Der Anbieter teilt mir mit, auf welche Art er meine Daten ausgewertet/analysiert.	.660	.635
i 4.6) Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	.651	.597
i 4.7) Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	.565	.541
Cronbach's Alpha = 0.887		

**Tabelle 11:** Faktorladungen Nutzerkontrolle

Auch unsere Studie bestätigt, dass Nutzer wissen möchten, welche ihrer Daten gesammelt und gespeichert werden (i 4.7). Sie interessieren sich dafür, auf welche Weise ihre Daten durch den Anbieter analysiert, beziehungsweise ausgewertet werden (i 4.5).

*"(...) in den letzten Jahren oder Monaten ist das Thema Datenschutz sehr, sehr zu einem wichtigen Thema geworden, vor allem durch die Mediendiskussion und durch einige Datenschutzskandale, die wir halt hatten."* (A10\_09.03.2009)

*"Ich denke, das Einkaufen wird sicher dahingehend missbraucht, dass meine Daten irgendwie gespeichert werden und die schauen, was ich einkaufe und mir dann dementsprechend [Empfehlungen geben], oder das vielleicht weitergeben an andere Firmen, die sich bei mir melden."* (N16\_16.03.2010)

Von zentraler Bedeutung für die wahrgenommene Kontrolle der Nutzer über ihre persönlichen Daten ist der Umgang mit der möglichen Weitergabe dieser Daten an dritte Parteien. Mag ein Nutzer auch Vertrauen zu einem Anbieter gefasst haben, so gilt dies nicht automatisch auch für dessen Kooperationspartner. Nutzer möchten daher informiert werden, wenn ihre Daten an Dritte weitergegeben werden (i 4.1), oder möchte in diesem Fall gar um Zustimmung gebeten werden (i 4.2). In gewissen Fällen möchten Nutzer eine Zusicherung erhalten, dass ihre persönlichen Daten gar nicht an dritte Parteien weitergegeben werden (i 4.6).

*"Sie müssen dem Kunden ja jederzeit sagen können, was mit seinen Daten passiert, Sie müssen ihm Auskunft darüber geben, Sie müssen seine Daten löschen, wenn er das gerne möchte."*

*Hier sichert man dem Kunden ja auch zu, dass wir seine Adressdaten nicht weitergeben an Dritte.“ (A7\_04.03.2009)*

*“Also, dann hat mir ein Freund gesagt, dass die die AGB geändert haben, dass sie alle Daten weitergeben können, deshalb hat er sich abgemeldet und deshalb sage ich, melde ich mich auch bald ab.“ (N37\_27.04.10)*

Eine sinnvolle Alternative kann es sein, den Nutzer selbst entscheiden zu lassen, mit welchen dritten Parteien seine persönlichen Daten geteilt werden können (i 4.3). Anbieter sollten sich demnach darum bemühen, ihren Transaktionspartnern Möglichkeiten der selektiven Freigabe und Kontrolle persönlicher Daten einzurichten (Schoenbachler & Gordon, 2002). Ein häufig genanntes Beispiel ist das Angebot von Opt-in-Funktionen, anstelle von reinen Opt-out-Möglichkeiten.

*“(…) wenn Sie mich jetzt über die Plattform kontaktieren, dann entscheide ich selber, (…) ob ich Sie quasi in mein Netzwerk nehme, ob ich die Einladung annehme, und dann kann ich selber sehr individuell bestimmen, welche Daten ich freigebe.“ (A8\_23.03.2008)*

*“Und deswegen bin ich momentan so, dass ich sage, solange das ein geschlossener Raum ist und man genau weiss, wer da mit drin ist, ist das okay, aber sowie die Möglichkeit besteht, dass irgendjemand sich dazu schalten kann und behauptet, ich bin dein 14-jähriger Freund oder so was, dann mache ich da nicht mehr mit. Das erlaube ich dann nicht und mache ich selber auch nicht, nur geschlossene Räume, nicht offene.“ (N6\_04.03.2010)*

Faire Informationspraktiken sollten den Sorgen der Nutzer entgegenwirken und ihre Risikowahrnehmung adressieren (Milne & Rohm, 2000). Eine Angabe von Daten, die über das für das Angebot notwendige Minimum hinausgehen, sollte stets freiwillig geschehen (i 4.4).

*“(…) in der Regel werden die Sachen freiwillig eingestellt, das heisst, natürlich wissen die Nutzer, dass andere das lesen können, und da ist es natürlich ganz wichtig, dass man Aufklärung betreibt, gerade bei Jugendlichen, damit die genau wissen, was sie damit auch anrichten können.“ (A4\_05.03.2009)*

*“Bei der Adresse leuchtet mir ein, dass die die halt brauchen, weil, wenn ich was bestelle, müssen sie es mir ja zukommen lassen, aber eine Telefon-Nummer [...] da bin ich immer so ein bisschen am Überlegen, ob da nicht dieser Fakt dann verkauft wird und man irgendwann wieder von einem Institut angerufen wird.“ (N27\_26.04.2010)*

Einige Forscher haben darauf hingewiesen, dass eine pro-aktive Kommunikationspolitik hinsichtlich der Verwendung und Weitergabe persönlicher Daten im Rahmen der Vertrauensbildung auch kontraproduktiv wirken kann, indem sie die Aufmerksamkeit auf potentielle Problemfelder lenkt und so die Risikowahrnehmung steigert (Milne & Boza, 1999; Sheehan & Hoy, 1999). Milne und Boza (1999, S. 9) unterscheiden daher zwischen offensi-

ven und defensiven Strategien des Vertrauensmanagements: "In a concern-reduction strategy, communication is secretive, in an attempt to avoid consumers' aversive responses. In this strategy, the optimal outcome is to avoid losing sales due to privacy concerns. In contrast, in a trust-building strategy, communication is informative and benefit driven, aimed at developing customer relationships." Vertrauensmanagement durch Kommunikation ist somit keine "One size fits all"-Aufgabe - verschiedene Anspruchsgruppen haben unterschiedliche Ansprüche und Interessen in Bezug auf die Vertrauenswürdigkeit eines Anbieters (Shankar, Urban & Sultan, 2002).

## THIRD PARTY ENDORSEMENTS: FREUNDE UND GOOGLE

Unter einem "Third Party Endorsement" wird eine unabhängige Stellungnahme einer dritten Partei - meist eines Experten - bezüglich der Qualität eines Angebots verstanden. Eine solche Beurteilung kann die Form eines Gütesiegels oder einer Auszeichnung annehmen. Es existieren zahlreiche Ansätze, die Vertrauenswürdigkeit eines Online-Angebots durch dritte Parteien beurteilen zu lassen (Wakefield & Whitten, 2006). Derartige Urteile ermöglichen Nutzern die Einschätzung eines Transaktionspartners durch wenige Blicke (Urban et al., 2000; Wang et al., 2004).

*"(...) bei jeder Form von Service oder Produktangebot gegenüber Kunden, bedienen sich ja eigentlich fast alle bis zu einem gewissen Grade Third Party Endorsements. (...) Also, das wird wahrgenommen, das wird auch ernst genommen, und das sind bis zu einem gewissen Grade, glaube ich, auch so Leuchttürme in der Unsicherheit, auf was man vertrauen kann." (A10\_09.03.2009)*

*"Und da hilft natürlich so ein Siegel (...), die schwarzen von den weissen Schafen vielleicht zu unterscheiden." (A9\_26.03.2009)*

*"Genau oder eben, es gibt ja mittlerweile auch schon so Zertifikate, so wie ein Trusted eShop oder so." (N15\_15.03.2010)*

Nach Cook und Luo (2003) wirken Third Party Endorsements wie ein Vermittler zwischen konkurrierenden Online-Anbietern und nervösen Online-Kunden. Da Online-Transaktionen meist keine Auseinandersetzung von Angesicht zu Angesicht ermöglichen, können die Aussagen dritter Parteien eine kritische Informationslücke schliessen (Corbitt et al., 2003; Kovar et al., 2000; Luo & Cook, 2007-2008; Shneiderman, 2000; Luo, 2002; Zucker, 1986; Luo & Cook, 2007-2008). Tatsächlich existieren heute vielfältige professionell vergebene Siegel, wie etwa jene der Stiftung Warentest, TRUSTe, VeriSign or Consumer Report (Cook & Luo, 2003; Krishnamurthy, 2001; McKnight, Choudhury & Kacmar, 2000; Palmer, Bailey & Faraj, 2000 - s. Abb. 15). Diese basieren in der Regel auf einer Art Test des Angebots, in manchen Fällen auch nur auf der Zusage gewisser Qualitätsstandards durch den

Anbieter. Mehrere Studien weisen nach, dass Programme von Drittparteien das Konsumentenvertrauen und ihre Kaufabsichten tatsächlich beeinflussen können (Luo & Cook, 2007-2008; Palmer et al., 2000; Wakefield & Whitten, 2006).

Factor 5	Loading	Extraction
i 5.1) Der Anbieter wird bei Suchmaschinen (z.B. Google) als eine der ersten Seiten aufgelistet.	.607	.520
i 5.2) Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.	.517	.589
i 5.3) Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z.B. Stiftung Warentest).	.494	.581
i 5.4) Der Anbieter wird von anderen Nutzern positiv eingeschätzt (Ratings)	.449	.529
Cronbach's Alpha = 0.765		

*Tabelle 12: Faktorladungen Third Party Endorsement*

Unsere Studie bestätigt, dass Nutzer auf professionell vergeben Gütesiegel (i 5.3) ebenso achten, wie auf Preise und ähnliche Auszeichnungen (i 5.2). Zahlreiche Anbieter bemühen sich um derartige Qualitätssignale. Die prominente Platzierung solcher Drittparteikennzeichen auf der Website sowie deren aktive Integration in die Kommunikationsaktivitäten der Anbieter, sind inzwischen gängige Geschäftspraxis (Eastlick et al., 2006; Ashworth & Free, 2006).

*"(...) wir nehmen aktiv an so Bewertungsritualen teil, die es in der Bankenwelt gibt. Das ist jetzt nicht die Stiftung Warentest, aber (...) 'Beste Bank' beispielsweise, oder aktuell läuft gerade die Brokerwahl von Börse Online usw., oder Börse Online Umfragen. Das nehmen wir sehr ernst und wenn wir dort etwas gewinnen, was sinnvoll ist, dann verwenden wir das auch aktiv." (A5\_20.03.2009)*

*"Unsere Kunden interessiert es, unsere Partner, jeder, der mit uns zusammen arbeitet (...) interessiert das [dass unsere Homepage zertifiziert ist]." (A9\_26.03.2009)*

Die Wirkung professioneller Siegel hängt offensichtlich von der Vertrauenswürdigkeit ihrer Anbieter ab (Luo & Cook, 2007-2008). Nicht selten erzeugen sie daher erhebliche Kosten. Immer mehr Anbieter verlassen sich darum auf die Urteile, Ratings, Kommentare und Berichte ihrer Nutzer (Pennington, Wilcox & Grover, 2003).

*"(...) je mehr dieser Siegel auch auf dem Markt sind, (...) wird es bald zum Standard und man rechnet eigentlich gar nicht mehr damit. Ich glaube, dass es überschätzt wird. Wir haben keinen dramatischen Einfluss nach der Siegeleinführung bei uns gespürt." (A2\_19.03.2009)*

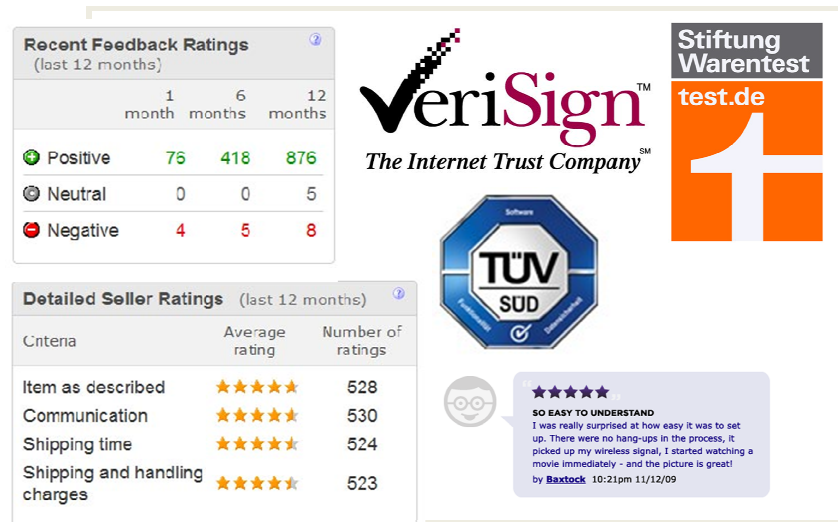


Abbildung 15: Mögliche Third Party Endorsements

Gemäss Pavlou (2002) erzeugt Mund-zu-Mund-Propaganda einen komparativen Vorteil durch Wohlwollen und Glaubwürdigkeit. Friedman et al. (2000) betonen: "People trust people, not technology". Nutzer achten demnach auf die Beurteilung eines Angebots durch andere Nutzer (i 5.4).

