MedienPädagogik

Zeitschrift für Theorie und Praxis der Medienbildung

www.medienpaed.com

ISSN 1424-3636

**Jahrbuch Medienpädagogik 4.**

Zweitveröffentlichung aus: Jahrbuch Medienpädagogik 4. (2005) Wiesbaden: VS Verlag für Sozialwissenschaften. Hrsg. v. Ben Bachmair, Peter Diepold und Claudia de Witt.

# Digitale Vertrauenskulturen

*Jana Dittmann und Winfried Marotzki*

Wie sich die Transformation moderner Gesellschaften in den nächsten Jahren fortsetzt, hängt ganz zentral von der Entwicklung, Implementierung und sozialen Kontrolle der GNR-Technologien (der Kombination aus Gen-, Nano- und Robotertechnologie) ab. Die Diskussion zur künstlichen Intelligenz, die im letzten Jahrzehnt geführt worden ist, hat mit dem Gebiet der Robotertechnologie gleichsam eine neue Arena gefunden und sich auf dieses Gebiet verlagert. Hier werden jetzt grundlegende, auch pädagogisch zentrale Fragen, wie z.B. die nach einem Personenkonzept, diskutiert (vgl. Richards u.a. 2002). Zentrale Bedenken, die sich auf die mit den neuen Technologien verbundenen Gefahren stützen, sind immer wieder vorgetragen worden (Joy 2000; Moravec 1999). Ohne diese verzweigte Debatte an dieser Stelle rekonstruieren zu wollen, kann doch ein Befund in verallgemeinernder Absicht hervorgehoben werden: In dem Maße, in dem Gesellschaften aufgrund des Einsatzes neuer Technologien einen Komplexitätsschub aufweisen, der sich bis in die Lebenswelten einzelner Menschen hinein auswirkt, rückt ein „Mechanismus“ von Sozialität immer stärker in das Zentrum der Aufmerksamkeit: Vertrauen. Nicht nur aus der hier herangezogenen Perspektive wird diese Ressource prekär. Vielmehr ist seit Beginn der neunzehnhundertneunziger Jahre ein Ansteigen der Publikationen zu dem Thema Vertrauen aus verschiedenen Perspektiven zu konstatieren, und zwar in Soziologie, Pädagogik, Philosophie, Politikwissenschaft und Ökonomie. Vertrauen wird als elementare Voraussetzung sozialer Prozesse gesehen. Wenn Vertrauen aber nicht mehr als selbstverständliche Voraussetzung sozialer Prozesse verstanden werden kann, häufen sich Maßnahmen zur Vertrauensbildung, gerät das Phänomen Vertrauen also in den Fokus der systematischen Reflexion.

In der vorliegenden Arbeit wollen wir uns auf solche Thematisierungsbereiche beziehen, in denen Vertrauensbildung deshalb nötig wird, weil die sozialen Umgebungen in hohem Maße technisch gestaltet sind, und zwar durch neue Informationstechnologien. Im Folgenden werden wir zunächst einen Überblick über die Thematisierungen des Vertrauensphänomens in sozialwissenschaftlicher Hinsicht geben. Zweitens soll die Diskussion über Vertrauenskulturen am Beispiel von Online-Auktionen nachgezeichnet werden. Drittens werden dann einige Perspektiven für eine Vertrauenskultur virtueller Commu-

Dittmann, Jana, und Winfried Marotzki. 2017. «Digitale Vertrauenskulturen». *MedienPädagogik*, MedienPäd.Retro: Jahrbuch Medienpädagogik 4 (2005), 187–208. doi:10.21240/mpaed/retro/2017.08.11.X.

nities (framework of trust) entwickelt. Denn diese Arbeit ist aus umfangreichen interdisziplinären Vorarbeiten an der Universität Magdeburg entstanden, die darauf abzielen, eine virtuelle 3D Community zu entwickeln und zu gestalten.

## 1. Sozialwissenschaftliche Thematisierungsweisen

Thematisierungen des Verhältnisses von Vertrauen und sozialer Ordnung finden sich bei den Klassikern der Soziologie, angefangen bei Thomas Hobbes, über Emile Durkheim, Georg Simmel bis zu Max Weber. Ohne hier im einzelnen auf die Unterschiede einzugehen, kann zusammenfassend gesagt werden, dass Vertrauen für alle ein zentraler Mechanismus sozialer Interaktion darstellt, weil es – so die sachliche Dimension – Komplexität reduziert, weil es – so die soziale Dimension – stabile Rahmenbedingungen für Handlungs- und Interaktionsprozesse schafft und weil es – so die zeitliche Dimension – Nichtwissen zeitlich überbrückt (vgl. genauer: Endress 2002, S. 10-27). Vertrauen ist der soziale *Grundmechanismus*, der auf die Grunderfahrung reagiert, dass Handeln sich unter Bedingungen unvollständigen Wissens vollzieht und vollständige individuelle Handlungsautonomie ohnehin unmöglich ist, insofern jede Handlung immer risikobehaftet vollzogen werden muss. Vertrauen überbrückt die Informationsunsicherheit und die Zeitproblematik. Die Diskurse der letzten Jahrzehnte zum Thema Vertrauen strukturieren wir in Form von drei Strängen:

### *1.1 Systemtheoretische Thematisierung*

In systemtheoretischer Hinsicht bietet die frühe Arbeit von Niklas Luhmann (1968) ein kompaktes Thematisierungsformat in grundlagentheoretischer Einstellung. Für ihn ist Vertrauen ein Mechanismus der Komplexitätsreduktion, um auf diese Weise spezifische Risikoprobleme sozialen Handelns zu lösen. Durch Vertrauen werden Erwartungen stabilisiert und dadurch wird individuelles Handeln gesichert, indem das Zeitproblem des Handelns und die Informationsunsicherheit überbrückt werden. Luhmann unterscheidet zwischen persönlichem Vertrauen (Vertrauen in Personen) und Systemvertrauen (Vertrauen in soziale und technische Systeme). Die Kontrolle des Systemvertrauens erfordert Fachwissen (z.B. gegenüber technischen Systemen), die Kontrolle des persönlichen Vertrauens nicht. „Praktisch kann Vertrauenskontrolle also nur im Hauptberuf ausgeübt werden. Alle anderen müssen sich auf die hauptberuflich Kontrollierenden verlassen (...) Das Vertrauen in die Funktionsfähigkeit von Systemen schließt Vertrauen in die Funktionsfähigkeit ihrer immanenten Kontrollen ein. Die Risikoneigung muß in diesen Systemen selbst unter Kontrolle gehalten werden“ (Luhmann 1968, S. 77). Dabei konstatiert er, dass die Entwicklung von der Dominanz des Typs des

