SOZIOLOGISCHES INSTITUT DER UNIVERSITÄT ZÜRICH

Vertrauensbildung im Internet

Caroline Weinzinger
cweinzinger@bluewin.ch

Aarau, September 2004

Inhaltsverzeichnis

1. Einleitung

Vertrauen zu schenken, ist eine Handlung, die meist wenig bewusst abläuft. Man macht sich nur selten aktiv Gedanken darüber, warum jemand vertrauenswürdig ist oder nicht. Auch bleiben im alltäglichen Leben die Gründe dafür, weshalb jemand vertraut, unreflektiert, ebenso wie die Frage nach den Voraussetzungen, die für die Bildung von Vertrauen erfüllt sein müssen. Bei der Entstehung und Verbreitung von neuen Technologien rücken diese Fragen jedoch ins Zentrum der Aufmerksamkeit, schliesslich kann nicht auf routinemässige Vertrauensmuster wie bei lang erprobten und bewährten Verfahren zurück gegriffen werden.

Das Internet bietet hier ein besonders ergiebiges Untersuchungsfeld, da es nicht nur enorme Möglichkeiten zur Partizipation aufweist, sondern auch durch diesen Umfang an Teilnehmern und den hohen Grad an Anonymität, einschränkende Gesetze und Regeln nur in begrenztem Rahmen durchsetzbar sind. In einem solchen fast gesetzlosen Raum wird die Bildung von Vertrauen zur Notwendigkeit – und zugleich zur Unmöglichkeit. Mit der Angst vieler Teilnehmer vor emotionalem oder materiellem Schaden ist erklärbar, warum das Internet zwar stetig wächst, jedoch noch nicht alle Möglichkeiten ausschöpfen kann, die in ihm schlummern. Weder werden Verträge vollständig über das Internet geschlossen, noch werden grössere Summen in reine Online-Geschäfte investiert, der Rückgriff auf reale Kontakte scheint immer noch von Nöten zu sein. Der Umweg über Postversand und persönliche Treffen kostet nicht nur Geld sondern auch Zeit.

In meiner Arbeit soll in einem ersten Schritt der Vertrauensbegriff theoretisch hinsichtlich seiner Funktion und den notwendigen Voraussetzungen beleuchtet werden. Diese Erkenntnisse sollen in einem zweiten Teil auf die Probleme angewendet werden, denen dieses Medium bei der Bildung und Aufrechterhaltung von Vertrauen begegnet. Dabei werde ich aufzeigen, welche Hürden sich im Internet bezüglich der Entstehung von Vertrauen stellen, welche Lösungsansätze sich bisher bewähren und welche Lösungen besonders in Zukunft dem Internet zu einem umfassenden Durchbruch in Kommunikation und Wirtschaft verhelfen können.

2. Theoretischer Hintergrund

2.1 Funktion von Vertrauen

2.1.1 Luhmann: Komplexitätsreduktion

Im Zusammenhang mit der Konzeptualisierung von Vertrauen ist an erster Stelle Niklas Luhmann zu erwähnen, der die Hauptfunktion von Vertrauen in der Reduktion von Komplexität sieht. Die Notwendigkeit von Komplexitätsreduktion wird umso bedeutsamer, je weiter entwickelt eine Gesellschaft ist. Sobald ein Einzelner nicht mehr alle Tätigkeiten der Gemeinschaft ausüben kann, ist er darauf angewiesen, anderen zu vertrauen, damit eine Arbeitsteilung möglich wird. „In dem Masse, als eine Sozialordnung komplexer und variabler wird, verliert sie als Ganzes den Charakter der Selbstverständlichkeit, der bekannten Vertrautheit [...]. Andererseits ergibt sich aus der Komplexität der Sozialordnung selbst ein gesteigerter Koordinationsbedarf und damit ein Bedarf für Festlegung der Zukunft, also ein Bedarf für Vertrauen [...]." (Luhmann 1968: 18) Da äussere Sicherheit in diesem Fall nicht mehr möglich ist, erfolgt eine Verlagerung nach „innen": Subjektive Gewissheit darüber, welche der Handlungsalternativen ein anderes Individuum wählen wird, ersetzt das sichere Wissen über das einzig mögliche Handeln, das in einer einfacheren Gesellschaft noch möglich ist. „Vertrauen erzeugt also subjektive Sicherheit, wo objektiv Unsicherheit herrscht."(Albach 1980, zit. nach Brinkmann/Seifert 2001: 24)
Interne Prozesse „arbeiten selektiv, indem sie für das System relevante Verhältnisse zwischen Umweltdaten als Information aufnehmen und verarbeiten." (Luhmann 1968: 24) Da innere Prozesse nicht alle Informationen verarbeiten können, muss ein Problem vereinfacht werden. Bei der Vertrauensproblematik geschieht dies durch Indifferenz und Generalisierung. Bei Indifferenz „schliesst [man] durch Vertrauen gewisse Entwicklungsmöglichkeiten von der Berücksichtigung aus. Man neutralisiert gewisse Gefahren, die nicht ausgeräumt werden können, die aber das Handeln nicht irritieren sollen." (Luhmann 1968: 23) Mit Generalisierung ist einerseits gemeint, dass in der Familie oder im sozialen Umfeld gelerntes Vertrauen auf neue Situationen und Personen verallgemeinert werden kann. Andererseits erfolgt diese Generalisierung durch symbolische Fixierung, dabei werden Einzelerlebnisse als Stichprobe für das ganze System herangezogen. Somit werden ständig Indizien für die Vertrauenswürdigkeit einer Person oder einer Organisation kontrolliert. Sind diese befriedigend, wird vertraut. Geben sie Hinweise auf einen Vertrauensmissbrauch, wird dem gesamten System das Vertrauen entzogen. (vgl. Luhmann 1968: 27f)

Ausserdem erfolgt das Schenken von Vertrauen in kleinen Schritten. Erst werden kleine Vertrauensvorschüsse gewährt, später, wenn sich das Vertrauen bewährt hat, lässt sich das Individuum auf grössere Risiken ein und tätigt höhere Investitionen.(vgl. Luhmann 1968: 41)