*"Bei uns aber mindestens genau so wichtig ist die Empfehlung über die Nutzer selbst. Ich hatte einen Bekannten, einen Freund, der war schon da, oder meine Tochter oder mein Sohn hat gesagt ich soll doch mal... das ist relevant." (A12\_12.03.2009)*

*"Und eigentlich ist es am besten, wenn man so was hört von Bekannten, von Freunden, die sagen, das ist am besten, oder wenn gerade so was wie Stiftung Warentest es mal richtig durchcheckt." (N37\_27.04.10)*

*"Ja, ich gebe da auch Bewertungen ab. Ich finde das wichtig, (...) da weiss dann der Nächste, ob er sich darauf verlassen kann oder nicht." (N31\_27.04.10)*

Ein besonders interessantes Ergebnis unserer Analyse ist die Feststellung, dass Online-Suchmaschinen zunehmend die Funktion eines Third Party Endorsements übernehmen (i 5.1). Erscheint also ein Angebot besonders weit oben unter den Suchresultaten, so signalisiert das, dass es sich um einen bekannten, etablierten Anbieter handelt. Nicht zuletzt kann dies auch ein Hinweis darauf sein, dass zahlreiche andere Nutzer diesen Dienst in Anspruch nehmen. Die Optimierung solcher Suchmaschinenresultate ist daher heute eine Standard-Massnahme des Online-Marketing.

## REALWELTBEZUG: AUCH BILDER WIRKEN

Nach Jarvenpaa und Tractinsky (1999) spielt die Existenz physischer Geschäftsräume eine vermittelnde Rolle bei der Entstehung von Vertrauen zwischen Nutzer und Anbieter. Olivero und Lunt (2004) stellen fest, dass Anbieter, die off-line als etabliert betrachtet werden können, auch online als "realer" empfunden werden. Umgekehrt wirken Anbieter, die nur schwierig aufzusuchen sind, weniger zuverlässig (Friedman et al., 2000). Der off-line Auftritt eines Anbieters vermag einem Nutzer zahlreiche Hinweise und Signale hinsichtlich seiner Vertrauenswürdigkeit zu vermitteln, die online nur schwierig zu replizieren sind. Reine Online-Angebote sind daher mit einem gewissen Nachteil behaftet (Nissenbaum, 2001; Zimmer, 2010).

*"Also, wenn man natürlich in der Form nicht anfassbar ist, weder von der Filiale - und noch viel stärker wäre das natürlich der Fall über ein Produkt, das man in der Hand halten kann -, dann ist man bis zu einem gewissen Grade abstrakt und könnte ja auch am nächsten Tag eigentlich nicht mehr da sein, abgeschaltet sein." (A10\_09.03.2009)*

Factor 6	Loading	Extraction
i 6.1) Der Anbieter besitzt Filialen, die ich aufsuchen kann.	.797	.723
i 6.2) Ich kenne das Unternehmen auch ausserhalb des Internets.	.797	.719
i 6.3) Die Büros des Anbieters werden auf einem Foto gezeigt.	.696	.655
i 6.4) Informationen über den Anbieter sind einfach zu finden (z.B. Grösse, Mitarbeiter, Geschichte).	.522	.565
Cronbach's Alpha = 0.813		

**Tabelle 13:** Faktorladungen Realweltbezug

Unsere Studie bestätigt, dass die Präsenz oder Bekanntheit eines Anbieters ausserhalb des Internets vertrauenssteigernd wirkt (i 6.2). Insbesondere Filialen spielen hier eine Rolle (i 6.1), in denen ein Nutzer unmittelbar mit seinem Gegenüber interagieren, Produkte testen, anprobieren oder für eine Reparatur vorbeibringen kann.

*"Das ist ganz wichtig, aber eben auch der Punkt Vertrauen, das heisst man hat das Gefühl, da ist jemand, dem man vertrauen kann, das heisst, man kann, wenn man ein Problem hat sich an jemanden wenden." (A4\_05.03.2009)*

Auch reine Online-Anbieter können jedoch Vertrauen dadurch erzeugen, dass sie einen "Realweltbezug" in ihren Web-Auftritt integrieren. Nutzer achten auf die einfache Auffindbarkeit von Informationen zum Anbieter, wie etwa dessen Sitz, Grösse, Geschichte, etc. (i 6.4). Derartige Informationen machen ein Unternehmen "greifbarer" (Jarvenpaa & Tractinsky, 1999).

*"Wir sind ja auch ein reales Unternehmen (...), haben unsere 200 Mitarbeiter. (...) Das heisst, man muss natürlich permanent zeigen, dass wenn man eine Community managt, dass man dies auch aktiv tut, aber das tun wir im Tagesgeschäft, (...) also unsere Mitglieder nehmen uns wahr auf der Plattform." (A8\_23.03.2009)*

*"Das ist ganz wichtig, das heisst man hat das Gefühl, da ist jemand, dem man vertrauen kann, das heisst, man kann, wenn man ein Problem hat, sich an jemanden wenden." (A4\_05.03.2009)*

Eine weitere Möglichkeit, einen Realweltbezug herzustellen, ist die Abbildung von Fotos - etwa der physischen Büros oder Mitarbeiter. Derartige Fotos dokumentieren die physische Präsenz eines Anbieters, welche vertrauensfördernd wirkt.

*"Es ist wichtig, dass man sich zeigt, dass man auf Messen auftaucht, dass die Leute wissen, wer hinter der Seite steht, dass man Fotos aufschaltet; dass man die Firma gut sichtbar macht. Auch Adressangaben sind wichtig, damit die User bei der Firma vorbeigehen könnten, falls sie dies wollen. Also auch physische Präsenz zeigen." (A14\_01.09.2009)*

## TECHNISCHE ZUVERLÄSSIGKEIT: EIN HYGIENEFAKTOR

Wir hatten gesehen, dass auch das Vertrauen in das Medium Internet als solches einen Einfluss auf die Bereitschaft eines Nutzers entfaltet, persönliche Daten online zur Verfügung zu stellen (Lee & Turban, 2001). Es ist jedoch festzustellen, dass Nutzer in der Regel die technischen Architekturen und Prozesse des Internets nicht wirklich verstehen - was wiederum die Bedeutung des Faktors Vertrauen erhöht (Johnson, 2007). Die technische Zuverlässigkeit einer Transaktionsplattform mag schwierig einzuschätzen sein, dennoch wird sie von Seiten der Nutzer erwartet. Wie Corbitt et al. (2003, S. 205) feststellen: "The appearances, the functionality and the service quality performed by an electronic storefront are a direct result of the technical design."

*"Anfangs war es durchaus so, dass die (...) Seite mal auch tageweise nicht ging, absolute Katastrophe! Das ist zum Glück Geschichte, also was das betrifft, kann man doch sagen, dass technisch der Marktplatz einwandfrei funktioniert." (A4\_05.03.2009)*

Als zuverlässig kann eine Website dann betrachtet werden, wenn es nicht zu technischen Fehlern (i 7.2) oder Abstürzen (i 7.1) kommt. Die Abwesenheit von Fehlern wird in der Literatur als ein zentraler Treiber des Nutzervertrauens beschrieben (Bart et al., 2005; Hoffman, Novak & Peralta, 1999a; Johnson, 2007).

*"Also, vor allen Dingen natürlich auch wie der Kauf oder der Bestellvorgang abläuft, funktioniert. Funktioniert da alles? Werde ich irgendwo ins Nirwana gelenkt; zum Beispiel? Das sind natürlich so Sachen, da verlieren Sie das Vertrauen der Verbraucher sofort." (A7\_04.03.2009)*

Factor 7	Loading	Extraction
i 7.1) Die Seite des Anbieters stürzt nicht ab.	.531	.625
i 7.2) Es kommt nicht zu technischen Fehlern.	.510	.585
i 7.3) Der Anbieter bietet mir genau was ich suche.	.509	.547
i 7.4) Die Seite lädt schnell.	.497	.574
i 7.5) Ich empfinde die abgefragten Seiten nicht als heikel oder zu persönlich.	.455	.541
Cronbach's Alpha = 0.748		

**Tabelle 14:** Faktorladungen Technische Zuverlässigkeit

Selbst kleinere Störungen, wie Tippfehler auf einer Homepage, wurden schon als negative Einflüsse auf das Vertrauen der Nutzer identifiziert (Nielsen, 1999; Fang & Salvendy, 2003). Letztlich erwarten die Nutzer vor allem, dass eine Seite schnell und reibungslos funktioniert (i 7.4) und die Funktion erfüllt, die der Nutzer erwartet (i 7.3). Lee und Turban (2001) beschreiben daher die technische Zuverlässigkeit eines Systems, als dessen Fähigkeit, jene Aufgaben zu erfüllen, die es erfüllen soll.

*“Also, vor allen Dingen natürlich auch wie der Kauf oder der Bestellvorgang abläuft, funktioniert. Funktioniert da alles?” (A7\_04.03.2009)*

Dabei sollte jedoch auch bedacht werden, dass sich Vertrauen im Laufe der Zeit bildet - so wichtig ein erster Eindruck ist, so bedeutsam ist auch die beständige Pflege einer vertrauensvollen Beziehung durch Gewährleistung befriedigender Transaktionserfahrungen. Umgekehrt gilt: es gibt keine zweite Chance, einen ersten Eindruck zu vermitteln. Je vertrauter ein Nutzer mit einem Angebot ist, desto eher ist er gewillt, auch einmal eine technische Störung zu verzeihen. Technische Zuverlässigkeit erhöht also die Vertrautheit und damit auch indirekt das Nutzervertrauen (Bhatnagar et al., 2000; Gefen, 2000; Sheehan & Hoy, 2000). Erneut eine Herausforderung insbesondere für jüngere, wenig etablierte Angebote.

*“Ja, also bei Kreditkarten ist es ja, hat man immer ein bisschen ein komisches Gefühl, aber ich glaube mittlerweile ist die Technik so weit, dass ich dem jetzt vertraue.” (N13\_09.03.2010)*

## ZUSAMMENFASSUNG

Die hier vorgestellte Studie bietet einen umfassenden Überblick über Einflussfaktoren des Nutzervertrauens im Internet auf der Ebene der Webpräsenz eines Anbieters. Sie bestätigt, dass Nutzer ihre persönlichen Daten als ein wertvolles Gut betrachten, welches selektiv in Austauschprozesse eingebracht wird. Damit ein Online-Angebot auf Akzeptanz stößt, muss es daher einen Nutzen bieten, welches das Risiko, das mit der Bereitstellung persön-

licher Daten unvermeidlich verbunden ist, überwiegt. Dieser Faktor übersteigt in seiner Bedeutung alle weiteren hier identifizierten. Es ist somit dringend notwendig zu verstehen, dass der Wunsch nach Sicherheit oder Privatheit stets in Relation zu diesen Bedürfnissen entgegen wirkenden Wünschen zu betrachten ist. Nicht totale Sicherheit schafft Vertrauen, sondern ein angemessenes Geben und Nehmen im Austausch zwischen Nutzern und Anbietern. Online-Angebote sollten daher nicht nur ihre Standards in Hinblick auf Sicherheit und Datenschutz kommunizieren, sondern vor allem auch die Qualität des gebotenen Nutzens.