(inter)personalen Vertrauens in kleinen und relativ undifferenzierten Gesellschaften hin zu einem Typus von Systemvertrauen gehe, der typisch für komplexe, hochgradig differenzierte, technisch orientierte Gesellschaften ist: „Eher wird man damit rechnen müssen, dass Vertrauen mehr und mehr in Anspruch genommen werden muß, damit technisch erzeugte Komplexität der Zukunft ertragen werden kann“ (Luhmann 1968, S. 20).

### *1.2 Die Rational Choice Perspektive*

Pointiert hat James S. Coleman (1991) diese Perspektive ausgearbeitet, derzufolge Vertrauen und rationales Handeln aufeinander bezogen sind. Die strukturell nicht mögliche Gleichzeitigkeit von Leistung und Gegenleistung bildet für Colemann das spezifische Risiko des Vertrauenschenkens, denn zeitliche Asymmetrien stellen in sozialen Austauschbeziehungen prinzipiell ein Risiko dar. Folgende Strukturmerkmale kennzeichnen die Logik von Vertrauen: (1) Die Vergabe von Vertrauen impliziert die Übertragung von Ressourcen. (2) Im Falle der Vertrauenswürdigkeit des Vertrauensnehmers verbessert der Vertrauensgeber seine Position, sonst verschlechtert er sie. (3) Die Übertragung von Ressourcen erfolgt, ohne dass der Ressourcenempfänger eine wirkliche Verpflichtung eingeht. (4) Eine Einschätzung der berechtigten Vergabe von Vertrauen impliziert eine Zeitverzögerung bis zu dem Zeitpunkt, an dem sie sich potentiell auszahlt (vgl. Endress 2002, S. 36).

Auf jeden Fall ist die Entscheidung für oder gegen ein Vertrauen für Coleman abhängig vom Stand des Wissens seitens des Vertrauensgebers über die Gewinnchancen und die möglichen Verluste. Diese Relevanz des Wissens verweist auf die Bedeutung von Bewährung. Individuen vergeben (als rationale Akteure) auf rationale Weise Vertrauen, wenn die wahrscheinlich erwartbaren Vorteile (Bewährung) größer sind als die wahrscheinlich erwartbaren Nachteile (Enttäuschung). Es liegt also ein Modell einseitiger Vertrauensvergabe vor; insofern – so urteilt Endress 2002 – liege ein eher reduzierter Phänomenbereich des Vertrauens vor. Informationen einholen und Informationen zukommen lassen ist hier das strategische Handlungsmuster, um Vertrauenswürdigkeit einschätzen zu können. Man sieht sehr schnell die Grenzen dieses Modells: Ein rational Handelnder im Sinne Colemans müsste, um zwischenmenschlichen Bereich Vertrauen zu vergeben, Informationen einholen. Gerade dieses zerstört aber häufig gerade Vertrauen.

### *1.3 Modernitätstheoretische Thematisierung*

Anthony Giddens (1996) hat herausgearbeitet, dass die Entwicklung der Moderne sich dadurch auszeichnet, dass die Menschen aus konkreten orts- und zeitgebundenen Interaktionszusammenhängen immer mehr herausgehoben werden (Entbettung). Damit einher geht der Prozess der Reflexivitätssteige-

rung (die Einzelnen müssen immer mehr selbst entscheiden und verantworten; elementare Mechanismen werden selbstbezüglich). Diese Tendenz hatte Luhmann bereits aufgezeigt: In dem Maße, in dem die Komplexität des sozialen Lebens ansteigt, müssen dessen elementare Mechanismen reflexiv werden. Luhmann verdeutlicht dieses an dem Beispiel des Lernens. Ab einer bestimmten Stufe der Komplexität kann Lernen nur dadurch gesteigert werden, dass der Lernende sich der Mechanismen des Lernens klar wird, um diese auf diesem Weg verändern zu können: Lernen des Lernens. Aber zurück zu Giddens: Ähnlich wie Luhmann argumentiert auch er, dass Menschen in dem Maße auf Systemvertrauen angewiesen sind, wie sich im Zuge der Entwicklung einer Informations- bzw. Wissensgesellschaft immer mehr Technik zwischen Mensch und (natürliche) Umwelt schiebt.

Der Begriff des Vertrauens lässt sich nach Giddens zunächst als Zutrauen zur Zuverlässigkeit einer Person oder eines Systems im Hinblick auf eine gegebene Menge von Ergebnissen oder Ereignissen bestimmen (Giddens 1996, S. 49). Vertrauen ist ein Zustand, der aus dem Glauben an die Zuverlässigkeit einer Person oder Institution oder Technik folgt (sich-verlassen-auf; keinen-Grund-zum-Zweifeln-haben). Das Erlebnis der Sicherheit beruht normalerweise auf einem Gleichgewicht zwischen Vertrauen und akzeptablem Risiko. Schwerpunktmäßig nimmt Giddens, und zwar wesentlich stärker als Luhmann, die institutionelle Vermitteltheit von Systemvertrauen in den Blick. Das Wesen moderner Institutionen ist für ihn nämlich zutiefst mit den Mechanismen des Vertrauens in abstrakte Systeme, vor allem Expertensysteme, verbunden. Gerade Expertensysteme (z.B. Arzt-Patient-Beziehung) sind für ihn typische Beispiele institutioneller Rahmungen und institutionalisierter Vertrauensmuster (frameworks of trust), z.B. das Versicherungssystem. Das sind für ihn gleichsam intermediäre Institutionen des Vertrauens. Man könnte dabei etwa an die Stiftung Warentest oder auch an Verbraucherzentralen denken.