2.1.2 Bornschier: Innovationsförderung

Während Luhmann den Zweck von Vertrauen darin sieht, dass das Individuum in einer komplexen Umwelt zurechtkommen kann, erkennt Bornschier im Vertrauen eine notwendige Voraussetzung für die Entstehung einer solchen Umwelt. Erst ein Umfeld mit gewissem Grundvertrauen ermöglicht die Akzeptanz und Übernahme von Innovationen, deren Wert erst in näherer oder ferner Zukunft abgeschätzt werden kann, und die daher einen grossen Unsicherheitsfaktor in sich tragen. „Der durch Vertrauen hinzugewonnene Handlungsspielraum [...] begünstigt [...] das Ausprobieren von unkonventionellen Handlungen, die notgedrungen jenseits von Sicherheit bietenden gesellschaftlichen Routinen stattfinden müssen. Vertrauen ist essenziell für diese Unsicherheitsbewältigung, die beim Umgang mit Neuem geleistet werden muss." (Bornschier 2001: 237) Diese Überlegung wird durch empirische Ergebnisse gestützt: „Die kulturelle Ressource generalisiertes Vertrauen, gemessen mit unserem Index Vertrauen und Toleranz, hat nach unseren Ergebnissen einen nachweisbaren Einfluss auf die frühe Verbreitung der neuen Technologie des Internets." (Bornschier 2001, 253) Neben der Bewältigung von Unsicherheit, kann Vertrauen auch zur Kostenreduktion bei der Entwicklung und Verbreitung neuer Technologien beitragen: „Theoretically, it is argued that generalized trust functions as a cultural resource, which makes economic exchange and transactions more productive by allowing for more, and more encompassing, actions (networking), by reducing transaction costs and costly controls as well as enhancing the flow of information." (Volken 2002: 1) Volken argumentiert, dass in einer neuen technologischen Umgebung Unsicherheiten bestehen, da niemand auf bereits entwickelte und erprobte Praktiken oder institutionelle Arrangements zurückgreifen kann. Vertrauen kann in diesem Umfeld Kosten reduzieren, die ansonsten für Überwachung, Kontrolle und die Durchsetzung von Sanktionen anfallen. Die freigewordenen Mittel können produktiv genutzt werden. „Trust as a cultural resource raises the overall innovative capacity of a social system, since it allows economic and also political agents to take advantage of their extended potential for action." (Volken 2002: 3)

2.2 Voraussetzungen für Vertrauen

Luhmann nennt vier Voraussetzungen, von denen mindestens eine erfüllt sein muss, damit Vertrauen entstehen kann. (vgl. Luhmann 1968: 31ff)

Denkbar ist erstens, dass eine Form von Vertrautheit mit der betreffenden Person besteht. „Dem Vertrauten traut man eher als dem Fremden" (Luhmann 1968: 31). Meist bleiben solche Vertrauensbeziehungen unreflektiert und würden einer rationalen Prüfung der Vertrauenswürdigkeit kaum standhalten. Immerhin genügt Vertrautheit, um eine subjektive Sicherheit zu entwickeln, dass das eigene Vertrauen nicht ausgenützt wird.

Das Risiko eines Vertrauensmissbrauchs kann, zweitens, minimiert werden, wenn die Motivationsstruktur der anderen Person bekannt ist. Dies erfolgt mittels einer einfachen Gewinn- und Verlustrechnung auf der Basis der Frage: „Würde ein Vertrauensbruch ihm besonders grosse, verlockende Vorteile bieten?" (Luhmann 1968: 32) Damit kann eingeschätzt werden, ob ein Vertrauensbruch einen Gesichtsverlust für diese Person bedeuten würde oder nicht.

Ausserdem stellen, drittens, offizielle oder latente Sanktionsaussichten einen gewissen Schutz vor Betrug dar. „In sozialen Zusammenhängen, die so strukturiert sind, nämlich durch relative Dauer der Beziehung, wechselnde Abhängigkeiten und ein Moment der Unvorhersehbarkeit ausgezeichnet sind, findet man einen günstigen Nährboden für Vertrauensbeziehungen. Es herrscht das Gesetz des Wiedersehens. [...] Das erschwert Vertrauensbrüche [...]." (Luhmann 1968: 35)

Zuletzt ist auch ein Umfeld zentral, dessen Moralvorstellungen klar abgrenzen, wo Naivität endet und ein Vertrauensbruch beginnt. Wichtig dabei ist zu wissen, „auf welcher Seite im Falle des Vertrauensbruches unbeteiligte Dritte stehen werden, ob und wie sehr sie den Vertrauensbrecher für schuldig oder den Vertrauenden für naiv oder töricht halten werden. [...] Die Typizität und Voraussehbarkeit solcher Schuldzurechnungen ist ebenfalls eine wesentliche Hilfe bei der Vertrauensentscheidung, ermöglicht sie es dem Vertrauenden doch, vorauszusehen, ob er nur den Schaden oder auch den Spott dazu riskiert." (Luhmann 1968: 36) Durch klare Moralvorstellungen wird der Einzelne davon entlastet, für das Schenken von Vertrauen die volle Verantwortung zu tragen.. (vgl. Luhmann 1968: 36)

Die Entscheidung, ob vertraut wird, gründet sich daneben auf vielfältige Soll-Erwartungen. „Identifiziert wurden drei Erwartungsdimensionen, die Akteure an VertrauensempfängerInnen richten: eine situationsspezifische Kombination von Kompetenz, Integrität und Gesinnung" (Brinkmann/Seifert 2001: 24). Voraussetzungen für Vertrauen sind also auf einer weiteren Stufe die Hoffnung darauf, dass das Gegenüber fähig, zuver-

lässig und willens ist, dem in es gesetzten Vertrauen gerecht zu werden. Diese Erwartungen sind ihrerseits jedoch bereits wieder ungesicherte Vertrauensakte, die sich auf Luhmanns Grundkomponenten stützen.

3. Dilemmasituation im Internet

Bei genauerer Betrachtung der Funktionen und Voraussetzungen von und für Vertrauen zeigt sich, dass das Internet im Verhältnis dieser beiden Grössen zueinander in ein Dilemma gerät: Einerseits ist gerade das Internet als neue Technologie auf viel Vertrauensvorschuss angewiesen, damit es sich entwickeln kann. Andererseits erfüllt es kaum die wichtigsten Voraussetzungen, die für einen Vertrauenserwerb nötig wären. Im folgenden soll auf diese beiden Aspekte eingegangen werden.