Ein guter Kundenservice steigert offensichtlich die Qualität eines Angebots. Online-Anbieter sollten sich daher bemühen, nicht nur einen schnellen, freundlichen und zuverlässigen Kundendienst zu bieten, sondern ihr Serviceniveau auch auf der Website zu signalisieren - etwa durch ein breites Angebot an Kontakt- oder Bezahloptionen. Auch die Möglichkeit, nach Eintritt auf eine Transaktion noch die Kontrolle über die Verarbeitung und Verbreitung persönlicher Daten zu behalten, steigert die Nutzungsbereitschaft. Nur weil ein Nutzer einmal auf ein Angebot eingetreten ist, bedeutet dies nicht, dass er die Kontrolle über die angegebenen Daten völlig aufgeben möchte. Insbesondere die Weitergabe von Daten an dritte Parteien wird als sensibel empfunden und kritisch beäugt.

Neben der Abwägung von Nutzen, Service, Risiko und Kontrolle orientieren sich Internetnutzer bei der Beurteilung eines Angebots an spezifischen Signalen seiner Vertrauenswürdigkeit. Das bedeutendste darunter ist eine bekannte, etablierte Marke. Dies stellt offensichtlich eine Herausforderung für junge, wenig verbreitete Angebote dar. Eine breite Nutzerbasis und ein seriöses, vertrautes Design signalisieren die Vertrauenswürdigkeit eines Anbieters ebenso, wie dessen positive Beurteilung durch Dritte. Dabei können neben professionellen Siegeln oder Preisen insbesondere auch die Wertungen und Kommentare anderer Nutzer hilfreich sein, wie auch die prominente Platzierung eines Angebots unter Suchmaschinenresultaten.

Wir konnten feststellen, dass Angebote, welche auch ausserhalb des Internets genutzt oder kontaktiert werden können, einen Vertrauensvorschuss geniessen. Reine Online-Angebote können versuchen, dies zu kompensieren, indem ihre realweltliche Existenz durch Bilddokumentationen oder die Angabe von Daten und Kontaktinformationen signalisiert wird. Wenngleich dieser Faktor in unserer Analyse schwierig zu extrahieren und mit Vertrauen zu korrelieren war, ergibt sich aus der Untersuchung ebenso wie aus der Literatur, dass die technische Zuverlässigkeit eines Angebots eine Art Hygienefaktor darstellt, also vorausgesetzt wird. Fehler, Abstürze oder die mangelnde Fähigkeit einer Plattform, ihren Zweck zu erfüllen, wirken vor allem in frühen Phasen einer Transaktionsbeziehung vertrauenszerstörend.

Einschränkend ist zu wiederholen, dass persönliche Eigenschaften der Nutzer ebenso einen Einfluss auf die Vertrauensbildung entfalten, wie institutionelle Rahmenbedingungen. Je

nach Land und Branche können daher verschiedene Vertrauensfaktoren unterschiedlich förderlich wirken. Die hier präsentierte Analyse bezieht sich insbesondere auf den deutschen Markt und beinhaltet Implikationen für solche Länder mit ähnlichen Rahmenbedingungen und Nutzertypologien. Die Bedeutung der beschriebenen Faktoren kann zudem variieren, je nach Reife einer Transaktionsbeziehung. Hat ein Nutzer bereits positive Erfahrungen mit einem Anbieter gesammelt, so verlieren gewisse Indikatoren oder Signale, wie etwa Siegel oder die Markenstärke, an Bedeutung, während andere, wie beispielsweise der Kundenservice, tendenziell an Einfluss gewinnen. Die Implikationen der beschriebenen Resultate für ein zeitgemäßes Online-Identitätsmanagement werden nun noch abschließend im folgenden Kapitel herausgearbeitet.

## V. IMPLIKATIONEN FÜR DAS IDENTITÄTSMANAGEMENT

Die in dieser Studie identifizierten Einflussfaktoren des Nutzervertrauens beinhalten Implikationen für eine Vielzahl von Transaktionskontexten. Sie können privaten Anbietern von Online-Anwendungen ebenso nützliche Hinweise bieten, wie öffentlichen - denn beide haben gleichermaßen das Vertrauen und die Akzeptanz der Nutzer zu gewinnen, wenn sie ihr Angebot erfolgreich positionieren wollen. Zahlreiche Angebote der öffentlichen Hand sind aktuell darum bemüht, eine hilfreiche und sichere Infrastruktur für die Abwicklung von privaten Geschäftsmodellen zu etablieren. Die elektronische Signatur, De-Mail (verbunden mit Ident und Safe) sowie insbesondere der neue Personalausweis mit seiner eID-Funktionalität sind Beispiele für solche Initiativen. Wenngleich sie vor allem dem Schutz der Sicherheit und Privatsphäre der Bürger im Netz dienen sollen, stossen sie dennoch ihrerseits immer wieder auch auf Skepsis und Sorgen unter den Nutzern. Was also, wenn öffentliche Angebote des elektronischen Identitätsmanagements das Vertrauen der Nutzer gewinnen müssen? Die identifizierten Vertrauensfaktoren bieten auch für diesen Fall Anhaltspunkte - hier beschrieben und illustriert mit Aussagen der Interviewteilnehmer dezidiert zur Frage des elektronischen Identitätsmanagements:

### REZIPROZITÄT

Nutzer sind bereit, persönliche Daten in eine Transaktion einzubringen, wenn sie im Austausch einen Nutzengewinn erwarten können, dessen Attraktivität das mit der Transaktion verbundene Risiko übersteigt. Um aber Risiko und Nutzen abschätzen zu können, müssen diese zuerst verstanden werden. Angebote des Identitätsmanagements erfordern selbstverständlich die Bereitstellung persönlicher Daten, da sie nicht zuletzt deren Schutz dienen sollen. Doch ist dem Nutzer wirklich bewusst, welche Daten in welchem Umfang und zu welchem Zweck der entsprechenden Applikation überlassen werden? Insbesondere neue Applikationen sollten hier nicht von einem Vertrauensvorschuss ausgehen, nur weil sie durch die öffentliche Hand bereitgestellt oder unterstützt werden. Auch sie haben dem Nutzer transparent und verständlich darzulegen, welche Rechte und Verpflichtungen mit der Nutzung der Applikation verbunden sind, und auf welche Weise die neue Anwendung Sicherheit und Privatsphäre der Nutzer auch vor Zugriffen des Betreibers und seiner Kooperationspartner schützt.

*"Ich finde das toll, wenn es so was gibt, aber ich glaube, da müsste man vorher sehr genau erklären, wie das Sicherheitssystem funktioniert, weil ich mir das nicht vorstellen kann."*  
(N1\_23.02.2010)

Wichtiger ist jedoch möglicherweise ein weiterer Punkt: das Risiko einer Transaktion wird stets in Relation zu ihrem Nutzen abgewogen. Welcher Nutzen ist jedoch mit einer Anwendung des Identitätsmanagements verbunden? Wenn der primäre Nutzen im Schutz von Sicherheit und Privatheit liegen soll, die Applikation jedoch ihrerseits Sorgen hinsichtlich dieser Bereiche auslöst, ist ein Nutzen nur schwer zu vermitteln.

*„Und ich muss ja nicht besonders oft irgendwelche Verträge abschliessen oder irgendwo meine Unterschrift leisten für wichtige Dokumente, und das sind so seltene Sachen, dass ich das gut auf Papier machen kann.“ (N20\_11.03.2010)*

*„Gut, das mache ich ja jetzt auch schon, also, einkaufen halt. Aber da sehe ich das Risiko jetzt nicht so gross. Ich meine selbst, wenn es passieren sollte, dass jemand meine Kreditkartendaten hat und damit was macht, dann habe ich ja immer noch die Möglichkeit am Ende des Monats auf meine Abrechnung zu schauen und zu sagen, Moment, das habe ich nicht gekauft, aber dann muss ich es ja auch nicht zahlen.“ (N10\_05.03.2010)*

*„Ich könnte mir vorstellen, dass es vielleicht sogar überflüssig ist, weil, ich meine, PayPal bietet ja quasi auch schon diese Sicherheit an, dass man sieht, dass einem garantiert wird, dass derjenige das überwiesen hat.“ (N11\_08.03.2010)*

Wird die Anwendung hingegen als eine Infrastruktur verstanden, die zahlreiche weitere Transaktionen im Netz ermöglicht - vom Shopping, Banking, Dating bis Networking - dann potenziert sich das Nutzenvolumen, welches in die Kalkulation einfließt. Anbieter sollten also möglicherweise nicht das Angebot des Identitätsmanagements als Applikation bewerben, sondern den Zugang zu zahllosen weiteren Angeboten, der so ermöglicht wird. Der Vorteil eines sicheren Zugangs zu den reichhaltigen kommerziellen Angeboten des Internets ist sehr viel leichter zu vermitteln, als der Vorteil eines neuen Personalausweises oder weiteren eMail-Accounts.

## MARKE & DESIGN

Etablierte, vertraute, verbreitete Online-Angebote gewinnen das Vertrauen der Nutzer schneller, als neue, noch unbekannte und wenig verbreitete. Für innovative Angebote des Identitätsmanagements stellt dies offensichtlich eine Herausforderung dar. Ist eine kritische Teilnehmerzahl noch nicht überschritten, können Angebote nicht davon profitieren, dass Nutzer sich über deren Vorteile unterhalten und sie weiterempfehlen. Stattdessen werden sie in jedem Einzelfall kritisch beäugt und vorsichtig erkundet.

*„Das müsste man sehen, wie sich das etabliert, ja.“ (N8\_05.03.2010)*

*„Ich habe so das Gefühl, sobald 50 Prozent der Leute um dich rum das mitmachen, machst du es auch mit, weil die Welt so geworden ist, habe ich so das Gefühl.“ (N5\_04.03.2010)*

*"Tja, also ich denke, ich würde es nutzen, wenn – es ist gleich wie mit allem, wenn es dann sich einbürgert und wenn es jeder hat und wenn es einfach so läuft, dann nutzt man es auch." (N19\_16.03.2010)*

Eine Möglichkeit, diesem Umstand zu begegnen, ist die Etablierung einer vertrauenswürdigen Marke für das Angebot. Die elektronische Steuererklärung ELSTER folgt etwa dieser Strategie. Der Vorteil eines solchen Ansatzes ist, dass die Etablierung einer Marke die Vermittlung des mit dem Angebot verbundenen Nutzens deutlich erleichtert - dies ist eine Kernaufgabe des Marketings. Auf der anderen Seite ist dieser Ansatz jedoch mit einem erheblichen Aufwand verbunden - die Etablierung einer neuen Marke ist zeitaufwändig und ressourcenintensiv.

Was also, wenn dieser Weg nicht beschritten werden soll? Erneut bietet der Umstand, dass Angebote des Identitätsmanagements eine Infrastrukturfunktion erfüllen, vielversprechende Auswege: so mag etwa der neue Personalausweis keine etablierte, vertrauenserweckende Marke aufweisen, zahlreiche Angebote des Internets, wie Amazon, eBay oder Facebook, tun dies jedoch offensichtlich schon. Gelingt es also deutlich zu machen, dass die eID Applikation einen sicheren Zugang zu bekannten und sympathischen Marken darstellt, dann strahlen deren Markenwerte auf die noch wenig vertraute Applikation aus. Wenn also etablierte Anbieter eID Funktionalitäten nahtlos in ihre Transaktionsprozesse integrieren, dann werden auch diese Funktionalitäten eine höhere Akzeptanz erfahren.

Nicht vergessen werden sollte, dass Elemente der Gestaltung ebenfalls auf die Vertrauensneigung der Nutzer ausstrahlen. Auch öffentliche Angebote des Identitätsmanagements sollten also saubere, professionelle und nach Möglichkeit sympathische Nutzeroberflächen aufweisen. Sofern die Nutzer bereits an gewisse Prozesse der Anmeldung und Nutzung gewohnt sind, sollten sich neue Angebote an diesen orientieren. Vertraute Oberflächen und Prozesse erzeugen Vertrauen. Ein hoher Lern- oder Umstellungsaufwand reduziert dagegen die Nutzungsbereitschaft. Nicht zuletzt erleichtert ein ansprechendes "Corporate Design" seinerseits auch wiederum den Aufbau einer vertrauenerweckenden Marke.