### *1.4 Empirische Analysen zum Aufbau von Vertrauen*

Untersuchungen zur Genese von Vertrauenskonstellationen sind auf unterschiedlichen Emergenzstufen des Sozialen durchgeführt worden. Die Einteilung von Endress (2002) in Mikro-, Meso- und Makroebenen halten wir für sinnvoll. Wir klammern lediglich die Studien zum Vertrauensaufbau in virtuellen Welten aus, weil wir sie im folgenden Abschnitt genauer behandeln werden. Zu den *Mikroanalysen* zählen Analysen von face-to-face Interaktionsprozessen. James M. Henslin (1968) untersucht beispielsweise, wie Taxifahrer sich relativ schnell ein Bild von einem neuen Kunden machen und dann auf Grundlage des so konstituierten Vertrauens ihn als Fahrgast akzeptieren oder eben nicht. *Mesoanalysen* untersuchen Vertrauen in Organisations- und Arbeitsprozessen, z.B. Studien zu professionellem Handeln (Arzt-Patient-Beziehung oder zum professionellen Handeln von Pfarrern). Makroanalysen thematisieren das Vertrauen zu gesellschaftlichen Institutionen und

in gesellschaftliche Transformationsprozesse. Am Beispiel der polnischen Gesellschaft hat beispielsweise Piotr Sztomka (1995) seine Analysen zur Entstehung von Vertrauens- bzw. Misstrauenskulturen durchgeführt. Vertrauen ist für ihn eine kulturelle Ressource zur Bewältigung der Zukunft. „Vertrauen regt Kooperation und gegenseitige Hilfe an, dämpft Konflikte und mäßigt persönliche Auseinandersetzungen“ (Sztompka 1995, S. 260). Vertrauen versteht Sztompka als Annahme über das erwartbare menschliche Handeln anderer und bezieht es somit auf mehr oder weniger unsichere Ereignisse, deren Ausgang zum jetzigen Zeitpunkt nicht bekannt sein kann. Für postkommunistische Gesellschaften diagnostiziert er einen durchgängigen und tiefgreifenden Vertrauensverlust. Zusammenfassend stellt er dar, dass sich vertrauensbildende Maßnahmen auf folgende Aspekte konzentrieren müssten: (1) Die Unsicherheit der Politik durch Bestimmtheit ersetzen; (2) Willkür bekämpfen, für mehr Berechenbarkeit; (3) Rechtssicherheit; (4) Geheimniskrämerei bekämpfen; (5) Pluralismus unterstützen; (6) Inkompetenz von Personen in zentralen Positionen bekämpfen und Integrität sichern.

Soweit die Rekonstruktion einiger zentraler Diskussionstopoi. Sie verdeutlicht zum einen die zentrale, offenbar nicht hintergehbare Funktion von Vertrauen für soziale Austauschprozesse. Zum anderen zeigt sie aber deutlich den Trend, dass Vertrauen im Sinne von Systemvertrauen dann immer zentraler wird, wenn sich Technik zwischen den Menschen und andere Menschen bzw. seine Umwelt schiebt.

Wir möchten diesen Sachverhalt im Folgenden exemplarisch am Beispiel neuer Informationstechnologien erörtern. Durch sie sind neue soziale Arenen entstanden, die neue Handlungsmöglichkeiten, aber eben auch neue Formen des Vertrauens und Misstrauens bieten. Beispielsweise finden ökonomische Akteure in Form des E-Commerce neue Handelsmöglichkeiten. Aus diesem Bereich wird unser erstes Beispiel kommen. Neue soziale Vergemeinschaftungsformen bilden sich im Internet, die verschiedenartigen Interesses gerecht werden. Darauf werden wir uns im darauffolgenden Schritt beziehen.

## 2. Vertrauen in digitalen Welten

Das Problem der Konstitution von Vertrauen im Internet ist bisher vornehmlich anhand von Online Versteigerungen diskutiert worden. Deshalb beziehen wir uns in diesem Argumentationsschritt auf diesen Spezialfall und öffnen dann den Fokus unserer Betrachtung, indem wir Gruppenphänomene im Internet hinsichtlich der Vertrauenskonstitution betrachten wollen.

Bekannt sind die beiden Internet-Auktionshäuser „Ricardo“ (www.ricardo.de) und „eBay“ (www.ebay.de). Auf sie beziehen sich die beiden Arbeiten, auf die wir hier exemplarisch eingehen wollen. Die Arbeit von Brinkmann und Seifert (2001) untersucht das Modell der Vertrauensbildung, das eBay in seinen allgemeinen Geschäftsbedingungen wie folgt einführt: „Um betrügeri-

sche Handlungen zu vermeiden, hat eBay ein öffentlich zugängliches Bewertungssystem eingerichtet, mittels dessen sich Nutzer nach der Durchfuehrung eines Vertrages gegenseitig bewerten können. Das Bewertungssystem soll Nutzern dabei helfen, die Zuverlaessigkeit anderer Nutzer einzuschätzen. Die Bewertungen werden von eBay nicht überprüft und können ihrer Natur nach unzutreffend oder irreführend sein“ (www.ebay.de. Allgemeine Benutzerbedingungen [AGBn] §4 [20.2.2003]).

Brinkmann/Seifert (2001) entwickeln in ihrer Arbeit zu „ebay“ ein dreidimensionales Vertrauensmodell:

*(1) Kompetenzerwartungen*

Die erste Dimension von Vertrauen besteht darin, dass der Vertrauende erwartet, dass der andere die entsprechende Kompetenz und Professionalität besitzt, um entsprechende Aufgaben auszuführen. Diese Dimension deckt Fälle der Laien-Professionellen-Beziehung ab, also z.B. Arzt-Patienten-Beziehung oder Lehrer-Schüler-Beziehung. Indikatoren für Vertrauenswürdigkeit in dieser Dimension sind beispielsweise Berufsabschlüsse, Qualifikationsnachweise, Zertifikate und Ähnliches. Diese Dimension deckt aber auch Fälle der Mensch-Maschine-Interaktion ab. Vertrauen in Technik (z.B. in die Sicherheit eines Verkehrsmittels) liegt dann vor, wenn unterstellt werden kann, dass diese Technik von kompetenten Akteuren hergestellt und hinsichtlich der Qualität geprüft sind. Vertrauensindikatoren sind hier in der Regel Markennamen und Qualitätszertifikate, aber auch Rankings (beispielsweise durch Verbraucherzentralen). Die Kommunikation von Vertrauenswürdigkeit in dieser Dimension ist dann die *Reputation*.