3.1 Notwendigkeit für Vertrauen im Internet

Das Internet bietet fast unbegrenzte Möglichkeiten, eigene Bedürfnisse zu befriedigen. Das Spektrum reicht vom Erwerb von Waren und Dienstleistungen bis hin zum Erhalt eines bestehenden oder sogar Aufbau eines neuen sozialen Umfelds. Der eigene Computer erlaubt die Teilhabe an einer der realen Umwelt fast äquivalenten Gesellschaft. Dennoch unterscheiden sich die zwei Erlebnissphären in den zentralen Dimensionen von Ort und Zeit: Weder sind die Kommunikationspartner üblicherweise in der Lage, sich persönlich kennenzulernen, somit bleibt Identität und Herkunft des Gegenübers meist unklar oder doch schwer nachprüfbar, noch bildet die zeitliche Dimension eine fixe Konstante im Internet. Letzteres betrifft die Datierung von Dokumenten ebenso wie das zeitliche Auseinanderfallen von Güterübergabe und Bezahlung. Dadurch müssen Interaktionspartner sich gegenseitig einen grosszügigen Vertrauensvorschuss gewähren. „Sicherheit bietende gesellschaftliche Routinen“ (Bornschier 2001: 237) fehlen im Internet noch weitgehend, zumal es sich beim *World Wide Web* um einen in weiten Teilen (noch) rechtsfreien Raum handelt: Durch den hohen Grad an Anonymität ist eine strafrechtliche Verfolgung von Betrügern schwerer oder gar nicht möglich und da man die Identitäten beliebiger Individuen vortäuschen kann, ist auch der Nachweis einer Straftat bei einer bestimmten Person kaum zu erreichen. Kontroll- und Sanktionsmechanismen und -instanzen fehlen also weitgehend.

Das Problem der Unsicherheit liegt aber bereits in der Komplexität der Technik: Da nur wenige Spezialisten den technischen Hintergrund genau genug kennen, um sich vor Viren und Indiskretionen die eigenen Daten betreffend selbst schützen zu können, ist die Mehrheit der Benutzer auf teure Programme zum eigenen Schutz oder grosses Vertrauen in das Funktionieren der Technik angewiesen. Aufgrund dieses Mangels an äusseren Sicherheiten wird die Bedeutung von Vertrauen in der Internetkommunikation sehr zentral. Nach Luhmann dient Vertrauen dazu, mangelnde äussere Sicherheit, durch den Aufbau von innerer Sicherheit auszugleichen, was Transaktionen im Internet erst ermöglicht.

3.2 Voraussetzungen für Vertrauen im Internet

Obwohl Vertrauen die Grundbedingung für eine weitreichende Ausbreitung des Internet darstellt, werden die Voraussetzungen, die Luhmann für die Bildung von Vertrauen nennt, gerade im Internet noch weniger erfüllt als im realen Leben.

So ist Vertrautheit mit einer Person im Internet schwerer aufzubauen als im realen Leben, wie Untersuchungen in virtuellen Teams belegen: Frühe Theorien vertraten die Ansicht, dass im Internet der Aufbau von Vertrauen im Internet ohne face-to-face Kontakte gar nicht möglich ist. „These theories suggest that computer-based communication media may eliminate the type of communication cues that individuals use to convey trust, warmth, attentiveness, and other interpersonal affections." (Jarvenpaa/Leidner 1998: 5) Empirische Studien zeigen allerdings, dass solche *sozialen Informationen*, die in direkten, persönlichen Kontakten mit Mimik, Gestik oder Stimmmodulation übertragen werden, auch über Geschriebenes – folglich durch den Computer – weitergegeben werden können, ihre Transferrate allerdings verlangsamt ist. Ergebnisse anderer Studien deuten sogar darauf hin, dass Internet-Beziehungen intensiver sein können als reale: „Walther found that social discussion, depth, and intimacy were greater in computer-mediated communication groups than in face-to-face groups, even for groups with geographically dispersed and culturally diverse partners who had never met face-to-face." (Walther 1995 und 1997 zit. nach Jarvenpaa/Leidner 1998: 5f) Die SIDE-Theorie (Social Identification/Deindividuation Theory von Lea und Spears 1992 zit. nach Jarvenpaa/Leidner 1998: 5f) argumentiert, dass auf Grund der geringen Anzahl von Informationen das Individuum sich stereotype Eindrücke einer Gruppe macht. Wenn sich eine Person durch die eigene Selbst-Kategorisierung einer Gruppe zugehörig fühlt, werden die Kommunikationspartner idealisiert, was die Motivation zu kooperieren erhöht. Daher ist es nicht überraschend, dass, wenn ein Team sehr verschiedene Charaktere beinhaltet, die Stereotypenbildung

erschwert ist. „Yet, the greater the team member diversity, the more time will be required for team members to form strong bonds." (Jarvenpaa/Leidner 1998: 5)

Auch die übrigen Voraussetzungen nach Luhmann sind schwerer erfüllbar im Internet. Das Umfeld und dessen Moralvorstellungen sind für neue Mitglieder langsamer erkennbar. Ebenso fehlen durch den Mangel an persönlichem Kontakt und die oft kurze Dauer der gegenseitigen Beziehungen die Grundlagen zur Einschätzung der Motivationsstruktur des Gegenübers.

Erschwerend kommt hinzu, dass es sich beim Internet – wie erwähnt – um einen rechtlich schwer zu kontrollierenden Raum handelt. Dadurch sind Sanktionen für Fehlverhalten kaum durchsetzbar, geschweige denn bei Dritten einklagbar.

Es zeigt sich also, dass Vertrauen für die Beteiligung an Transaktionen im Internet eine notwendige Voraussetzung ist. Allerdings wird der Aufbau von Vertrauen durch den Mangel an Sicherheiten und Informationen verlangsamt und erschwert. Um alle Möglichkeiten dieser neuen Technologie nutzen zu können, ist eine Lösung dieser Dilemmasituation unerlässlich. Bisher existieren jedoch nur Insellösungen für dieses Problem, die im kommenden Kapitel genauer beleuchtet werden sollen. Sie erweisen sich zwar für die momentanen Belange als sehr wirkungsvoll, jedoch weisen sie zahlreiche Lücken auf, die einer umfänglicheren Benutzung des Internets – besonders in wirtschaftlicher Hinsicht – entgegenwirken. Auf vertrauensstiftende Mechanismen, die diese Lücken füllen können, soll später eingegangen werden.

4. Vetrauensproblematik in verschiedenen Bereichen des Internet

Die Probleme, die sich Ustern im Internet bei der Vertrauensbildung stellen, können je nach Bereich sehr unterschiedlich sein. Während in virtuellen *Communities* vor allem die Angst vor emotionalen Schädigungen wie Blossstellungen, Spott oder Ausnutzung im Vordergrund steht, geht es bei elektronischen Auktionen oder im e-Business eher um materielle Schäden, die durch einen Vertrauensmissbrauch entstehen könnten. Im folgenden Kapitel sollen nicht nur die Schwierigkeiten, die sich in der Vertrauensbildung in verschiedenen Bereichen des *World Wide Web* stellen, beleuchtet, sondern auch die Notwendigkeit von Vertrauen in den jeweiligen Umgebungen aufgezeigt werden.