## **KUNDENSERVICE**

Die Zugänglichkeit, Hilfsbereitschaft und Zuverlässigkeit des Kundendienstes hat einen massgeblichen Einfluss auf die Vertrauensbereitschaft der Nutzer. Bei Rückfragen oder Unsicherheiten im Rahmen der Anmeldung oder Abwicklung einer Transaktion wünschen sich Internetnutzer also einen freundlichen und kompetenten Ansprechpartner. Auch Angebote der öffentlichen Hand sollten sich auf diesen Wunsch einstellen und entsprechende Verantwortlichkeiten definieren und Ressourcen bereitstellen. Vor allem aber sollte die potentielle Verfügbarkeit eines solchen Kundendienstes deutlich signalisiert werden. Einfach aufzufindende Kontaktangaben und verschiedene Möglichkeiten der Kontaktaufnah-

me dienen hier als vertrauensstiftendes Signal, dass im Notfalle auch eine entsprechende Servicekapazität zur Verfügung steht. Die Möglichkeit, sich im Falle von Fragen oder Sorgen an einen kompetenten Kundendienst wenden zu können, dürfte insbesondere im Rahmen solcher Geschäftsmodelle hilfreich sein, die als sensitiv hinsichtlich der Sicherheit und Privatheit der Nutzer betrachtet werden können. Dies dürfte bei Angeboten des Identitätsmanagements zweifellos der Fall sein.

## NUTZERKONTROLLE

Die Bereitschaft eines Nutzers, einem Transaktionspartner persönliche Daten zur Verfügung zu stellen, impliziert nicht, dass er auch bereit ist, die Kontrolle über diese Daten gänzlich aufzugeben. Insbesondere sofern ein Anbieter beabsichtigt, diese Daten mit dritten Parteien zu teilen, möchten Nutzer informiert oder um eine Zustimmung gebeten werden. Der Eindruck, die weitere Analyse und Verbreitung der eigenen Daten nicht kontrollieren zu können, löst Sorgen aus und zerstört Vertrauen. Um das Vertrauen der Nutzer dagegen zu gewinnen, ist es notwendig, nur solche Daten abzufragen, die für den Betrieb des entsprechenden Angebots tatsächlich notwendig sind. Auch im Rahmen des Identitätsmanagements sollte der Umfang der abgefragten Daten also transparent und nachvollziehbar sein.

*"Also, der Staat weiss mittlerweile so viel schon über mich und ich kann mich kaum davor schützen, der hat Einblick in alle meine Konten, in meine Gesundheitsdaten. Das ist schon so vernetzt, da kann ich gar nichts mehr schützen, es sei denn, ich bin wirklich jetzt im Ausland und auch da wird es immer schwerer." (N1\_23.02.2010)*

Sofern eine Weitergabe persönlicher Daten an dritte Parteien notwendig ist, so ist dieser Prozess für die Nutzer nachvollziehbar zu gestalten. Opt-in Modelle können hier vertrauenserweckend wirken, wenn also die Nutzer souverän entscheiden können, mit welchen Parteien welche Daten geteilt werden. Auf diese Weise ist sichergestellt, dass eine Datenverbreitung nicht ohne Wissen und Zustimmung der Nutzer geschieht. Im Rahmen des Identitätsmanagements könnten daher Nutzerkonten hilfreich sein, welche sichtbar machen, zu welchem Zeitpunkt welche Daten mit welchen Transaktionspartnern geteilt wurden. So ist auch rückblickend Transparenz gewährleistet, dem Nutzer wird die Souveränität über die eigenen Daten nachvollziehbar signalisiert.

Auch unabhängig von der Weitergabe an dritte Parteien sollte stets deutlich gemacht werden, zu welchen Zwecken persönliche Daten gespeichert und ausgewertet werden. Hier dürften insbesondere Angebote der öffentlichen Hand vor einer Herausforderung stehen. Wie kann dem Bürger glaubwürdig vermittelt werden, dass sensitive Daten, wie sie mit Online-Transaktionen verbunden sind, tatsächlich nur dem Anbieter der eID Applikation einsichtig sind? Wie kann glaubwürdig sichergestellt werden, dass solche Daten nicht ver-

waltungsintern geteilt werden? Die Steuerbehörden oder Strafverfolgungsbehörden stellen aus Sicht der Nutzer "dritte Parteien" dar, welche die Notwendigkeit eines Datenzugriffs möglicherweise mit Leichtigkeit plausibel begründen können.

*"Ich weiss nicht, ob ich so einer Datenkrake wie dem deutschen Staat irgendwie noch wirklich mehr über mich geben möchte." (N2\_02.03.2010)*

*"Dass es auch abartig ist, wenn man denkt, was für Daten die aggregieren können, jetzt mit der Vorratsdatenspeicherung, alles, alles Steuern, Hartz IV, alles, alles kommt zusammen." (N5\_04.03.2010)*

Auch eine Veränderung der Rechtslage ist hier meist nicht auszuschliessen, nachdem eine Applikation erst einmal etabliert wurde. Derartige Ängste vor verwaltungsinternen Datenweitergaben dürften aufgrund ihrer politischen Natur besonders schwierig zu besänftigen sein, wenn die Infrastruktur des Identitätsmanagements in staatlicher Hand liegt.

*"Und was man davon halten soll, ich weiss es auch nicht, das ist sehr, sehr schwierig, denn so lange alle guten Willens sind und niemand Missbrauch vorhat, ist es ja an sich okay, aber man weiss nie, wann wird das missbraucht und von wem und wer hat alles Zugang." (N6\_04.03.2010)*

## THIRD PARTY ENDORSEMENTS

Empfiehl eine vertrauenswürdige Quelle eine Anwendung, so trifft diese auf eine höhere Nutzungsbereitschaft. Freunde, Bekannte und Verwandte dürfen als solche vertrauenswürdige Quellen betrachtet werden. Hier zeigt sich erneut die Herausforderung neuer Applikationen, eine kritische Nutzungsschwelle zu überschreiten: je mehr Bürger öffentliche Angebote des Identitätsmanagements nutzen, desto eher tauschen sie sich darüber aus, vermitteln eine Normalität ihrer Nutzung oder empfehlen diese möglicherweise gar. Es existieren bei der Etablierung neuer Angebote also Schneeballeffekte - Implementationsstrategien sollten darum darauf ausgerichtet sein, in einem kurzen Zeitraum kritische Nutzermassen zu erreichen. Auf Basis einer solchen Nutzermasse sollte die Applikation gezielt auf Review- oder Social Bookmarking-Seiten den Beurteilungen, Wertungen und Empfehlungen der Nutzer ausgesetzt werden. Wenn schliesslich ein unentschlossener Bürger die Nutzung eines neuen eID Angebots erwägt, greift er möglicherweise bei der Entscheidungsfindung gerade auf die dort abgebildeten Meinungen anderer Nutzer zurück.

*"Ich müsste, glaube ic,h erst mal abwarten, wie es sich entwickelt und wie vielleicht die Resonanz von den anderen Leuten ist, die ich so kenne, und dann würde ich das glaube ich versuchen." (N13\_09.03.2010)*

*"Der Erste würde ich jetzt nicht sein wollen, aber genau, wenn es gute Resultate zeigt, dann würde ich das auch machen, ja." (N9\_05.03.2010)*

Auch Tests und Empfehlungen professioneller dritter Parteien wirken vertrauensstiftend. Sofern eine Applikation solchen Tests unterworfen wurde, sollten entsprechende Gütesiegel gut sichtbar auf den Nutzeroberflächen präsentiert werden. Die Glaubwürdigkeit der empfehlenden Institution überträgt sich so auf ein noch junges Angebot. Auch mit Preisen und Auszeichnungen ist entsprechend zu verfahren. Unsere Studie zeigt, dass die Resultate der Internet-Suchmaschinen ein bedeutendes Vertrauenssignal darstellen. Auch öffentliche Angebote sollten daher vor Suchmaschinenoptimierungen nicht zurückschrecken, um bei einer entsprechenden Suche durch einen Nutzer ein prominentes Ranking zu erzielen.

*"Ich würde mich bei Google oder Wikipedia informieren." (N8\_05.03.2010)*

*"Oh, ich würde wahrscheinlich das einfach googlen, würde einfach mal sehen, was, wenn ich 'ePA' eingeben oder 'neueste elektronische Möglichkeit, Einkauf im Internet sicher zu machen' oder so, würde ich da versuchen zu googlen, und dann auf die jeweiligen Seiten, die dann da erscheinen würden, gehen." (N11\_08.03.2010)*

Die im Zusammenhang mit dem Vertrauensfaktor Marke & Design empfohlene Einbettung in die Transaktionsprozesse etablierter Anbieter ist im übrigen ihrerseits auch als eine Art Third Party Endorsement zu verstehen. Wenn ein vertrauenswürdiger Anbieter freiwillig auf die öffentlichen Infrastrukturen des Identitätsmanagements zurückgreift, so ist dies ein Signal für dessen Qualität und Zuverlässigkeit.

## REALWELTBEZUG

Online-Anbieter, welche auch eine physische Präsenz - etwa in Form von Filialen - aufweisen, sind gegenüber reinen Online-Anbietern im Vorteil, wenn es um die Gewinnung von Nutzervertrauen geht. Öffentliche Angebote des Identitätsmanagements sollten daher neben einem angemessenen Kundenservice auch den möglichen Vorteil einer flächendeckenden Verwaltungspräsenz gezielt ausspielen. Als Beispiel kann hier etwa die elektronische Steuererklärung ELSTER dienen, welche in den lokalen Finanzämtern auch durch ein geschultes Personal vertreten wird. Sofern also die gebietskörperschaftliche Verantwortung in einer Weise arrangiert werden kann, die eine solche lokale Vertretung ermöglicht, sollten die entsprechenden Ansprechpartner vor Ort ausreichend geschult und ihre Erreichbarkeit konsequent kommuniziert werden.

*"Ich würde mich wahrscheinlich auch im Internet informieren, und ich weiss nicht, wo ich mich sonst noch beraten lassen könnte. Ich weiss nicht, welche Behörde oder wo ich da wirklich Informationen bekäme, auf die ich mich verlassen könnte." (N16\_16.03.2010)*

*"Na ja, sagen wir mal so, es gibt ja Ämter, da weiss man, dass man sofort drankommt und dass die auch nett sind, aber es gibt schon Ämter, wo ich sage, da muss ich jetzt nicht unbedingt privaten und persönlichen Kontakt haben." (N27\_26.04.2010)*

Öffentliche Angebote sollten sich nicht darauf ausruhen, dass der staatliche Betreiber den Nutzern aus Medien und gelegentlichen Verwaltungsakten bekannt ist. Gerade auf Bundesebene drohen Infrastrukturanbieter für den einzelnen Bürger abstrakt und unnahbar zu bleiben - hier verfügt die kommunale Verwaltung über einen deutlichen Vorteil, indem sie - etwa im altbekannten Rathaus - eine spür- und greifbare Alltagspräsenz aufweist. Sofern öffentliche Angebote diese lokale Infrastruktur nicht einbinden können, empfiehlt es sich, die physische Präsenz der verantwortlichen Institution deutlich zu kommunizieren: Adresse, Kontaktmöglichkeiten, weitere Informationen zu Grösse, Geschichte und Organisation der Institution gehören ebenso zu Signalen einer realen Verantwortlichkeit, wie etwa Fotos von Geschäftsräumlichkeiten oder Mitarbeitern. Je menschlicher und greifbarer sich der Anbieter präsentiert, desto eher wird er das Vertrauen der Nutzer gewinnen.

## TECHNISCHE ZUVERLÄSSIGKEIT

Die Abwesenheit von Fehlern, Abstürzen oder Unterbrechungen ist ebenso ein Treiber des Nutzervertrauens, wie die reibungslose Erfüllung der versprochenen Funktionalität. Wir sprachen von der technischen Zuverlässigkeit eines Angebots als einem Hygienefaktor - diese wird schlicht vorausgesetzt, sobald ein Angebot verfügbar ist und beworben wird. Ist sie nicht vorhanden und treten entsprechende Fehler auf, so wird das Vertrauen auch jener Nutzer vernichtet, welche zu einem frühen Zeitpunkt bereit waren, auf ein Angebot einzugehen. Es sollte also keiner weiteren Ausführung bedürfen, die dringende Notwendigkeit festzustellen, dass - naturgemäss sensible - Angebote des Identitätsmanagements alle notwendigen Testläufe bestanden haben und tatsächlich voll funktionsfähig und einsatzbereit sein müssen, wenn sie den potentiellen Nutzern vorgestellt und angedient werden.