*(2) Integritatserwartungen*

„Die Integrität einer Vertrauensperson setzt sich zusammen aus ihrer Offenheit/Erreichbarkeit, Wahrhaftigkeit, Glaubwürdigkeit und Zuverlässigkeit“ (Brinkmann/Seifert 2001, S. 25).[1]

*(3) Gesinnungserwartungen*

Es wird erwartet, dass die Vertrauensperson sich wohlwollend und loyal verhält. „Wer vertraut, hegt die Erwartung, dass seine Interessen nicht verletzt und der eigenen Person kein Schaden zugefügt wird, selbst wenn dazu für eine Vertrauensperson die Gelegenheit und ein Anreiz besteht“ (Brinkmann/Seifert 2001, S. 26). Akteure dürfen aus der Vertrauensbeziehung einen Vorteil ziehen, aber nicht auf Kosten des Anderen. Es muss Fairness im Sinne eines ausgeglichenen Gebens und Nehmens bestehen.

1 Offenheit bedeutet vollständige Informationslage, und Erreichbarkeit bedeutet Kommunikationsbereitschaft. Wahrhaftigkeit bedeutet wahrheitsgemäße Informationen. Glaubwürdigkeit bedeutet, dass gegebene Versprechen auch eingehalten wer- den, also eine gewisse Übereinstimmung zwischen Worten und Taten. Zuverlässigkeit ist eine Stetigkeitserwartung, Kontinuitätserwartung des Verhaltens und Handelns.

Die Autoren fassen ihr Modell zusammen: „Vertrauen läßt sich jetzt definieren als die gefühlsmäßige und/oder kalkulierte Bereitschaft eines Akteurs, auf die Kontrolle eines anderen zu verzichten und eine riskante Vorleistung (Handlung) zu erbringen, die meistens mit einer kognitiven Erwartung und dem Gefühl einhergeht, dass der oder die VertrauensempfängerIn gleichzeitig kompetent, integer und wohlwollend ist“ (Brinkmann/Seifert 2001, S. 27).

Die Autoren konzentrieren sich im Folgenden nicht auf die technische Seite der Vertrauenskonstitution bei „ebay“, sondern ausschließlich auf „das Problem der interpersonalen Vertrauenskonstitution im Rahmen einer sozialen Beziehung im Internet“ (Brinkmann/Seifert 2001, S. 28). Aufgrund der fehlenden Kopräsenz müssen die Internetauktionäre einander vertrauen, denn Käufer und Verkäufer sind einander in der Regel völlig fremd und besitzen keine eigenen Erfahrungen mit der Vertrauenswürdigkeit des jeweils anderen. Zur Lösung dieser Vertrauensproblematik hat der Betreiber der Plattform „ebay“ fünf vertrauensstiftende Kontroll- und Regulationsformen installiert:

*Erstens:* Selbstregulierung der Community im Feedback-Forum durch ein Vertrauensprofil: Die Mitglieder sollen sich in erster Linie selbst gegenseitig kontrollieren. „Das Vertrauensprofil stellt einen Lösungsversuch der Auktions-Plattform für das Problem der Reputationsbildung dar, das sich kleinen (Privat-) Anbietern ohne Markennamen auf Internetmärkten stellt“ (Brinkmann/Seifert 2001, S. 29). Jeder Akteur, ob Käufer oder Verkäufer, bewertet nach jeder Transaktion den jeweils anderen hinsichtlich verschiedener Kriterien. Diese Bewertungen werden in das Vertrauensprofil aufgenommen. „Jeder Akteur im Rahmen einer Internet-Auktion fungiert dabei mit seiner Bewertung für nachfolgende Auktionäre als Dritter, der im Sinne eines Ratgebers (...) die Vertrauenswürdigkeit der Akteure im Hinblick auf vorausgegangene Auktionen einschätzt und in Form einer reputationsbildenden Bewertung dokumentiert“ (Brinkmann/Seifert 2001, S. 29).

*Beispiel 1*: Bewertungssystem eBay


Fast alle vergleichbaren Anbieter haben solche Dokumentationen, die sich auf das vertrauensrelevante Transaktionsverhalten beziehen, implementiert. Über-

wiegend wird in der Fachliteratur attestiert, dass dieses System funktioniert, obwohl es immer auch wieder kritische Stimmen gibt (vgl. Intern.de 2003).

*Zweitens:* Kontrolle der Plattform durch die Plattformbetreiber, d.h. Selektion von „schwarzen Schafen".

*Drittens:* Garantien durch den Plattformbetreiber (Schadensersatz): „Das Angebot des Schadensersatzes reduziert das Risiko der Vertrauensvergabe für den Kaufinteressenten und erleichtert diese" (Brinkmann/Seifert 2001, S. 30).

*Viertens:* Zertifizierung auf der Basis von zusätzlichen Personendaten: Fundierung des Vertrauens in Identität (weil die Leute Online mit einem Alias auftreten). eBay überlegt, ob die Kunden bei der Anmeldung ihre Personendaten freigeben (z.B. Personalausweis faxen) sollten, um so eine Konvergenz von Online und Offline-Identität zu erreichen.