4.1 Communities

Online-Communities bieten auf vielfältigste Weise Möglichkeiten für einen Vertrauensmissbrauch: Fehlinformationen von kompetent wirkenden Gesprächspartnern können Probleme von Ratsuchenden massiv verstärken. In Gruppen, die sehr persönliche Themen behandeln, kann der Spott eines *Trolls*[1], sehr verletzend sein. „Trolls can be costly in several ways. A toll can disrupt the discussion on a newsgroup, disseminate bad advice, and damage the feeling of trust in the newsgroup community." (Donath 1996: 15) Vermehrte Enttäuschungen dieser Art könnten dazu führen, dass Online-Foren generell gemieden werden, was den Interessen der Betreiber solcher Seiten entgegen liefe, die nur durch hohe Besucherfrequenzen Werbeeinnahmen oder Benutzergebühren generieren können.

4.2 eBay

Auf Plattformen wie eBay können Private Waren anderer Privatleute ersteigern oder eigene Waren versteigern. Teilnehmern und Teilnehmerinnen von eBay oder ähnlichen Auktionsforen im Internet stellen sich auf zwei Ebenen Vertrauensprobleme: „Zunächst müssen die ‚User' den technischen Sicherheitsstandards des Online-Verkehrs vertrauen. Sie müssen sich beispielsweise darauf verlassen können, dass ihre Kreditkartennummer oder andere persönliche Daten Unbefugten nicht zugänglich sind. [...] Die Internet-Auktionäre müssen einander vertrauen, da die Auktion örtlich und zeitlich zergliedert ist (fehlende Kopräsenz). Anders als zum Beispiel im Supermarkt begegnen sich Verkäufer und Käufer nicht. Die Transaktion muss ohne face-to-face-Absicherung auskommen, Käufer und Verkäufer sind einander in der Regel völlig fremd und besitzen keine eigenen Erfahrungen mit der Vertrauenswürdigkeit des jeweils anderen." (Brinkmann/Seifert 2001: 28) Der Tauschhandel ist durch „Anonymität und Einmaligkeit charakterisiert [...]. Verkäufer und Käufer können eine ‚virtuelle Identität' annehmen, mit Fantasienamen und Scheinadressen auftreten [...]".(Diekmann/Wyder 2002, 675) Neben dieser mangelnden örtlichen Kopräsenz ist vor allem das zeitliche Auseinanderliegen des Warenerhalts und dessen Bezahlung eine Schwierigkeit, die augenblicklich nur mit Vertrauen überwunden werden kann. Daher versuchen die Betreiber von eBay möglichst viele vertrauensstiftende Institutionen zur Verfügung zu stellen, von denen ihre Kunden profitieren können. Ganz

[1] „Trolls" werden Personen genannt, die in Chat-Foren nicht ernstgemeinte, meist beleidigende Kommentare hinterlassen und sich an der entstehenden Verwirrung und verletzten Reaktionen der Getäuschten ergötzen. (vgl. Donath 1996: 15)

eliminieren lassen sich Vertrauensbrüche dennoch nicht. EBay meldet allerdings, dass „bei zwei Millionen Auktionen im Zeitraum Mai bis August 1997 gerade 27 Betrugsfälle gemeldet wurden." (Diekmann/Wyder 2002, 675) Diese Zahl ist sehr gering, was dem Vertrauen in das Auktionshaus zu Gute kommt.

4.3 e-Business

Studien zeigen, dass „[...]nur 20-25% derjenigen Personen, die online sind, auch online einkaufen."(Czurda/Dietschi/Wunderli 2000: 816) Die Ängste, die hinter diesem geringen Anteil stehen, sind in Vertrauensdefiziten zum Medium Internet zu suchen. Nicht nur die Sorge über einen möglichen Betrug oder die Ungewissheit über die Qualität der erworbenen Ware steht dabei im Vordergrund, sondern auch die Identitätsproblematik: Einerseits fürchten potenzielle Käufer, dass ihre privaten Daten und Transaktionen durch das Internet publik werden könnten, andererseits vermissen sie die Transparenz bezüglich der Personen, mit denen sie in geschäftlichen Kontakt treten.

Auch bei Geschäftsbeziehungen zwischen Unternehmen im Internet kann eine mangelnde physische Präsenz Schwierigkeiten bereiten. Darauf deuten unter anderem auch die Ergebnisse einer Studie[2] im Bereich des E-Procurement[3] hin: „66 Prozent [...] der Unternehmen ziehen es vor, Internetgeschäfte nur mit solchen Unternehmen abzuwickeln, die auch eine physische Präsenz vorweisen können und nicht nur im Netz vorhanden sind." (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 9) Nur bei Firmen, die bereits Vertrauen geniessen, bereitet die Sicherheitsthematik keine Diskussionen. „Die Unternehmen gewähren grossen und bekannten Marken einen Vertrauensvorschuss und sind bei unbekannten Online-Anbietern misstrauisch." (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 9) Bestehendes Vertrauen kann also Kosten reduzieren, die ansonsten in Bemühungen investiert werden müssten, die Sicherheit zu maximieren und zu kommunizieren: „Auch greifen 64 Prozent der europäischen Unternehmen noch immer auf unzureichende und überholte Sicherheitstechnologien wie z.B. Passwortlösungen zurück. [...] Lediglich 27 Prozent der Unternehmen verlangen digitale Authentizitätszertifikate als Identitätsnachweis." (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 13) Für die

[2] Alle Daten stammen aus einer Untersuchung, in der im Mai 2000 415 Entscheidungsträger europäischer Unternehmen in Deutschland, Frankreich, Grossbritannien und den Niederlanden, deren Jahresumsatz zwischen 15 und 750 Millionen Euro lag, in Interviews befragt wurden.

Steigerung der über das Internet abgewickelten Geschäfte wird es also notwendig sein, Sicherheitsgarantien bereitzustellen, damit auch Vertrauen zu neuen Online-Geschäftspartnern generiert werden kann.

5. Vertrauen stiftende Mittel

In einem zweiten Schritt werden Lösungsansätze präsentiert, wie Unsicherheiten und andere Gründe für Misstrauen minimiert werden können.