Je reibungsloser ein Angebot dabei funktioniert, desto vertrauenswürdiger wirkt es. Eine effiziente Abwicklung der notwendigen und versprochenen Prozesse ist hier ebenso von Bedeutung, wie etwa schnelle Ladezeiten einer Webseite. Die Vorteile einer nahtlosen Integration von eID Applikationen in die Prozesse etablierter Anbieter hatten wir bereits dargestellt.

*"Ich hätte keine Lust, ein weiteres, wenn auch nur kleines Gerät, in meinem Haushalt zu haben, 'nur' um den Online-Handel sicherer zu machen. Ich würde mir wünschen, dass es irgendwie mit bestehender Technologie funktioniert." (N3\_03.03.2010)*

*"Also, ich glaube nicht, dass irgendwelche Zusatzgeräte, die man sich irgendwo aufstellen muss, überhaupt eine Zukunft haben, weil alles immer mobiler wird und auch immer mobiler sein muss." (N12\_08.03.2010)*

Gleiches gilt für die Attraktivität übersichtlicher, professioneller Benutzeroberflächen, welche nach Möglichkeit bekannte Prozessabläufe aufgreifen und so Vertrauen stiften sollten. Trotz der häufig umstrittenen und bisweilen aufreibenden politischen Natur öffentlicher Projekte eines innovativen Identitätsmanagements sollten also Eigenschaften eines professionellen Angebots nicht vernachlässigt werden: störungsfreie technische Infrastrukturen und Prozesse sowie ein funktionales und ansprechendes Design.

## FAZIT

Abschliessend sollte erneut darauf hingewiesen werden, dass neben Eigenschaften des eigentlichen Angebots auch individuelle Nutzercharakteristika und der institutionelle Rahmen des Angebots einen massgeblichen Einfluss auf die Nutzungsbereitschaft der Bürger entfalten. Angesichts unterschiedlicher Vertrauensneigungen oder auch politischer Weltanschauungen kann nicht davon ausgegangen werden, dass selbst ein professionell gestaltetes und vertriebenes öffentliches Angebot des elektronischen Identitätsmanagements flächendeckend auf Akzeptanz stösst. Eine interessante Erkenntnis der im Rahmen dieser Studie durchgeführten Interviews war darüber hinaus, dass die Wahrnehmung von Sorgen hinsichtlich Sicherheit und Privatheit im Internet - und damit die Bedeutung des Vertrauensmanagements - sowohl auf Seiten der Nutzer wie auch auf der der Anbieter gewissen themenkonjunkturellen Schwankungen unterliegt. Gleiches dürfte damit für die hier identifizierten Vertrauensfaktoren gelten.

Wir hatten bereits festgestellt, dass Internetnutzer in der Regel mit der Herausforderung konfrontiert sind, die Vertrauenswürdigkeit eines Online-Angebots einzuschätzen, ohne die technischen Prozesse und Infrastrukturen vollständig zu verstehen, die diesem Angebot zugrunde liegen. Wie also sollen Nutzer beurteilen, ob ihre Sorgen hinsichtlich des Schutzes von Sicherheit und Privatheit im Rahmen einer Transaktion berechtigt sind, oder nicht? Die hier identifizierten Faktoren stellen in vielen Fällen Indikatoren dar, welche als Signal hinsichtlich der Vertrauenswürdigkeit eines Angebots interpretiert werden - etwa Empfehlungen dritter Parteien, die Bekanntheit einer Marke oder die realweltliche Erreichbarkeit eines Anbieters. Unbeantwortet bleibt dabei jedoch die Frage, warum gerade diese Signale als Vertrauensfaktoren akzeptiert werden. Mit anderen Worten: wie wird das gesellschaftliche Verständnis von Sicherheit und Datenschutz, ihrer Notwendigkeit und tatsächlichen Verfügbarkeit konstruiert?

*„Ich hätte gerne eine breite Debatte, wo sich alle einschalten können, so in führenden deutschen Zeitungen, in der FAZ und in der SZ zum Beispiel, in der Zeit, wo dann möglichst viele Leute eben zu Wort kommen, so dass ich das Gefühl habe, das ist was, wo sich alle beteiligt haben und alle vorher gefragt wurden, die man fragen muss, um zu wissen, wie man das etablieren kann und was wichtig ist und die mir dann die Sicherheit geben, dass die kritischen Stimmen gehört wurden und dass es eine gute Sache ist.“ (N1\_23.02.2010)*

*"Also, ich verfolge die Diskussion ein bisschen in der Presse über den Datenschutz in dem Zusammenhang. Im Moment bin ich mir nicht sicher, ob ich das wirklich will."  
(N7\_05.03.2010)*

Sowohl die interviewten Nutzer wie auch Anbieter verliessen sich hier weitgehend auf den vor allem medial vermittelten öffentlichen Diskurs. Wenn also, etwa ausgelöst durch einen aktuellen Datenschutz-Skandal, die öffentliche Debatte vermittelt, dass die Sicherheit des Nutzers im Netz, der Schutz seiner persönlichen Daten, von besonderer Dringlichkeit ist, so reagieren die Nutzer mit höherer Aufmerksamkeit und Kritikbereitschaft, die Anbieter kommunizieren umso bemühter ihre Vertrauenswürdigkeit.

*"Ja, und darüber merken Sie auch immer Wellen, die dann [wenn Datensicherheit in den Medien thematisiert wird] reinkommen, sage ich mal, wo dann Kunden sich auch erkundigen sozusagen, was macht ihr, woher kommt das." (A6\_19.02.2009).*

*"Ja, natürlich, also das denke ich schon, vor allen Dingen in den letzten Jahren oder Monaten ist das Thema Datenschutz sehr, sehr zu einem wichtigen Thema geworden, vor allem durch die Mediendiskussion und durch einige Datenschutzskandale, die wir halt hatten."  
(A11\_20.04.2009).*

Somit sind die hier beschriebenen Vertrauensfaktoren, abhängig von der medialen Aufmerksamkeit oder thematischen Dringlichkeit von Sicherheit und Privatheit, nicht immer gleichermassen im öffentlichen Bewusstsein präsent. Es ist sogar vorstellbar, dass eine Veränderung des öffentlichen Diskurses - etwa aufgrund technologischer Innovationen oder veränderter politischer und rechtlicher Rahmenbedingungen - zur nachhaltigen Abwertung einzelner Vertrauensfaktoren und dem Entstehen neuer Einflussgrößen führten. Die öffentliche Hand ist hier in der einmaligen Lage, jene Rahmenbedingungen mitgestalten zu können, denen ihre Angebote unterworfen sind.

In jedem Fall ist es ein notwendiges Element der Einführung und Kommunikation innovativer Applikationen des elektronischen Identitätsmanagements, den öffentlichen und medialen Diskurs rund um Sicherheit und Privatheit im Netz zu verfolgen, und dessen Implikationen für die durch Nutzer wahrgenommene Signale der Vertrauenswürdigkeit abzuwägen. Nutzer erwarten nicht zuletzt von Repräsentanten der öffentlichen Hand, dass sie sich im Rahmen dieses Diskurses engagieren und damit Orientierung bieten. Es ist unsere Hoffnung, dass die vorliegende Studie von Seiten ISPRAT sowie des Instituts für Medien- und Kommunikationsmanagement der Universität St. Gallen einen hilfreichen Beitrag zur anhaltenden Debatte rund um Sicherheit und Privatheit im Netz darstellt.

# VI. VERÖFFENTLICHUNGEN

- Hoffmann, C.P. & von Kaenel, A. (2009). Vertrauen - aber wie? Sicherheit versus Privatheit im Internet. *Datareport*, 4, 22-24.
- Hoffmann, C.P. & von Kaenel, A. (2010a). Online Trust Management: Eine Herausforderung für die Unternehmenskommunikation. In G. Bentele, M. Piwinger & G. Schönborn (Hrsg.), *Kommunikationsmanagement. Strategien, Wissen, Lösungen* (1-26). Neuwied: Luchterhand.
- Hoffmann, C.P. & von Kaenel, A. (2010b). Vertrauen: Notwendige Grundlage von Online-Transaktionen. In R. Schliesky (Hrsg.), *Technikgestütztes Identitätsmanagement. Schriften zur Modernisierung von Staat und Verwaltung* (81-98). Kiel: Lorenz-von-Stein-Institut für Verwaltungswissenschaften.
- Hoffmann, C. P., von Kaenel, A. & Meckel, M. (2011). Online Reputation Management: Identifying Drivers of Online Trust. *15th International Conference on Corporate Reputation, Brand, Identity and Competitiveness* (Mai 2011), New Orleans, Louisiana US.
- Hoffmann, C. P., von Kaenel, A., Meckel, M. & Suphan, A. (2011). Core Cues in Initial Trust Formation: Exploring Differences between Online Business Models. *71st Annual Meeting of the Academy of Management* (August, 2011), San Antonio, Texas US.
- Hoffmann, C. P., Meckel, M. & von Kaenel, A. (2010). The Role of Public Relations in Online Trust Management. *60th Annual Conference of the International Communication Association* (Juni 2010), Singapore.
- Von Kaenel, A., Hoffmann, C. P. & Meckel, M (2010) Online Vertrauensmanagement : Herausforderung für die Organisationskommunikation. *Jahrestagung der Schweizerischen Gesellschaft für Kommunikations- und Medienwissenschaft (SGKM)* (Mai 2010), Luzern.

# VII. LITERATUR- UND QUELLENVERZEICHNIS

- Aaker, D. (1995). Building strong brands. *Brandweek*, 36(37), 28-34.
- Aaker, D. (2000). *Brand leadership*. New York: Free Press.
- Afuah, A. & Tucci, C.L. (2001). *Internet Business Models and Strategies*. Boston: McGraw-Hill.
- Albrecht, J. P. (2007). *Sicherheit statt Rechtsstaat – Der Konflikt bei der Vorratsdatenspeicherung spitzt sich zu*. In: ForumRecht (FoR) 1/2007, S. 13–15. Gefunden am 15.03.2010 unter [http://janalbrecht.eu/beitraege/allgemein/for\\_vorratsdaten.pdf](http://janalbrecht.eu/beitraege/allgemein/for_vorratsdaten.pdf)
- Arminger, G. (1979). *Faktorenanalyse. Statistik für Soziologen*. Stuttgart: Teubner.
- Ashworth, L. & Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics*, 67(2), 107-123.
- Augsburger Allgemeine (2009, 31. Oktober). Datenklau bei SchülerVZ: Verdächtiger nimmt sich das Leben. *Augsburger Allgemeine*. Gefunden am 05. Januar 2010 unter [www.augsburger-allgemeine.de/Home/Nachrichten/Aus-aller-Welt/Artikel-datenklau-schueler-VZ-Selbstmord-\\_arid,1963138\\_regid,2\\_puid,2\\_pageid,4293.html](http://www.augsburger-allgemeine.de/Home/Nachrichten/Aus-aller-Welt/Artikel-datenklau-schueler-VZ-Selbstmord-_arid,1963138_regid,2_puid,2_pageid,4293.html)
- Backhaus, K., Erichson, B., Plinke, W. & Weiber, R. (2011). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung* (13. Auflage). Berlin: Springer.
- Bart, Y., Shankar, V., Sultan, F. & Urban, G. (2005). Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing*, 69(4), 133-152.
- Belanger, F., Hiller, J.S. & Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270.
- Bhatnagar, A., Misra, S. & Rao, H.R. (2000). On risk, convenience and internet shopping behavior. *Communications of the ACM*, 43(11), 98-105.
- Bhattacharjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems*, 19(1), 211-241.
- Blech, J., Bonstein, J., Dworschak, M., Evers, M., Kneip, A., Müller, M. U., Schmitt, S. & Schmundt, H. (2009). Nackt unter Freunden. *Der Spiegel*, 10, 118-131.
- boyd, D. & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1). Gefunden am 29. November 2010 unter <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>
- Brinkmann, U. & Seifert, M. (2001). "Face to interface": Zum Problem der Vertrauenskonsti-

tution im Internet am Beispiel von elektronischen Auktionen. *Zeitschrift für Soziologie*, 30(1), 23-47.