*Fünftens:* Stiftung sozialer Kontexte: „Regulativ wirken schließlich auch die sozialen Netzwerke bzw. ‚Communities', die als Nebeneffekt der ökonomischen Transaktionen entstehen und über das rein Geschäftliche hinausweisen" (Brinkmann/Seifert 2001, S. 31). eBay unterstützt solche Communities, die sich zuweilen auch Offline treffen. Die zwischen den Mitgliedern einer Community festzustellenden sozialen Ähnlichkeiten und charakteristischen Gemeinsamkeiten wirken regulativ und stiften eine charakteristische Art von Vertrauen, das darauf beruht, dass gemeinsame Hintergrundüberzeugungen geteilt werden. In einem Interview sagen die Betreiber von eBay: „Letztlich vollzieht das, was wir hier erleben, die historische Entwicklung von Städten und Siedlungen nach. Diese haben sich in der Geschichte immer dort gebildet, wo aufgrund von Handelsstrassen oder Häfen ein Marktplatz vorhanden war. Um diesen Marktplatz herum haben sich dann auch die sozialen Gefüge entwickelt. Im Zentrum der Marktplatz, am Rande die Cafes: genau dieses Modell versuchen wir nachzubilden, denn es hat sich als wichtig erwiesen, das neben dem konkreten Geschäft auch die Geschichten um das Produkt sichtig sind" (Interview cit. Brinkmann/Seifert 2001, S. 31).

Die Autoren stellen in ihrer Studie im Wesentlichen die Resultate der von ihnen durchgeführten quantitativen und qualitativen Analyse einer Zufallsstichprobe aus den Feedback-Foren dar. Die von eBay selbst geäußerte Einschätzung der hohen Relevanz der Selbstregulierung bestätigen die Autoren in ihrer Untersuchung. Wenn ein Akteur im Laufe der Zeit mehrere schlechte Bewertungen erfährt, wird auch weniger Vertrauen gewährt und es kommen mit hoher Wahrscheinlichkeit auch weniger Transaktionen zustande. Es ist dann für ihn unter Umständen günstiger, mit einer neuen Identität von vorne zu beginnen. Insofern rückt die Verifizierung von Identitäten an dieser Stelle in das Blickfeld, und zwar zunächst als technisches Problem (formale Identität), denn wenn dies geschieht, muss sicher gestellt sein, dass der Nutzer diese Identitäten auch einsehen und rekonstruieren kann.

Brinkmann und Seifert fassen die Resultate zusammen, indem sie die interpretierten Daten auf die drei Dimensionen ihres Vertrauensmodells beziehen: Es lassen sich verschiedene Arten von *Kompetenzerwartungen* nachweisen: Expertenwissen (über Produkte), technische/handwerkliche Fähig-

keiten (beim Versand der Ware), Ausübung einer Routinehandlung (z.B. nicht ausreichende Frankierung der Sendung), rollenspezifische Kompetenz (d.h., es darf auf Verkäuferseite nicht passieren, dass nach erfolgreicher Auktion die Ware nicht mehr da ist, weil sie schon anderweitig verkauft wurde). *Integritätserwartungen* werden beispielsweise dann verletzt, wenn keine Reaktion darauf erfolgt, eine Kommunikation anzubahnen. „Damit ist die ungenügende Erreichbarkeit von InteraktionspartnerInnen die meistgenannte Problematik in der Integritätsdimension. Die Unzugänglichkeit wird als unfreundlich empfunden. (...) Im Umkehrschluß bedeutet dies, dass eine gute Erreichbarkeit Kommunikatitonsbereitschaft signalisiert, die für die Stiftung von Vertrauen höchst relevant ist“ (Brinkmann/Seifert 2001, S. 41). Unzuverlässigkeit und Inkonsistenz werden vor allem beim Ausbleiben der Ware thematisiert. Wahrhaftigkeit steht in Frage, wenn jemand behauptet, das Geld sei nicht angekommen. *Gesinnungserwartungen* werden verletzt, wenn vorsätzliche Täuschung (Betrugsabsicht) unterstellt werden muss.

Abschließend stellen die Autoren fest, dass die Logik der Vertrauensprofile darin bestehe, die fehlende Primärerfahrung durch eine Vielzahl von Sekundärbeurteilungen zu substituieren. Die Institutionalisierung von Vertrauen in Form von Vertrauensprofilen funktioniere. Insbesondere die Erreichbarkeit als Dimension der Integritätsdimension spiele eine grosse Rolle. Es liege bei eBay eine soziale (kommunikative) Einbettung der Transaktionen (der Marktvorgänge) vor. „Gewöhnlich sind Intermediäre, die Reputation über Akteure verbreiten und damit Aussagen über deren Vertrauenswürdigkeit machen, Einzelpersonen oder Institutionen (z.B. die Stiftung Warentest). Im Fall der Internetauktion setzt sich der Intermediär aus einer mehr oder minder großen Anzahl von Einzelbewertungen zusammen, die als Gesamtheit das Vertrauensprofil abbilden“ (Brinkmann/Seifert 2001, S. 43).

Die zweite einschlägige Studie von Diekmann und Wyder (2002) untersucht am Beispiel von Handyversteigerungen beim Internetauktionshaus Ricardo Auswirkungen des Reputationssystems auf Preise und Zahlungsmodalitäten. Sie gelangen zu dem Resultat, dass Reputation eine positive Auswirkung auf den Verkaufspreis habe: „Anbieter mit hoher Reputation legen im Durchschnitt höhere Mindestpreise fest, haben einen größeren Verkaufserfolg und können es sich leisten, die Zahlungsmodalität stärker zu ihren Gunsten zu beeinflussen“ (Diekamnn/Wyder 2002, S. 690). Sie betonen die grundlegende soziale Regulationsfunktion von Reputation: Unter der Bedingung von Reputation werde soziale Ordnung möglich. Sie fördere im hohen Maße Kooperation. „Verkäufer haben einen Anreiz, in Kooperation zu investieren. Kunden werten die Reputation als ein Signal für ein geringeres Risiko der Transaktion und sind bereit, dafür eine Gebühr, eine Art Versicherungsprämie zu entrichten“ (Diekmann/Wyder 2002, S. 689f.). Für die Herstellung von Kooperation durch Reputation sind folgende Bedingungen zu erfüllen: (a) die Voraussetzung, muss er füllt sein, dass sich die zu bewertende Aktion prinzipiell wiederholen wird, also nicht einmalig ist; (b) die Transkation muss relativ schnell, unkompliziert und objektiv nachvollziehbar zu bewerten sein; (c) die Transaktionen sollten

von allen (oder möglichst vielen) bewertet werden: je mehr Bewertungen desto zuverlässiger ist der Vertrauensindex; (d) sämtliche Bewertungen sollten prinzipiell allen Interessierten zugänglich sein (Transparenz).