5.1 Reputation

Wo eigene Erfahrungen mit einem anderen Interaktionspartner fehlen, können die Beurteilungen Dritter als wichtige Informationsquelle für dessen Vertrauenswürdigkeit dienen.
Bei eBay erfolgt eine Beurteilung von Käufern und Verkäufern durch frühere Handelspartner. Durch die positive, neutrale oder negative Kritik Dritter können potenzielle Käufer leichter abschätzen, ob sie das Risiko eingehen, betrogen zu werden. Diese Kritik erfolgt einerseits mittels der Vergabe von Sternen (zwischen einem und fünf Sternen je nach Zufriedenheit) andererseits mittels verbaler Kommentare. Ausserdem errechnet eBay einen Index, wobei die Anzahl negativer Bewertungen von der Anzahl positiver Bewertungen abgezogen wird.
Auch bei Newsgroups und *Communities* spielt Reputation eine wichtige Rolle. Hier können sich Teilnehmer diese durch regelmässige und inhaltlich wertvolle Kommentare erwerben. Allerdings gehört zu einem guten Ruf auch Klarheit über die Identität des Schreibers. „No matter how brilliant the posting, there is no gain in reputation if the readers are oblivious to whom the author is." (Donath 1996: 2)

5.2 Sanktionen

Bei eBay stellt eine schlechte Reputation bereits eine indirekte Sanktion dar. Während ein Verkäufer mit hohen Reputationswerten seine Waren leichter versteigern kann und dabei auch höhere Preise erreicht (McDonald/Slawson 2000, zit. nach Brinkmann/Seifert 2001: 29), fallen die Verkaufsmöglichkeiten ab, sobald diese Werte sinken. (Brinkmann/Seifert 2001: 37f)

[3] „Electronic Procurement oder E-Procurement bezeichnet Einkaufsaktivitäten über das Internet im Business-to-Business (B2B) Bereich." (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 4)

Daneben werden Seiten wie jene von eBay von ihren Betreibern vor Betrügern geschützt, indem diese nach einer Vorwarnung von der Plattform ausgeschlossen werden (Brinkmann/Seifert 2001: 30) und mit rechtlichen Schritten rechnen müssen. Dabei wird es wichtig, dem virtuellen Individuum eine Person in der realen Welt eindeutig zuordnen zu können. „Die Anmeldung an der Plattform kann dafür nicht herhalten, da die angegebenen Namen („real names") und Adressen nicht vom Plattformbetreiber kontrolliert werden. Deren Prüfung findet erst durch die Transaktionspartner statt." (Brinkmann/Seifert 2001: 31) Dieser Schwachstelle soll in Zukunft Abhilfe mittles Zertifikaten geschafft werden, auf die später noch eingegangen wird, dafür wäre die Zusendung einer Kopie des Personalausweises jedes Teilnehmers erforderlich.(Brinkmann/Seifert 2001: 31)

Auch in *Online-Communities* können Sanktionen verhängt werden: Betroffene können sich an den Systemadministrator wenden, (Donath 1996: 23) der anhand der ihm bekannten Daten Rekurs auf die reale Person nehmen und sie beispielsweise aus einem Chat-Forum ausschliessen kann. Dies ist allerdings nur in solchen Umgebungen möglich, wo Teilnehmende ihre Personalien angeben müssen, um Zugang zu erhalten. Überall, wo Pseudonyme verwendet werden und keine Verbindung zwischen realer und virtueller Person nachweisbar ist, können nur Sanktionen ergriffen werden, die innerhalb des Netzes Benutzer vor weiteren Schäden schützen. Eine Möglichkeit ist die Installation eines *killfiles*, damit gemeint ist ein spezieller Filter, der alle Kommentare der sanktionierten Person auf dem Bildschirm ausblendet. (Donath 1996: 18)

5.3 Versicherung

Bei eBay werden Verluste bis zu 1000 DM, die durch Betrügereien entstehen, von den Betreibern dem Geschädigten ersetzt. Dadurch wird verhindert, „[...] dass das Vertrauen in das Gesamtsystem durch derartige Enttäuschungen unterminiert wird." (Brinkmann/Seifert 2001: 30)

Auch bei Anbietern von Zertifizierungsdiensten (die später behandelt werden sollen) wird laut schweizerischem Recht (die entsprechende Verordnung zur elektronischen Signatur soll am 1. Januar 2005 in Kraft treten) zur Deckung der Haftung ein „Betrag von mindestens 2.5 Millionen Franken pro Versicherungsfall oder 10 Millionen Franken pro Versicherungsjahr" (Bundesamt für Kommunikation 2004: Art. 2) als Versicherung verlangt. Ein staatlich anerkannter Zertifizierungsdienst muss also die Haftung für Missbräuche übernehmen, was in Zukunft das Vertrauen in digitale Signaturen und Zertifikate erheblich stärken wird.

5.4 Informationen und soziale Kontexte

Informationen über die Vertrauenswürdigkeit des Gegenübers können durch einen Rückschluss auf dessen Identität gewonnen werden. So kann bei *Communities* aus dem Namen der Domain in der e-Mail-Adresse herausgelesen werden, ob der Account von einer Universität, einer Firma oder einer beliebigen Privatperson stammt, obwohl diese noch lange keine Garantie dafür leisten, dass ein Absender aus einem Labor wirklich ein Wissenschaftler und nicht zum Beispiel Mitglied des Computer Support Dienstes ist. (Donath 1996: 5) Allerdings bringt sie das virtuelle Gegenüber seiner realen Identität näher, sei es über das Herkunftsland der Adresse (z.B. Thailand oder Israel) oder über den Namen des Unternehmens (z.B. Greenpeace). „And, while there are not yet any recognized ‚wealthy' virtual neigborhoods, it is probably only a matter of time until exclusive on-line addresses become symbols of status." (Donath 1996: S. 5)

Eine Möglichkeit, eine vertrauensstiftende Verbindung zwischen der eigenen virtuellen und realen Identität herzustellen, besteht unter anderem darin, den vollen Namen, Titel, Abteilung und Telefonnummer des Büros preiszugeben. Dieser Schritt ermöglicht es Skeptikern, die Angaben zu verifizieren. Diese sogenannten „business-card signatures" (Donath 1996: 11) sind besonders in technischen Newsgroups üblich. Ähnliche Effekte können durch den Hinweis auf die eigene Homepage erreicht werden. (Donath 1996: 11)

Solche Informationen dienen auch dem „characteristic based trust": „Je grösser die soziale Ähnlichkeit zwischen Vertrauendem und VertrauensempfängerIn, desto stärker unterstellen Akteure, dass ihre InteraktionspartnerInnen die gleichen Hintergrundüberzeugungen teilen, auf die Vertrauen aufbauen kann." (Brinkmann/Seifert 2001: 31) Bei eBay wird diese Vertrauensstütze durch „chat-Foren" gefördert.

Auch beim Handel zwischen Firmen im Internet können Informationen Sicherheit vermitteln. „Internetunternehmen, die nicht auf die Vorteile bereits etablierter Unternehmen zurückgreifen können, müssen stärker in den Sicherheitsbereich investieren und die auch kommunizieren. So kann das Dienstleistungsangebot durch eine Sicherheitsgarantie ergänzt werden." (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 14) Bei bereits etablierten Unternehmen ist eine solche Betonung der Sicherheit nicht mehr nötig.