- Bucher, E., Fieseler, Ch. & von Kaenel, A. (2009). Web 2.0 - Eine Annäherung an die Herausforderungen des neuen Internetzeitalters aus Sicht der Unternehmenskommunikation. In G. Bentele, M. Piwinger & G. Schönborn (Hrsg.), *Kommunikationsmanagement. Strategien, Wissen, Lösungen* (1-24). Neuwied: Luchterhand.
- Chadwick, S.A. (2001). Communicating trust in e-commerce interactions. *Management Communication Quarterly*, 14(4), 653-658.
- Chau, P.Y.K., Au G. & Tam K.Y. (2000). Impact of Information Presentation Modes on Online Shopping: An Empirical Evaluation of a Broadband Interactive Shopping Service. *Journal of Organizational Computing & Electronic Commerce*, 10(1), 1-21.
- Chellappa, R. & Sin, R. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), 181-202.
- Cheskin/Sapient (1999). *eCommerce trust study*. Cheskin Research and Studio Archetype. San Francisco: Business Wire.
- Cook, D. & Luo, W. (2003). The Role of Third-Party Seals in Building Trust Online. *e-Service Journal*, 2(3), 71-84.
- Corbitt, B., Thanasankit, T. & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce Research & Applications*, 2(3), 203-215.
- Culnan, M.J. & Armstrong, P.K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104-115.
- Das, T.K. & Teng, B.-S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review*, 23(3), 491-512.
- Denzin, N.K. (1983). Interpretative Interactionism. In G. Morgan (Ed.), *Beyond Method: Strategies for Social Research*. London: Sage.
- Dozier, D.M. & Ehling, W.P. (1992). Evaluation of Public Relations Programs: What the Literature Tells Us About Their Effects. In J. E. Grunig (Ed.), *Excellence in Public Relations and Communication Management* (159-184). Hillsdale: Lawrence Erlbaum.
- Eastlick, M.A., Lotz, S.L. & Warrington, P. (2006). Understanding Online B-to-C Relationships: An integrated Model of Privacy Concerns, Trust and Commitment. *Journal of Business Research*, 59(8), 877-886.
- Ebersbach, A., Glaser, M. & Heigl, R. (2008). *Social Web*. Konstanz: UVK.
- Eck, K. (2008). *Karrierefalle Internet. Managen Sie Ihre Online-Reputation, bevor andere es tun!* München: Carl Hanser Verlag.

- Egger, F. (2000). "Trust me, I'm an online vendor": towards a model of trust for e-commerce system design. *Proceedings of the CHI '00 extended abstracts on Human factors in computing systems* (101-102). New York: ACM Press.
- Facebook (2010). *Pressebereich. Statistiken*.  
<http://www.facebook.com/press/info.php?statistics>
- Fang, X. & Salvendy, G. (2003). Customer-Centred Rules for Design of e-Commerce Web Sites. *Communications of the ACM*, 46(12), 332-336.
- Fiala, B. (2011). Facebookeintrag vom 22.02.2011 auf der Gruppe Stop Vorratsdatenspeicherung! Gefunden am 15. März 2011 unter <http://www.facebook.com/pages/STOP-VORRATSDATENSPEICHERUNG-/181620984640>
- Friedman, B.A., Kahn, P.H. & Howe, D.C. (2000). Trust Online. *Communications of the ACM*, 43(12), 34-40.
- Gallant, L., Boone, G. M. & Heap, A. (2007). Five heuristics for designing and evaluating Web-based communities [Electronic Version]. *First Monday*, 12(3).
- Gefen, D. (2000). E-Commerce: The role of familiarity and trust. *Omega: The International Journal of Management Science*, 28(6), 725-737.
- Geider, F.J., Rogge, K.-E. & Schaaf, H.P. (1982). *Einstieg in die Faktorenanalyse*. Heidelberg: Quelle & Meyer.
- Geyskens, I., Steenkamp, J.-B.E.M. & Kumar, N. (1998). Generalizations about trust in marketing channel relationships using meta-analysis. *International Journal of Research in Marketing*, 15(3), 223-248.
- Glaser, B. (1992). *Basics of Grounded Theory Analysis - Emergence vs Forcing*. Mill Valley, CA: Sociology Press.
- Glaser, B. & Strauss, A. (1967). *The Discovery of Grounded Theory*. Chicago: Aldine.
- Gläser, J. & Laudel, G. (2006). *Experteninterviews und qualitative Inhaltsanalyse*. Wiesbaden: VS Verlag.
- Gmür, M. (2002). *Der öffentliche Mensch. Medienstars und Medienopfer*. München: Deutscher Taschenbuch Verlag.
- Göldi, A. (2008). *Das Komplexitätsproblem von Social-Media-Marketing*.  
<http://netzwertig.com/2008/12/18/werbung-das-komplexitaetsproblem-von-social-media-marketing/>
- Greif, B. (2009). SchülerVZ-Datendiebstahl: 20-Jähriger wegen versuchter Erpressung verhaftet. *ZDNet.de*. Gefunden am 05. Januar 2010 unter [www.zdnet.de/news/wirtschaft\\_sicherheit\\_security\\_schuelervz\\_datendiebstahl\\_20\\_jaehriger\\_wegen\\_versuchter\\_erpressung\\_verhaftet\\_story-39001024-41516081-1.htm](http://www.zdnet.de/news/wirtschaft_sicherheit_security_schuelervz_datendiebstahl_20_jaehriger_wegen_versuchter_erpressung_verhaftet_story-39001024-41516081-1.htm)

- Grunig, J.E. (1993). Image and Substance: From Symbolic to Behavioral Relationships. *Public Relations Review*, 19(2), 121-139.
- Grunig, J.E. & Hunt, T. (1984). *Managing Public Relations*. New York: Holt.
- Ha, Y-Y. & Perks, H. (2005). Effects of consumer perceptions of brand experience on the web: Brand familiarity, satisfaction and brand trust. *Journal of Consumer Behaviour*, 4(6), 438-452.
- Harris, L. & Goode, M. (2004). The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of Retailing*, 80(2), 139-158.
- Heise (2011). Heise Online Demonstration "Freiheit statt Angst - Stoppt den Überwachungswahn" gefunden am 15. März 2011 unter [http://www.heise.de/newsticker/bilderstrecke/bilderstrecke\\_1077559.html?back=1077549;bild=2](http://www.heise.de/newsticker/bilderstrecke/bilderstrecke_1077559.html?back=1077549;bild=2)
- Hoffman, D.L. & Novak, T.P. (2009). Flow Online: Lessons Learned and future prospects. *Journal of Interactive Marketing*, 23(1), 23-24.
- Hoffman, D.L., Novak, T.P. & Peralta, M.A.(1999a). Building Consumer Trust Online. *Communications of the ACM*, 42(4), 80-85.
- Hoffman, D.L., Novak, T.P. & Peralta, M.A. (1999b). Information Privacy in the Market-space: Implications for the Commercial Use of Anonymity on the Web. *The Information Society*, 15(2), 129-139.
- Hoffmann, C.P. & von Kaenel, A. (2009). Sicherheit versus Privatheit im Internet. Vertrauen - aber wie? *Datareport*, 4, 22-24.
- Hoffmann, C.P. & von Kaenel, A. (2010a). Online Trust Management : Eine Herausforderung für die Unternehmenskommunikation. In G. Bentele, M. Piwinger & G. Schönborn (Hrsg.), *Kommunikationsmanagement. Strategien, Wissen, Lösungen* (1-26). Neuwied: Luchterhand.
- Hoffmann, C.P. & von Kaenel, A. (2010b). Vertrauen: Notwendige Grundlage von Online-Transaktionen. In R. Schliesky (Hrsg.), *Technikgestütztes Identitätsmanagement. Schriften zur Modernisierung von Staat und Verwaltung*. Band 7. Kiel: Lorenz-von-Stein-Institut für Verwaltungswissenschaften.
- Hoffmann, C.P., Meckel, M. & von Kaenel, A. (2010). The Role of Public Relations in Online Trust Management. *60th Annual Conference of the International Communication Association* (June 2010), Singapore.
- Hoffmann, C.P., von Kaenel, A. & Meckel, M. (2011). Online Reputation Management: Identifying Drivers of Online Trust. *15th International Conference on Corporate Reputation, Brand, Identity and Competitiveness* (Mai 2011), New Orleans, Louisiana US.

- Hoffmann, C.P., von Kaenel, A., Meckel, M. & Suphan, A. (2011). Core Cues in Initial Trust Formation: Exploring Differences between Online Business Models. *71<sup>st</sup> Annual Meeting of the Academy of Management* (August 2011), San Antonio, Texas US.
- Hopf, C. (1991). Qualitative Interviews in der Sozialforschung. Ein Überblick. In Flick, U., v. Kardorff, E., Keupp, H., v. Rosenstiel, L. & Wolff, S. (Hrsg.), *Handbuch qualitative Sozialforschung. Grundlagen, Konzepte, Methoden und Anwendungen*. München: Psychologie Verlags Union.
- Jarvenpaa, S.L. & Tractinsky, N. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, 5(2). Gefunden am 29. November 2010 unter <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1999.tb00337.x/full>
- Jarvenpaa, S.L., Tractinsky, N. & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, 1, 45-71.
- Jevons, C. & Gabbott, M. (2000). Trust, Brand Equity and Brand Reality in Internet Business Relationships: An Interdisciplinary Approach. *Journal of Marketing Management*, 16(6), 619-634.
- Johnson, D. (2007). Achieving customer value from electronic channels through identity commitment, calculative commitment, and trust in technology. *Journal of Interactive Marketing*, 21(4), 2-22.
- Jones, S., Wilikens, M., Morris, P. & Masera, M. (2000). Trust Requirements in e-Business. *Communications of the ACM*, 43(12), 81-87.
- Jung, T., Youn, H. & McClung, S. (2007). Motivations and Self Presentation Strategies on Korean-Based „Cyworld“ Weblog Format Personal Hompages. *CyberPsychology and Behavior*, 10(1), 24-31.
- Kilian, T., Hass, B. H. & Walsh, G. (2007). Grundlagen des Web 2.0. In B. H. Hass, G. Walsh & T. Kilian (Hrsg.), *Web 2.0 Neue Perspektiven für Marketing und Medien* (3-22). Berlin Heidelberg: Springer.
- Köhler, B. (2008). *Was heisst Social Media?* <http://blog.metaroll.de/2008/04/22/was-heisst-social-media/>
- Kovar, S.E., Burke K.G. & Kovar B.R. (2000). Consumer responses to the CPA WebTrust™ assurance. *Journal of Information Systems*, 14, 17-35.
- Krishnamurthy, S. (2001). An Empirical Study of the Causal Antecedents of Customer Confidence in E-Tailers. *First Monday* 6(1). Gefunden am 6. Dezember 2010 unter [http://131.193.153.231/www/issues/issue6\\_1/krishnamurthy/index.html](http://131.193.153.231/www/issues/issue6_1/krishnamurthy/index.html)
- Lambert, S. (2006). Do we need a "Real" Taxonomy of e-Business Models? *Flinders University School of Commerce Research Paper Series*, 06-6. Gefunden am 6. Dezember 2010 un-

ter [http://www.flinders.edu.au/shadomx/apps/fms/fmsdownload.cfm?file\\_uuid=FDBE4DE1-EB6B-7B71-0BCE-8FC142552687&siteName=sabs](http://www.flinders.edu.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=FDBE4DE1-EB6B-7B71-0BCE-8FC142552687&siteName=sabs)

- Lanier, C.D. & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12(2). Gefunden am 6. Januar 2009 unter <http://www.amsreview.org/articles/lanier02-2008.pdf>.
- Lee, M.K. O. & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, 6(1), 75-91.
- Lester, T. (2001). The Reinvention of Privacy. *The Atlantic Monthly*, 378(3), 27-39.
- Lewicki, R. J. & Bunker, B.B. (1995). Trust in relationships: A model of development and decline. In B.B. Bunker & J.Z. Rubin (Hrsg.), *Conflict cooperation and justice: Essays Inspired by the Work of Morton Deutsch* (133-173). San Francisco: Jossey-Bass.
- Lischka, K. (2010). *Facebook macht mehr öffentlich*. *Spiegel Online*.  
<http://www.spiegel.de/netzwelt/web/0,1518,689990,00.html>
- Luo, W. & Cook, D. (2007-2008). An empirical Study of Trust of Third Party Rating Services. *Journal of Computer Information Systems*, 48(2), 66-73.
- Luo, X. (2002). Trust production and privacy concerns on the internet. A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, 31, 111-118.
- Mahadevan, B. B. (2000). Business Models for Internet-Based E-Commerce: An Anatomy. *California Management Review*, 42(4), 55-69.
- Mayring, P. (2002). *Einführung in die qualitative Sozialforschung*. Weinheim: Beltz.
- McAllister, D.J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of management Journal*, 38(1), 24-59.
- McKnight, D.H. & Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, 6(2), 35-59.
- McKnight, D.H., Choudhury, V. & Kacmar, C. (2000). Trust in e-commerce vendors: A two-stage model. *ICIS '00 Proceedings of the twenty first international conference on Information systems* (532-536). Atlanta: ACM Press.
- McKnight, D.H., Choudhury, V. & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, 13(3), 334-359.
- Mehrmann, E. (1995). *Vom Konzept zum Interview. Informationsgespräche richtig planen und führen*. Düsseldorf: ECON.