## 3. Aspekte eines Framework of Trust fur Communities: Das Dreiecksverhältnis von Identität, Vertrauen und Technik

Exemplarisch am Beispiel von Online-Versteigerungen haben wir diskutiert, welche Mechanismen für die Konstitution von Vertrauen bei wirtschaftlichen Transaktionen im Internet möglich sind. Dabei zielen die dargestellten Mechanismen vor allem auf *sozialtechnische Gestaltungsmöglichkeiten,* die nach Winkel „der Verbesserung des gesellschaftlichen Sicherheitsmanagements“ (Winkel 1999, S. 198) dienen. Da das Internet als Kommunikationsgrundlage auf einer Vielzahl von technischen Komponenten basiert, sind darüber hinaus *ingenieurtechnische Gestaltungsmaßnahmen* notwendig, um das Vertrauen in die interaktiven Informationstechnologien zu erhöhen. Nach Winkler richten sich ingenieurtechnische Gestaltungsmaßnahmen „in erster Linie auf die Implementierung von Sicherheitsvorkehrungen in der Form von Hardware und Software“ (Winkel 1999, S. 197)[2].

Insbesondere ist zu konstatieren, dass für die diskutierten vertrauensbildenden Maßnahmen die Identifizierung der Nutzer (formale Identität) als Grundvoraussetzung für Vertrauen angesehen wird, wie dies ja auch schon in der Studie zu ebay deutlich wurde. In der digitalen Welt eröffnen sich jedoch eine Vielzahl von Schwierigkeiten, die Identität eines Nutzers eindeutig festzustellen: Einerseits existieren Bestrebungen, Kommunikationsbeziehungen zu anonymisieren, um den Persönlichkeitsschutz zu garantieren, andererseits tritt der Internetnutzer nicht durch sein persönliches Erscheinen auf und lässt seine Identität durch die Technik modellieren.

Virtuelle Communities mit ihrer Vielzahl von Akteuren stellen in dieser Hinsicht eine besondere Herausforderung dar, eine Zuordnung von einem oder sogar von mehreren Nutzern zu einer realen Identität vorzunehmen. Es ist möglich, dass ein Internetnutzer mehrere Internetidentitäten annehmen kann, er kann zwischen Identitäten wechseln, neue erstellen oder gar fremde Identitäten übernehmen. Dies gehört nicht nur zu den Vertrauensrisiken von Virtuellen Communities, dies ist Bestandteil ihrer Faszination. Aber nur durch die eindeutige Feststellung der formalen Identität eines Nutzers können technisch realisierte Anreizsysteme wie die positiven oder negativen Listen bei eBay funktionieren und Vertrauen thematisieren, wodurch eine Dreiecksbeziehung von Identität, Technik und Vertrauen entsteht, die in Virtual Communities modelliert werden muss (vgl. Abb. 1).

2 Aus der Sichtweise der Informatik beinhaltet das Fachgebiet der IT-Sicherheit (vgl. BSI 2003) organisatorische und technische Maßnahmen.

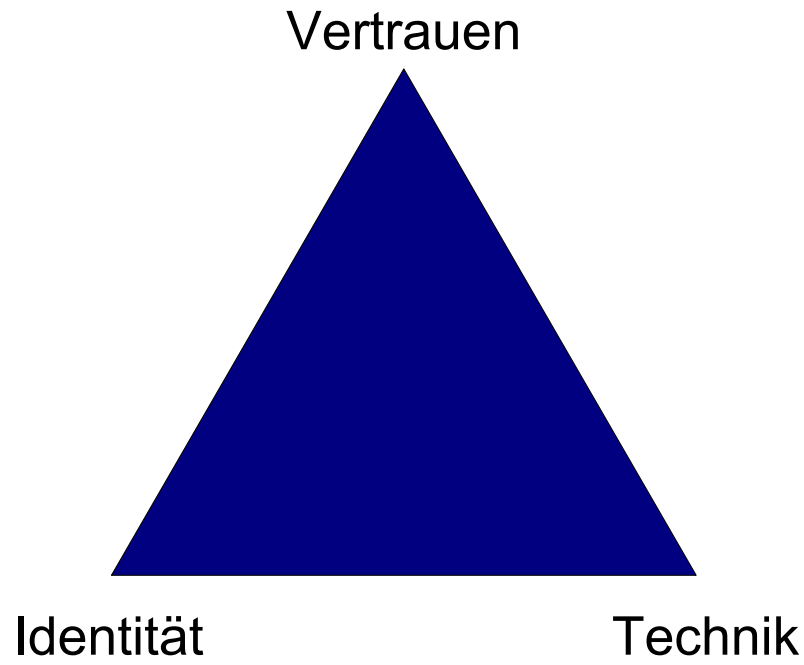


**Abb. 1**

Unter *Identität* verstehen wir formale, persönliche Identität sowie Rollenidentität. Die *formale Identität* bezieht sich, wie bereits erwähnt, auf die Identifizierung der jeweiligen Offline-Person, d.h. es soll auf diese Weise sichergestellt sein, dass hinter einer Online-Person (z.B. einem Avatar) auch eine bestimmte Offline-Person steht. Diese Identifizierung würde den Online-User gleichsam Offline identifizieren. Das ist nicht nur für Internetauktionshäuser wie eBay wichtig, sondern gilt auch für Communities. Offline-Personen, die online agieren und dort soziale Beziehungen aufbauen, müssen sicher sein können, dass Online-Personen, denen sie dort begegnen, bei der erneuten Begegnung auch dieselben sind. Auf diese Art der formalen Identität wird in den Communities unterschiedlich stark Wert gelegt. Traditionell ist es beispielsweise in Newsgroups verpönt, sich einen Nickname zuzulegen, es wird der reale Namen (Realname) eingefordert. Aber auch wenn in vielen Spielecommunities Nicknames und beliebig konstruierbare Avatare Standard geworden sind, ist es für die Entwicklung einer Vertrauenskultur doch wichtig, zu wissen, dass hinter ein und derselben Online-Person eindeutig eine reale Person steht.