5.5 Codierung

Die Angst vor dem Missbrauch privater Daten und Informationen, die für Zahlungszwecke oder aus anderen Gründen offengelegt werden müssen, verlangt vielen Leuten einen

grossen Vertrauensakt ab. Daher ist es für Betreiber einer solchen Seite unerlässlich, Daten im Internet vor dem unbemerkten Zugriff Fremder zu schützen. Eine Möglichkeit dafür ist die Verwendung von Codes oder Kennwörtern.

In *Online-Communities* übernehmen diese „Verschlüsselungen" die Teilnehmer selbst, indem sie beispielsweise Codeausdrücke im Absender verwenden. So kann die Verwendung von Programmiersprache Insiderwissen und Zugehörigkeit zu einer Newsgroup im Programmierbereich ausdrücken, das gleiche leisten Fachausdrücke, wie auf einer Motorradseite ersichtlich wird, deren Teilnehmer dem eigenen Namen und e-Mail-Adresse Informationen zum Motorradclub, bei dem sie Mitglied sind, zu den Motorradtypen, die sie besitzen oder besassen, beifügen.(Donath 1996: 14) Allerdings sind auch diese Informationen nicht fälschungssicher. „The account name in the header can be faked, identity claims can be false, social cues can be deliberately misleading." (Donath 1996: 14)

5.6 Trust-Vereinigungen, Zertifikate und Signaturen

Die zwei zentralen Vertrauensprobleme, denen der User im Internet begegnet, sind einerseits die Unsicherheit bezüglich der Identität des Gegenübers und andererseits die fehlenden Garantien für die Zuverlässigkeit und Ehrlichkeit eines Handels- oder Kommunikationspartners.

Der ersten Problematik kann mittels Signaturen Abhilfe geschafft werden: Dabei wird ein „elektronisches Dokument fest mit einer Identität verknüpft." (Engeler 2003: 14) Anders als bei einer Unterschrift auf Papier, wird dabei der gesamte Text mit dem privaten Schlüssel des Absenders codiert. Eine Möglichkeit dafür ist, die Buchstabenwerte erst in Zahlenwerte zu übersetzen und diese Zahlen danach mit einem eigenen, geheimen Code in neue, verschlüsselte Zahlen zu transferieren, die vom Empfänger nur mit Hilfe dieses Schlüssels decodiert werden können. „Im Gegensatz also zur normalen Unterschrift, verändert sich die digitale Unterschrift je nach Textvorlage." (Engeler 2003: 15) Ausserdem wird nicht nur die Identität des Absenders gewährleistet, sondern auch der Inhalt des von ihm verfassten Textes, da jede Änderung in der Zahlenfolge auch eine Abweichung an der entsprechenden Stelle des Textes bewirkt. Allerdings hat die digitale Unterschrift einen Nachteil: „Die persönliche Komponente, welche die Handschrift hat (jede Handschrift hat individuelle Merkmale, quasi wie ein Fingerabdruck), ist bei der digitalen Unterschrift weg. Jeder, der im Besitz des Privaten Schlüssels ist, kann damit unterschreiben und niemand kann nachweisen, dass eine andere Person unterzeichnet hat." (Engeler 2003: 15) Trotz dieser Missbrauchsmöglichkeiten überwiegen die Vorteile der elektronischen

Signatur, die neben Vertrauensgewinnen auch Kosteneinsparungen bewirken kann. So würde sie dazu beitragen, dass SPAM-Mails eliminiert werden könnten, die durch den zeitlichen Aufwand, sie zu löschen, und Speicherplatzverluste hohe Kosten in der Wirtschaft verursachen, „[...] da man sich bereits heute vorstellen kann E-Mail-Clients so zu konfigureren, dass nur E-Mails mit gültiger digitaler Signatur entgegengenommen werden sollen." (Schnellhorn 2003: 3)

Über die Signatur hinausgehend können Zertifikate neben der Garantie für die Herkunft und den unveränderten Inhalt eines Textes auch Garantien für die Identität des Senders liefern: „Digitale Zertifikate sind genaugenommen ein Spezialfall einer digitalen Signatur, nämlich solche, die eine Identität liefern, welche vom Computer überprüft werden kann. Demnach ist ein Digitales Zertifikat ein von einer unabhängigen Instanz unterschriebener Datenblock, der einen Public Key sowie andere Informationen (z.B. Name Email, Staatsangehörigkeit...) enthält." (Schellhorn 2003, 2)

Der Umgang mit digitalen Signaturen und Zertifikaten wird in der Public Key Infrastructure (PKI) geregelt. Dabei handelt es sich um eine Umgebung, in der „genau festgelegt [ist], wer unter welchen Umständen wie Zertifikate unterzeichnet oder sperrt und wie in den unterschiedlichsten Situationen mit den Zertifikaten umgegangen werden muss, damit mit der grösstmöglichen Sicherheit Public Keys einzelnen Individuen zugeordnet werden können." (Schellhorn 2003: 2). Sie ist somit ein den Signaturen und Zertifikaten übergeordnetes Kontrollsystem.

„Heutzutage finden sich PKIs lediglich im B2B [Business-to-Business] oder im internen Geschäftsverkehr." (Engeler 2003: 16) Die Ursache dafür ist darin zu suchen, dass eine zentrale Lösung von Seite der Firmen her zuwenig Nutzer anlockt und daher nicht rentieren kann. „Ein erster Versuch für die Etablierung einer kommerziellen Lösung einer öffentlichen PKI ist zunächst gescheitert. Der von den schweizerischen Banken initiierte Versuch über eine kommerzielle Firma, der Swisskey AG, wurde schon nach rund drei Jahren Betrieb im Jahr 2001 abgebrochen. Insgesamt wurden für dieses Projekt 25 Millionen Schweizerfranken eingesetzt. Im Gegensatz dazu konnten nur rund 9500 Zertifikate für Firmen- und Privatkunden ausgestellt werden." (Engeler 2003: 23)

In der Schweiz werden ab dem 1. Januar 2005 alle Pflichten von Zertifizierungsstellen gesetzlich geregelt, was das Vertrauen von Firmen und Privaten in Zertifikate ausgestellt von akkreditierten Unternehmen stärken könnte. Auch das drängende Problem des rechtlichen Umgangs mit elektronischen Signaturen zu lösen, wird mit dieser Verordnung gelöst. Im