- Milne, G.R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing*, 19(1), 1-6.
- Milne, G.R. & Boza, M.-E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13(1), 5-24.
- Milne, G.R. & Rohm, A.J. (2000). Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. *Journal of Public Policy & Marketing*, 19(2), 238-249.
- Morgan, R.M. & Hunt, S.D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), 20-38.
- Neubauer, R. (2010). Konkurrenz für Facebook. *St.Galler Tagblatt*, S.8.
- Nielsen, J.A. (1999). *Trust or bust: Communicationg trustworthiness in web design*. Gefunden am 27. Oktober 2009 unter [www.useit.com/alertbox/990307.html](http://www.useit.com/alertbox/990307.html)
- Nissenbaum, H. (2001). Securing Trust Online: Wisdom or Oxymoron? *Boston University Law Review*, 81(3), 101-131.
- Nowak, G. & Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters. *Journal of Direct Marketing*, 9(3), 46-60.
- O'Donnell, S. (2002). An Economic Map of the Internet. *TPRC 30th Research Conference on Communication, Information and Internet Policy* (September 2002), Alexandria, VA, US.
- OECD (2007). *Participative Web and User-Created Content. Web 2.0, Wikis and Social Networking*. <http://213.253.134.43/oecd/pdfs/browseit/9307031E.PDF>
- Olivero, N. & Lunt, P. (2004). Privacy versus Willingness to Disclose in e-Commerce Exchanges: The Effect of Risk Awareness on the relative Role of Trust and Control. *Journal of Economic Psychology*, 25(2), 243-262.
- O'Reilly, T. (2006). *Web 2.0 Compact Definition: Trying again*. Sebastopol: O'Reilly Media.
- Palfrey, J. & Gasser, U. (2008). *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.
- Palmer, J.W., Bailey, J.P. & Faraj, S. (2000). The role of intermediaries in the development of trust on the www: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication*, 5(3).
- Pavlou, P. (2002). Trustworthiness as a Source of Competitive Advantage in Online Auction Markets. *Academy of Management Proceedings*, 1, A1-A6.
- Peluchette, J. & Karl, K. (2010). Examining Students' Intended Image on Facebook: "What Were They Thinking?!" *Journal of Education for Business*, 85, 30-37.

- Pennington, R., Wilcox, H.D. & Grover, V. (2003). The Role of System Trust in Business-to-Consumer Transactions. *Journal of Management Information Systems*, 20(3), 197-226.
- Phelps, J., Nowak, G. & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), 27-41.
- Phelps, J.E., D'Souza, G. & Nowak, G. J. (2001). Antecedents and Consequences of Consumer Privacy Concerns: An empirical Investigation. *Journal of Interactive Marketing*, 15(4), 2-17.
- Preibusch, S., Hoser, B., Gürses, S. & Berendt, B. (2007). Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling. *Data Mining for User Modelling Workshop*, Corfu. <http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf>
- Riegelsberger, J. & Sasse, A.M. (2001). Trustbuilders and trustbusters. The role of trust cues in interfaces to e-commerce applications. *Proceedings of the 1st IFIP Conference on e-commerce, e-business, e-government (i3e)* (17-30.). Zurich, Switzerland.
- Rifkin, J. (2010). Facebook macht Junge toleranter. Interview mit Jeremy Rifkin. *Migros-Magazin*, 13, 30-33.
- Rousseau, D., Sitkin, S.B., Burt, R.S. & Camerer, C. (1998). Not so different after all: A cross-discipline View of Trust. *Academy of Management Review*, 23(3), 393-404.
- Ruisinger, D. (2007). *Online Relations. Leitfaden für moderne PR im Netz*. Stuttgart: Schäffer-Poeschel Verlag.
- Rust, R. T., Kannan, P.K. & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30(4), 455-464.
- Schoenbachler, D.D. & Gordon, G.L. (2002). Trust and Customer Willingness to provide Information in Database-driven Relationship Marketing. *Journal of Interactive Marketing*, 16(3), 2-16.
- Seidler, Ch. (2009). Datenpanne drängt SchülerVZ in die Defensive. *Spiegel Online*. Gefunden am 05. Januar 2010 unter [www.spiegel.de/netzwelt/netzpolitik/0,1518,655820,00.html](http://www.spiegel.de/netzwelt/netzpolitik/0,1518,655820,00.html).
- Shankar, V., Smith, A.K. & Rangaswamy, A. (2003). Customer satisfaction and loyalty in online and offline environments. *International Journal of Research in Marketing*, 20(2), 153-175.
- Shankar, V., Urban, G.L. & Sultan, F. (2002). Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions. *Journal of Strategic Information Systems*, 11(3-4), 325-344.
- Sheehan, K.B. & Hoy, M.G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28(3), 37-51.

- Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.
- Shneiderman, B. (2000). Designing Trust into Online Experiences. *Communications of the ACM*, 43(12), 57-59.
- Solove, D.J. (2007). *The future of reputation: gossip, rumor, and privacy on the Internet*. New Haven/London: Yale University Press.
- Speier, C., Harvey, M. & Palmer, J. (1998). Virtual management of global marketing relationships. *Journal of World Business*, 33(3), 263-276.
- Spiegel Online (2010, 16. Oktober). Nutzer kopiert massenhaft "SchülerVZ"-Profile. *Spiegel Online*. Gefunden am 05. Januar 2010 unter [www.spiegel.de/netzwelt/netzpolitik/0,1518,655703,00.html](http://www.spiegel.de/netzwelt/netzpolitik/0,1518,655703,00.html)
- Spiegel Online Thema (2011). Thema Vorratsdatenspeicherung. Gefunden am 15. März 2011 unter <http://www.spiegel.de/thema/vorratsdatenspeicherung/>
- Strauss, A. & Corbin, J. (1997) *Grounded Theory in Practice*. Thousand Oaks, CA: Sage.
- Strauss, A. & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd edition). Thousand Oaks: Sage.
- Strübing, J. (2004). *Grounded Theory: zur sozialtheoretischen und epistemologischen Fundierung des Verfahrens der empirisch begründeten Theoriebildung*. Wiesbaden: VS Verlag.
- Tabachnick, B. G. (2007). *Using multivariate statistics* (5th ed.). Boston, Mass.: Pearson.
- Timmers, P. (1998). Business Models for Electronic Markets. *Electronic Markets*, 8(2), 3-8.
- Überla, K. (1977). *Faktorenanalyse. Eine systematische Einführung für Psychologen, Mediziner, Wirtschafts- und Sozialwissenschaftler*. Berlin: Springer-Verlag.
- Urban, G.L., Amyx, C. & Lorenzon, A. (2009). Online Trust: State of the Art, New Frontiers, and Research Potential. *Journal of Interactive Marketing*, 23(2), 179-190.
- Urban, G.L., Sultan, F. & Qualls, W.J. (2000). Placing Trust at the Center of Your Internet Strategy. *Sloan Management Review*, 42(1), 39-48.
- Van Eimeren, B., & Frees, B. (2009). *Der Internetnutzer 2009 - multimedial und total vernetzt? Ergebnisse der ARD/ZDF-OnlineStudie*. [http://www.ard-zdf-onlinestudie.de/fileadmin/Online09/Eimeren1\\_7\\_09.pdf](http://www.ard-zdf-onlinestudie.de/fileadmin/Online09/Eimeren1_7_09.pdf)
- Van Riel, C. B. M. (1992). *Principles of Corporate Communication*. London: Prentice Hall.
- Vidmar, N. & Flaherty, D.H. (1985). Concern for Personal Privacy in an Electronic Age. *Journal of Communication*, 35(2), 91-103.
- Von Kaenel, A., Hoffmann, C.P. & Meckel, M. (2010). Online Vertrauensmanagement: Herausforderung für die Organisationskommunikation. *Jahrestagung der Schweizerischen Gesellschaft für Kommunikations- und Medienwissenschaft (SGKM)* (Mai 2010), Luzern.

- Wakefield, R. & Whitten, D. (2006). Examining User Perceptions of Third-Party Organization Credibility and Trust in an E-Retailer. *Journal of Organizational & End User Computing*, 18(2), 1-19.
- Walczuch, R. & Lundgren, H. (2004). Psychological Antecedents of institution-based Consumer Trust in e-Retailing. *Information & Management*, 42(1), 159-177.
- Wang, S., Beatty, S.E. & Foxx, W. (2004). Signaling the trustworthiness of Small Online Retailers. *Journal of Interactive Marketing*, 18(1), 53-69.
- Yen, H.J.R. & Gwinner, K.P. (2003). Internet Retail Customer Loyalty: The Mediating Role of Relational Benefits. *International Journal of Service Industry Management*, 14, 483-500.
- Yoon, S.-J. (2002). The Antecedents and Consequences of Trust in Online-Purchase Decisions. *Journal of Interactive Marketing*, 16(2), 47-63.
- Zimmer, D. (2010). Wenn Web Händler Offline gehen. Gefunden am 19. April 2011 unter <http://www.internetworld.de/Heftarchiv/2010/Ausgabe-22-2010/Wenn-Web-Haendler-offline-gehen>
- Zucker, L.G. (1986). The production of trust: Institutional sources of economic structure, 1840-1920. In L. L. Cummings (Ed.), *Research in Organizational Behavior*, Vol. 8, (53-111). Greenwich, CT: JAI Press.

## ANHANG

### A: LEITFADEN ANBIETER-BEFragung

Einleitend wurde den Gesprächspartnern Ausgangspunkt und Hintergrund des Projekts erläutert. Es wurde angesprochen, dass Online-Geschäftsmodelle häufig darauf beruhen, dass Nutzer im Internet bereit sein müssen, dem Anbieter persönliche Daten bereitzustellen.

- Sicht des Unternehmens: Wie wird die Bedeutung des Kundenvertrauens für das eigene Geschäftsmodell eingeschätzt?
- Warum vertrauen Kunden dem Unternehmen? Warum sind sie bereit, ihm Daten anzuvertrauen?
- Worauf achten Kunden, wenn sie sich entscheiden, mit dem Unternehmen eine Geschäftsbeziehung einzugehen?
- Hat das Unternehmen einen Einfluss auf das Vertrauen der Kunden? Wie wird hier Einfluss genommen? Genau: welche Massnahmen werden ergriffen?
- Einschätzung: Reflektieren Kunden den Umgang mit ihren Daten? Stellt der Datenschutz ein Anliegen der Kunden dar?
- Wie reagiert das Unternehmen auf Sorgen oder Bedenken der Kunden?
- Bürger zeigen gelegentlich grosse Zurückhaltung, ihre Daten dem Staat anzuvertrauen? Sind Privatunternehmen hier in einem Vorteil? Warum?