Die *persönliche Identität* bezieht sich auf die Identität, die sich eine reale Person Online gibt. In der Regel handelt es sich dabei um eine Liste von selbst gewählten Eigenschaften, die über die Identity Card einsehbar, aber von der Person auch veränderbar sind. *Rollenidentität* oder soziale Identität stellt sich in den sozialen Aktionen im virtuellen Raum her. In den Foren bilden sich beispielsweise bestimmte Rollen aus, z.B. derjenige, der sich bei der *Formel 1* in technischen Dingen gut auskennt. Über solche Rollenidentität wird Reputation aufgebaut.

Unter *Vertrauen* verstehen wir zunächst das Bündel von Eigenschaften, das in den Abschnitten 1.1 bis 1.3 herausgearbeitet worden ist. *Technik* beinhaltet nach Winkel (1999) alle Maßnahmen in Form von Hard- und Softwareimplementierung.

Das Dreieck Vertrauen, Identität und Technik ist so zu lesen, dass (1) eine *Vertrauenskultur* die Bedingung dafür ist, dass Identität im o.g. dreifachen Sinne sichergestellt ist und sich entwickeln kann und dass sie Bedingung dafür ist, dass Technikgestaltung akzeptiert wird (Vertrauen in Systeme). (2) *Identität* im Sinne von personaler Identität und Rollenidentität ist Bedingung dafür, dass sich eine Vertrauenskultur entwickeln kann, und sie ist Bedingung dafür, dass Technik auch gestaltend entsprechende Möglichkeiten sichern und bereitstellen kann. (3) Technische Gestaltungen sind Bedingung dafür, dass Identität sichergestellt und sich entwickeln kann, und sie ist Bedingung dafür, dass eine Vertrauenskultur entstehen kann[3]. Im Folgenden sollen diese drei Aspekte näher entwickelt werden.

### *3.1 Vertrauen als Bedingung von Identität und Technik*

Bei der Modellierung von Vertrauen im Rahmen unseres Dreiecks bündeln wir verschiedene grundlegende vertrauensbildende Aspekte. Die oben angeführten sechs Perspektiven nach Szompka (1995) können als Regelsicherheit zusammengefasst werden. Eine Community benötigt klare Regeln, Regulationsmuster wie Normen und Werte – sozialer Natur –, die durch geltende Gesetze und Rechtsvorschriften, durch den Dienstleister (Betreiber einer Community) oder durch die Nutzer selbst demokratisch festgelegt und kontrolliert werden. Das Regelwerk muss allen Akteuren bekannt sein und alle Aktionen müssen regelgeleitet und rekonstruierbar erfolgen. Regelwerke für Communities müssen also von ihrer Genese her transparent (wie sind sie zustande gekommen?), von ihrer Umsetzung her legitim sein (wie begründet sich das Recht der Durchsetzung des Regelwerkes?), und sie müssen Geltung haben (jeder muss sich an sie halten, ansonsten drohen Sanktionen). Technisch gesehen, sind die Aspekte der Funktionsfähigkeit, der Verfügbarkeit und der Integrität der verwendeten Technologien wesentliche Aspekte von Vertrauen. Aus Sicht der IT-Sicherheit können wir dem Sammelbegriff Vertrauen die folgenden Sicherheitsaspekte zuordnen (nach Dittmann u.a. 2001):

3 Einschlägige Studien zeigen, dass eine gezielte Auswahl von Maßnahmen als Katalysator für die Vertrauensbildung wirken kann. Reimer (2003) stellt darüber hinaus fest, dass in komplexen Netzwerken die Sicherheit tendenziell abnimmt, dass Vertrauen aber tendenziell wachsen kann, indem man bewusst und verantwortungsvoll mit unvermeidbaren Restrisiken umgehen lernt. Reimer weist des weiteren darauf hin, dass zu unhandliche Vorrichtungen für Sicherheit auch Unsicherheit bedeuten können, denn sie werden vom kompetenten Nutzer abgeschaltet, skalierbare und adaptive Sichrheitseigenschaften können hingegen Vertrauen erzeugen (vgl. Reitenspiess 2003).

*Vertraulichkeit:* Informationen sollen nur den dazu berechtigten Parteien (dies können Personen oder auch Geräte sein) zur Verfügung stehen.

*Integrität:* Es soll sichergestellt werden, dass Daten nicht unautorisiert geändert wurden. (3) *Verfügbarkeit und Zuverlässigkeit:* Informationen oder Betriebsmittel sollen bestimmten Parteien bei Bedarf zur Verfügung stehen und definierte Aufgaben erledigen. (4) *Authentizität:* Sowohl Daten als auch Parteien, die miteinander kommunizieren, sollen auf ihre Echtheit hin geprüft werden können. Man unterscheidet dementsprechend zwischen der Authentizität des Datenursprungs (Data Origin Authenticity), die auch die Integrität der Daten beinhaltet, und der Authentizität der Parteien (Entity Authenticity). (5) *Nachweisbarkeit* Mit Nichtabstreitbarkeitsmechanismen soll gegenüber Beteiligten und Unbeteiligten bewiesen werden, ob ein bestimmtes Ereignis eingetreten ist bzw. eine bestimmte Aktion ausgeführt wurde oder nicht. Das Ereignis oder die Aktion kann dabei das Erzeugen, das Übermitteln, die Entgegennahme oder das Vorlegen einer Nachricht sein.[4]