Hinblick auf die Zertifizierungsdienste wird der Ruf der diese Funktion übernehmenden Firmen für das ihnen entgegengebrachte Vertrauen relevant sein, was wiederum darüber entscheiden wird, ob dieses neue Angebot genutzt wird oder Firmen und Private sich weiterhin eher auf persönliche Kontakte und Verträge in Papierform verlassen. So wird in der bereits erwähnten Studie von PriceWaterhouseCoopers festgehalten: „Vertrauen in ein Unternehmen kann auch von externer Seite generiert werden. Grundlegende Voraussetzung dafür ist eine allgemein anerkannte Reputation der externen Institution“ (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 14) „Derzeit geniessen die fünf führenden Prüfungs- und Beratungsgesellschaften (Big Five), die grossen Telekommunikationsgesellschaften sowie die Global Player im Industriesektor das grösste Vertrauen bei der möglichen Übernahme einer Überwachungsfunktion für E-Procurement im B2B-Bereich.“ (PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft 2000: 15)

Im Zuge all dieser Entwicklungen wird in der Schweiz (nach Finnland, Estland und Italien, die in diesem Bereich in der Vorreiterrolle sind) über die Entwicklung einer elektronischen Identitätskarte nachgedacht. Die Zertifizierungsstelle wäre hier der Staat, der seinen Bürgern ermöglichen würde, sich elektronisch registrieren zu lassen, um mit dem so erhaltenen Zertifikat an Wahlen und Abstimmungen teilzunehmen oder auch die administrativen Vorgänge bei einem Wohnsitzwechsel elektronisch abzuwickeln. Eine solche Identitätskarte könnte aber nicht nur für staatliche Belange eingesetzt, sondern auch in die Privatwirtschaft übernommen werden, wo sie zu enormen Kosteneinsparungen (allein durch den Verzicht der einzelnen Unternehmen auf den Aufbau eigener PKIs) führen würde. (Engeler 2003: 24f)

5.7 Probleme bei der Umsetzung von Zertifikaten

5.7.1 Vertrauen in weiche oder falsche Zertifikate

Laut Gesetz muss den Zertifizierungsstellen für die Ausstellung eines Zertifikats ein Identitätsnachweis vorliegen. (vgl. Bundesamt für Kommunikation 2004: Art. 5) Das genügt zwar für eine gültige Unterschrift im Internet, sagt aber wenig über die Vertrauenswürdigkeit des Schüsselinhabers aus. Zwar können weitere Attribute für ein Zertifikat angegeben werden, die z.B. mit einem Handelsregisterauszug bewiesen werden müssen, wie deutlich die Unterschiede zwischen reinem Identitätsnachweis und einem Zertifikat mit zusätzlichen Attributen für den potenziellen Kunden erkennbar sind, muss sich aber erst

weisen. Der alleinige Hinweis auf den Besitz eines Zertifikats, welcher Art es auch sein mag, könnte dazu führen, dass sich unerfahrenere Kunden schnell in falscher Sicherheit wiegen und ihr Vertrauen leichter ausgenützt wird. Eine solche Entwicklung wäre besonders dann zu fürchten, wenn die Zahl der verschiedenen Zertifizierungsstellen und damit der von ihnen ausgestellten Zertifikate so gross wird, dass eine Übersicht und Kontrolle, ob diese Zertifikate wirklich von einer lizenzierten Instanz verliehen wurden, fast unmöglich würde. Ähnliche Probleme stellen sich schon heute in der realen Welt für Kunden, die Gütesiegel für umweltfreundliche Produkte oder Fair-Trade-Labels von nichtssagenden Werbeaufschriften unterscheiden möchten.

5.7.2 Sperren von Zertifikaten

Ein weiteres Problem das sich im Zusammenhang mit Zertifikaten stellt, ist die Transparenz über die Sperrung von Zertifikaten. Zertifikate werden dann gesperrt, wenn der Inhaber eines Signaturschlüssels diesen verliert. In einem solchen Fall „muss sie oder er innerhalb von 24 Stunden die Ungültigerklärung des eigenen Zertifikats veranlassen. Das Gleiche gilt für die Inhaberin oder den Inhaber des Signaturschlüssels, der weiss oder den begründeten Verdacht hat, dass ein Dritter Kenntnis des Passworts erlangt hat." (Bundesamt für Kommunikation 2004: Art. 13) Zwar ist es möglich, Listen von gesperrten Zertifikaten (sogenannte *certificate revocation lists*, kurz: CRL), die in regelmässigen Abständen überarbeitet werden, aus dem Internet herunterzuladen: „Leider wachsen die CRLs bei populären CAs[4] schnell an und verlangen den Nutzern somit längere Downloadzeiten ab. Desweiteren gibt es natürlich einen Zeitraum zwischen dem Sperren und dem Bereitstellen der neuen CRL, in welchem neu gesperrte Zertifikate nicht als solche zu erkennen sind." (Schnellhorn 2003: 5) Eine Lösung dieses Problems könnte die Ausstellung von Echtzeit-Zertifikaten sein: „Dieses System sieht vor, dass die Gültigkeit eines Zertifikates in einer ständig online erreichbaren Datenbank abgefragt werden kann." (Schnellhorn 2003: 5) Diese Variante ist jedoch auf einen schnellen Server angewiesen und für Hacker-Attacken anfällig. (Schnellhorn 2003: 5)

5.7.3 Risiken der totalen Kontrolle

Gerade die elektronische Identitätskarte scheint die Lösung eines der vorrangigsten Vertrauensprobleme zu beinhalten: Virtuelle und reale Person werden wieder vereint. Wenn die Teilnahme an Auktionen und in Internet-Foren sowie der Kauf von Produkten

von einer gültigen elektronischen Identitätskarte abhängt, können Vergehen leichter sanktioniert und Betrugsfälle rechtlich belangt werden. Mindestens zwei der vier wichtigsten Voraussetzungen, die Luhmann für die Entstehung von Vertrauen nennt, würden erfüllbar: Einerseits eine erleichterte Einschätzung der Motivationsstruktur des Gegenübers, zumal die Motivation zum Vertrauensmissbrauch bei Androhung einer gesetzlichen Verfolgung geringer ist als in der Anonymität eines schrankenlosen Internets. Damit ist andererseits auch bereits die Möglichkeit von Bestrafung von Fehlverhalten als zweite der genannten Voraussetzungen nach Luhmann angesprochen.