## B: LEITFADEN NUTZER-BEFragung

- Wie oft nutzen Sie das Internet? (täglich / mehrmals die Woche / einmal die Woche / seltener)
- Arbeiten Sie beruflich mit dem Internet? Nutzen Sie das Internet privat? (Verhältnis?)
- Nutzen Sie [z.B. Online-Banking/Social Networks/eCommerce/...]?
  - Konkret: welchen Anbieter? Warum haben Sie diesen Anbieter gewählt? Wie sind Sie auf ihn gekommen? Warum haben Sie ihn anderen Anbietern vorgezogen?
- Wie verlief der Anmeldeprozess? Mussten für Ihr Empfinden viele persönliche Daten angegeben werden?
  - Hatten Sie hier Bedenken? Warum?
  - Welche Daten wurden konkret erfragt? Welche davon wurden als heikel empfunden?
  - Haben Sie die Datenschutzbestimmungen des Anbieters gelesen? Warum?
- Für wie sicher halten Sie Transaktionen im Internet? Warum?
- Wie schützen Sie Ihre persönlichen Daten im Netz?
- Welche Internet-Anbieter schätzen Sie als besonders vertrauenswürdig ein? Warum?
  - Worauf achten Sie, wenn Sie die Vertrauenswürdigkeit eines Anbieters beurteilen?
  - Gibt es Anbieter, die Sie bewusst nicht nutzen, weil Sie ihnen nicht vertrauen? Warum?
- [Hinweis auf sorglosen Umgang mit persönlichen Daten in Sozialen Medien.]  
Warum glauben Sie, verhalten sich manche (jüngere) Nutzer so sorglos?
- Haben Sie schon einmal vom neuen Personalausweis gehört? [Ggfls. Erklärung]
- Halten Sie so ein Angebot für sinnvoll/nützlich? Könnten Sie sich vorstellen, es selbst zu nutzen? Warum?
- Angaben zu Geschlecht, Alter, Beruf und Bildungsabschluss.

## C: FRAGEBOGEN DER ONLINE-UMFRAGE

Anfang

Herzlich Willkommen!

Diese Umfrage wird durchgeführt durch die Universität St. Gallen (Schweiz). Unsere Studie soll herausfinden, wie im Internet das Vertrauen der Nutzer entsteht. Alle Antworten sind anonym und werden vertraulich behandelt. Die Umfrage dauert ca. 10 Minuten.



Wir danken Ihnen sehr für Ihre Teilnahme!

Quoten

Zum Einstieg benötigen wir wenige statistische Angaben zu Ihrer Person.

**Geschlecht:**

Weiblich

Männlich

**Alter:**

Bitte auswählen  
 bis 15  
 16-25  
 26-45  
 46-65  
 66 +

**Höchster Bildungsabschluss:**

Noch in schulischer Ausbildung

Beruflehre

Sonstige

Hauptschulabschluss

Abitur / Fachabitur

Realschulabschluss

Fachhochschule / Studium

**Erwerbstätigkeit:**

Angestellt (Vollzeit / Teilzeit)

In Ausbildung / Lehre

Selbstständig erwerbstätig

in Rente

Arbeitsuchend

Hausfrau / -mann

keine Angabe

**Branche:**

Automobil / Luftfahrt / Schifffahrt

Kommunikation / Medien

Bauwesen / Infrastruktur

Landwirtschaft / Bergbau

Beratung / Recht

Maschinenbau

Energie / Umwelt / Recycling

Medizin / Pharma / Chemie

Finanzen / Versicherung / Immobilien

Nahrungs- und Genussmittel

Gesundheits- & Sozialwesen

Öffentlicher Dienst

Gross- und Einzelhandel

Tourismus / Gastgewerbe / Kultur / Sport

Informations- & Kommunikationstechnologien / Elektronische Geräte

Transport / Logistik

Sonstiges



## Einstieg - 2

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich habe keine Bedenken, Online-Transaktionen durchzuführen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manchmal fühle ich mich unsicher, wenn ich im Internet meinen Interessen nachgehe.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online-Anbieter übervorteilen normalerweise ihre Kunden nicht.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online-Anbieter behandeln Ihre Kunden grundsätzlich anständig.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es gibt genug Sicherheitsmechanismen im Internet, damit ich es bedenkenlos für meine persönlichen Interessen nutzen kann.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich vertraue darauf, dass mich rechtliche Rahmenbedingungen vor Problemen im Internet bewahren.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich vertraue darauf, dass mich technische Anwendungen vor Problemen im Internet bewahren (z.B. Verschlüsselungen).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Im Allgemeinen ist das Internet eine stabile und sichere Umgebung, um persönlichen Interessen nachzugehen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Im Allgemeinen habe ich Vertrauen zu anderen Menschen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich verlasse mich meistens auf andere Menschen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Im Großen und Ganzen habe ich Vertrauen in die Menschheit.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin der Meinung, dass Menschen generell zuverlässig sind.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Im Allgemeinen vertraue ich anderen Menschen, außer es gibt Gründe, dies nicht zu tun.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Einstieg - 3

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich kann mir relevante Informationen im Internet beschaffen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich kann abschätzen, welche Informationen im Internet zuverlässig sind.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich vertraue meiner Fähigkeit, die Qualität einer Website einzuschätzen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin in der Lage, ein Profil in einem Sozialen Netzwerk anzulegen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin in der Lage, ein Video im Internet zu publizieren (z.B. auf Youtube).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin in der Lage, Informationen auf einem Blog oder bei Twitter zu veröffentlichen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich kann meine Gedanken und Ideen im Internet mitteilen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich bin in der Lage, einen Beitrag auf Wikipedia zu erstellen oder zu ergänzen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich interessiere mich für neue Entwicklungen im Internet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich probiere gerne neue Online-Plattformen und Applikationen aus.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2. Teil Vertrauensfaktoren

Denken Sie an den letzten Online-Anbieter, bei dem Sie sich als Nutzer registriert haben, wobei die Anmeldung die Eingabe einiger persönlicher Daten erforderte (z.B. für das Anlegen eines persönlichen Nutzer-Profiles).

Um welche Art von Online-Angebot handelte es sich dabei? Bitte wählen Sie aus der folgenden Liste:

- Online-Shopping (z.B. Amazon, eBay, Lufthansa)
- Online Banking (z.B. Comdirect, Postbank, PayPal)
- Soziale Netzwerke / Online-Community (z.B. Facebook, Xing, Parship)
- Online-Information (z.B. Google, Zeitungen, Blogs, eMail, YouTube)

Bitte nennen Sie den Anbieter, an den Sie denken:

Wie schätzen Sie den von Ihnen ausgewählten Anbieter ein?

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Wohltuend	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kompetent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ehrlich	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zuverlässig	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vertrauenswürdig	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sympathisch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich werde die Dienste des gewählten Anbieters in den nächsten 3 Monaten erneut in Anspruch nehmen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2. Teil - 1

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Es ist gut erkennbar, welche Verpflichtungen ich eingee (z.B. Kosten).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Allgemeinen Geschäftsbedingungen sind leicht zu finden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter verfügt über strikte Datenschutzrichtlinien.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter bietet viele Informationen über das eigene Unternehmen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z.B. Garantien, Rückgaberecht).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Umfang der abgefragten Daten steht in einem passenden Verhältnis zum Nutzen, den mir der Dienst bietet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter bietet mir genau was ich suche.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Datenschutzbestimmungen sind leicht verständlich.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich empfinde die abgefragten Daten nicht als heikel oder zu persönlich.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Datenschutzbestimmungen sind leicht zu finden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2. Teil - 2

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Links sind gut kenntlich gemacht.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter hat bereits viele Kunden bzw. Nutzer.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es handelt sich um einen bekannten Anbieter.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter existiert schon eine Weile.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Seite des Anbieters ist einfach und übersichtlich gestaltet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter ist führend in seinem Bereich.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich fühle mich auf der Seite wohl.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Das Design des Anbieters wirkt seriös und professionell.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2. Teil - 3

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Es kommt nicht zu technischen Fehlern	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich kenne das Unternehmen auch ausserhalb des Internets.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Seite lädt schnell.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter besitzt Filialen, die ich aufsuchen kann.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Informationen über den Anbieter sind einfach zu finden (z.B. Grösse, Mitarbeiter, Geschichte).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Kundendienst ist einfach erreichbar.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich kann erkennen, dass der Anbieter seine Systeme gut vor fremden Eingriffen schützt (z.B. durch Verschlüsselung).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Seite des Anbieters stürzt nicht ab.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Kontaktdaten des Anbieters sind einfach zu finden (z.B. Adresse, Telefonnummer).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Büros des Anbieters werden auf einem Foto gezeigt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Kundenservice des Anbieters ist freundlich.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, eMail, Adresse).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2. Teil - 4

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Der Anbieter wurde mir von einem Bekannten empfohlen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter wird von anderen Nutzern positiv eingeschätzt (Ratings).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z.B. Stiftung Warentest).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich habe keine negativen Berichte über den Anbieter in der Presse gelesen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter wird bei Suchmaschinen (z.B. Google) als eine der ersten Seiten aufgelistet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 3. Teil: Persönliche Daten

**Zum Abschluss: Welche der folgenden Daten mussten Sie angeben, als Sie sich beim genannten Anbieter angemeldet haben?**

- |  |  |
|--|--|
| <input type="checkbox"/> Vor- und Nachname     | <input type="checkbox"/> Beruf                               |
| <input type="checkbox"/> User-Name / Pseudonym | <input type="checkbox"/> Branche                             |
| <input type="checkbox"/> Geschlecht            | <input type="checkbox"/> Zivilstand                          |
| <input type="checkbox"/> Strasse & Hausnummer  | <input type="checkbox"/> Sexuelle Orientierung               |
| <input type="checkbox"/> Postleitzahl / Ort    | <input type="checkbox"/> Einkommensdaten                     |
| <input type="checkbox"/> Telefonnummer         | <input type="checkbox"/> Bankverbindung (Kontodaten)         |
| <input type="checkbox"/> eMail                 | <input type="checkbox"/> Kreditkarten                        |
| <input type="checkbox"/> Geburtsdatum          | <input type="checkbox"/> ID / Passnummer                     |
| <input type="checkbox"/> Geburtsjahr/Alter     | <input type="checkbox"/> Kontaktdaten von Freunden/Bekanntem |
| <input type="checkbox"/> Bildungsabschluss     | <input type="checkbox"/> Fotos                               |

## DAS INSTITUT FÜR MEDIEN- UND KOMMUNIKATIONS-MANAGEMENT (MCM), UNIVERSITÄT ST. GALLEN

Das =mcm*institute* ist ein international ausgewiesenes Forschungs-, Qualifikations- und Beratungszentrum für Medien- und Kommunikationsmanagement sowie für Medien und Kultur. Wir unterstützen Studierende, Forscher und Entscheider in Wirtschaft und Gesellschaft, den Herausforderungen des digitalen Zeitalters gerecht zu werden. Das =mcm*institute* setzt sich aus den vier Lehrstühlen Communications Management, Corporate Communications, Culture and Media sowie Social Media and Mobile Communications zusammen.



*Abbildung 16: Das Team des Lehrstuhls MCM2*

Der Lehrstuhl für Corporate Communications (MCM 2) des =mcm*institute* verbindet in seiner Forschungs- und Lehrtätigkeit Aspekte des strategischen Managements mit der Organisationskommunikation - und denkt aus dieser Perspektive vor, wie die Kommunikationsarbeit von Organisationen auf die Herausforderungen neuer Medien und neuer Mediennutzungen reagieren kann.

Der Lehrstuhl MCM 2 hilft mit seinen Forschungsergebnissen jene Fragen zu beantworten, die Führungskräfte in Wirtschaft, Politik und Gesellschaft bewegen. Unsere Forschungs- und Beratungsprojekte zielen dabei zum einen auf die klassischen Felder des Kommunikationsmanagements, wie etwa Unternehmenswahrnehmung und Reputation, Investor Rela-

tions, Interne Kommunikation und Public Affairs. Zum anderen werden die neuen Entwicklungen und Zukunftsfelder der Organisationskommunikation analysiert, die insbesondere durch die neuen Sozialen Medien vorangetrieben werden. Nicht zuletzt widmen wir uns auch der Wahrnehmung und Resonanz der Organisationskommunikation in den klassischen Medien, die auch in einem dynamischen Umfeld nicht an Relevanz einbüßen.