Doch auch die Schattenseite der Kontrolle wird hier deutlich, die letztlich vom Staat ausgeübt wird, der als „Wurzelzertifizierungsdienst“ fungiert, indem er alle Zertifizierungsstellen akkreditiert oder ihnen die Anerkennung verweigert. Ein autoritärer Staat könnte die Zensur und Bespitzelung seiner Bürger leichter durchsetzen, die momentan an der dezentralen Struktur des Internets oft scheitert. Das grundlegend demokratische Medium Internet könnte durch zahlreiche Regulierungen in seiner Eigenart verändert werden. Mit Feststellung der Identität der Nutzer können Probleme im Datenschutz entstehen. Ausserdem wäre die Sperrung des Internetzugangs für nicht linientreue Personen denkbar, beispielsweise indem ihnen digitale Signaturen verweigert würden, ihre e-Mails also automatisch abgewiesen würden, wie wir bezüglich der Möglichkeiten im Umgang mit SPAM-Mails gesehen haben. Denkbar wäre auch das Risiko einer totalen Kommerzialisierung des Internets, indem URLs nur noch gegen Bezahlung, was ein Zertifikat voraussetzen würde, aufgerufen werden könnten.

[4] CA = Certification Authority (Zertifizierungsdienste)

6. Schluss

Der Mangel an räumlicher und zeitlicher Koexistenz von Transaktionspartnern führt zu Unsicherheiten bezüglich Identität und Vertrauenswürdigkeit, was die Prozesse der Vertrauensbildung verlangsamt oder – ohne reale Bezugspunkte wie nachprüfbare Adressen oder den Umweg über den Postversand von Verträgen – sogar verunmöglicht. Ausserdem kann mühevoll gebildetes Vertrauen durch Enttäuschungen leichter zerstört werden.

Die bisherigen Mittel, die zur Förderung von Vertrauen eingesetzt werden, beruhen vor allem auf Reputationseffekten und nur bedingt auf Sanktionsmöglichkeiten. Dies könnte sich mit der Etablierung von Zertifikaten ändern. Mit einer routinemässigen Verknüpfung von virtueller und realer Identität können BenutzerInnen des Internets davon ausgehen, dass einem Vertrauensmissbrauch Sanktionen in der realen Welt folgen werden, was die Motivation anderer Teilnehmer zu betrügen reduziert. Trotz der Sicherheitslücken und Missbrauchsrisiken würde die Verwendung von Zertifikaten und digitalen Signaturen somit zu mehr Vertrauen im Internet beitragen. Mit der steigenden Sicherheit im Internet wird das Dilemma aufgelöst, das sich im Augenblick noch vielen Usern stellt. Zur Ausnutzung aller Möglichkeiten, die das Internet bietet, und damit zu dessen weiterem Wachstum müssen die notwendigsten Voraussetzungen für Vertrauen erfüllt sein. Einen grossen Schritt in diese Richtung wird die flächendeckende Einführung von Zertifikaten leisten.

Die verhältnismässig kleinen Risiken, die die Verwendung von Zertifikaten noch in sich tragen, existieren auch im realen Leben. Zu nennen wäre hier das Risiko der Fälschung einer Unterschrift oder der Vertrauensbruchs durch eine als vertrauenswürdig eingestuften Person.

Allerdings stellt sich die Frage, ob das Internet einem höheren Anspruch an Sicherheit genügen muss als die reale Umwelt, um das gleiche Mass an Vertrauen zu gewinnen. Dieses Problem müsste jedoch in psychologischen Studien untersucht werden. Ein solcher Vertrauensmangel läge dann nicht in objektiv feststellbaren Sicherheitsrisiken sondern in subjektiven Risikowahrnemungen, die somit nicht mit der Behebung von Unsicherheiten sondern eher mit Image-Kampagnen aufzufangen wären.

7. Literaturverzeichnis

Bornschier, Volker (2001): Generalisiertes Vertrauen und die frühe Verbreitung der Internetnutzung im Gesellschaftsvergleich. In: Kölner Zeitschrift für Soziologie und Sozialpsychologie 26, H. 2, S. 373-400.

Brinkmann, Ulrich, Seifert, Matthias (2001): „Face to Interface“: Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. In: Zeitschrift für Soziologie 30, H. 1, S. 23-47.

Czurda, Henrik, Dietschi, Christian, Wunderli, Christine (2000): Vertrauensbildung im E-Business durch WebTrust. In: Der Schweizer Treuhänder, H. 8, S. 815-821.

Diekmann, Andreas, Wyder, David (2002): Vertrauen und Reputationseffekte bei Internet-Auktionen. In: Kölner Zeitschrift für Soziologie und Sozialpsychologie 54, S. 674-693.

Donath, Judith S. (1996): Identity and Deception in the Virtual Community. In: http://judith.www.media.mit.edu/Judith/Identity/IdentityDeception.htm (17. 09. 2004)

Engeler, Hans (2003): Elektronische Vertragsunterzeichnung und Archivierung in einer Webapplikation. Diplomarbeit. eduSwiss. http://www.ess.ch/esshome/content/download/Diplomarbeit_V_1_0.pdf (17. 09. 2004)

Jarvenpaa, Sirkka L., Leidner, Dorothy E. (1998): Communication and Trust in Global Virtual Teams. In: Journal of Computer-Mediated Communiction 3, H. 4, S. 1-38. http://www.ascusc.org/jcmc/vol3/issue4/jarvenpaa (17. 09. 2004)

Luhmann, Niklas (1968): Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart.

Schnellhorn Patrick (2003): Digitale Identifikation – Zertifikate und PKI. In: http://www11.informatik.tu-muenchen.de/lehre/seminare/proseminareSiPr-WS0304/14-identifikation2.pdf (17.09.2004)

PwC Deutsche Revision Aktiengesellschaft Wirtschaftsprüfungsgesellschaft (2000): Vertrauen bildet sich nicht in „E-speed“. Vertrauen und E-Procurement in europäischen Unternehmen. In: http://www.pwcglobal.com/gx/eng/ins-sol/survey-rep/etrust/pwc_etrust_deu.pdf (17.09.2004)

Volken, Thomas (2002): Elements of Trust: The Cultural Dimension of Internet Diffusion Revisited. In: Electronic Journal of Sociology, 6, H. 4. In: http://www.sociology.org

Walker, John(2004): Ende des Internet? In: http://www.heise.de/tp/deutsch/special/ende/default.html (17.09.2004)

Bundesamt für Kommunikation (2004): Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur. [Entwurf vom 1. Juni 2004] In: www.bakom.ch/imperia/md/content/deutsch/telecomdienste/internet/digitalesignatur/oscse.pdf (17.09. 2004)

Anmerkung

Die typographische Gestaltung sowie die wissenschaftliche Zitierweise wurden nach den Richtlinien des IPMZ (Institut für Publizistik- und Medienwissenschaft an der Universität Zürich) durchgeführt.