### *3.2 Technik als Bedingung von Vertrauen und Identität*

Im Gegensatz zu den in Abschnitt 2 herangezogenen Arbeiten, die die technische Dimension bei der Erörterung von Vertrauen in virtuellen Welten ausgeklammert haben, beziehen wir diese ein und diskutieren exemplarisch vertrauensbildende Technikmaßnahmen. Voranstellen möchten wir, dass Vertrauen in Technik sehr stark vom individuellen Sicherheitsbedürfnis, der Sicherheitseinstellung und dem Sicherheitsinteresse – ebenfalls abhängig auch von kulturellen Einflüssen – abhängt. Man unterscheidet deshalb gelegentlich „subjektive Sicherheit“ und „objektive Sicherheit“ (vgl. Grimm 1994). Die subjektive Sicherheit, also das individuelle Sicherheitsbedürfnis, die individuelle Sicherheitseinstellung und das individuelle Sicherheitsinteresse, ist von Community zu Community unterschiedlich. Es ist vor allem dann schwierig zu bestimmen, wenn Communities international zusammengesetzt sind, wenn also verschiedene kulturelle Selbstverständlichkeiten und Habitus im Spiel sind. Es ist bereits in „einfachen“ Mailinglisten oder Newsgroups zu beobachten, dass in bestimmten Abständen diese kulturellen Verortungen selbst thematisiert werden und dann zu einem expliziten Element der diskursiven Deliberation werden.[5]

Wir wollen uns im Folgenden den technischen Maßnahmen widmen, die sich auf die „objektive Sicherheit“ beziehen. Dass diese immer wichtiger werden, ist in den Abschnitten zu Luhmann und Giddens herausgearbeitet

4 Oftmals werden die beiden letzten Sicherheitsaspekte mit den drei ersten erklärt und erscheinen nicht separat als eigenständige Aspekte.

5 Ein gutes Beispiel dafür ist die von Geert Lovink und Pit Schultz betriebenen Mailingliste *Nettime-l*, die 1995 in Venedig gegründet wurde und seit dieser Zeit zu einer Plattform des internationalen kulturellen Austauschs geworden ist (nettime-l@bbs.thing.net).

worden. In dem Maße, wie gesellschaftliche Komplexität ansteigt, nimmt auch die Notwendigkeit an Systemvertrauen zu und damit die Anforderungen an technische Standards, dieses notwendige Systemvertrauen nicht zu gefährden. Bezogen auf virtuelle Communities liegt die technische Umsetzung eines agentenbasierten Vertrauensmodells von Abdul-Rahman/Heiles (2000) vor. Der Ansatz setzt jedoch die eindeutige Bestimmbarkeit von formalen Identitäten voraus und modelliert kein Systemvertrauen, sondern bearbeitet interpersonelle und Reputationsmechanismen.

Ein einschlägiges Instrument, um Systemvertrauen aufzubauen, ist im Sinne des rational choice-Ansatzes eine Informations- und Kompetenzpolitik, also die Bereitstellung und Vermittlung von Wissen und – darauf basierend – der Aufbau der Fähigkeit, Risiken einzuschätzen und damit umzugehen. Schädler (1999) untersucht beispielsweise vertrauensbildende Maßnahmen hinsichtlich der verwendeten Techniken für Zahlungssysteme im Internet und zeigt, dass sich für eine Vertrauensbildung die Herstellung von Transparenz der Abläufe und die Aufklärung über die verwendeten Technologien und der abzuschätzenden Risiken anbieten. Vertrauensprofile, wie sie in eBay zu finden sind, basieren auf transaktionsorientierten Mechanismen, um das Vertrauen in Personen zu erhöhen, und stellen ein institutionalisiertes Feedback-Forum mit dezentralem Selbstregulierungsmechnanismus dar. Interessant sind hier nach Eggs u.a. (2002) vor allem Reputationsmechnismen, wie beispielsweise negative Reputationsdienste in Form von „Black Lists“ oder positive Reputationsdienste, mit denen korrektes Verhalten archiviert wird.

Neben der „Informations- und Kompetenzpolitik“ fördern Expertenmeinungen sowie technische Normung und Standards sowie deren Anwendung das Vertrauen (vgl. z.B. Sicherheit bei der Kreditkartenabrechnung über SET [was ist das?] etc.). Innerhalb der IT-Sicherheit spricht man von „Sicherheitspolitik“, um die strategische Ausrichtung und die Unterstützung der Geschäftsführung bei der Informationssicherheit zu beschreiben und um Ziele, Zwecksetzungen, Absichten und Hauptverantwortlichkeiten der IT-Sicherheit zu definieren. Für das Management der Informationssicherheit stellt der Standard ISO 17799[6] eine internationale Grundlage zur Verfügung und kann insofern als gutes Beispiel für die Vertrauensherstellung gesehen werden, wie sie innerhalb des Rational Choice-Ansatzes modelliert wird. Jedoch ist Informations- und Kompetenzpolitik zwar notwendig, aber nicht hinreichend, um ein „framework of trust“ für Communities zu entwickeln, das sich durch das Dreieck von Vertrauen, Identität und Technik auszeichnet.

Da dem Laien-Nutzer oft technisches Wissen zum Verständnis fehlt, nutzen Anbieter von technischen Systemen oft Zertifzierungsdienste, um die korrekte Funktionsweise und die „objektive Sicherheit“ von unabhängigen Dritten überprüfen zu lassen. Ein klassisches Beispiel dafür ist die Zertifizierung nach Verbraucherschutz-Richtlinien, wie es von www.trustedshops.de angeboten wird. „Trusted Shops entstand Anfang 2000 in enger Zusammen-

6 ISO17799 http://www.noweco.com/wp_iso17799d.htm, 2003.

arbeit mit Verbraucherschutzverbänden. Zielsetzung ist es, den Forderungen führender Politiker nach mehr Sicherheit im Internet gerecht zu werden – und dem Verbraucher diese Sicherheit auf Dauer zu bestätigen“ (http://www.trustedshops.de/de/shops/obligations_de.html [20.3.2003]).[7].

Um Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten zu schaffen, ist die Prüfung und Bewertung von IT-Produkten und IT-Systemen nach einheitlichen Qualitätskriterien durch unabhängige Stellen ein wichtiges Mittel. Als Grundlage wurden in vielen Ländern Kataloge von Sicherheitskriterien – allgemeiner und umfassender als die von Trusted Shops – für die Prüfung und Bewertung der Sicherheit von Informationstechnik erarbeitet[8]. Die geprüfte Sicherheitsleistung wird nach den Sicherheitskriterien durch ein Zertifikat bestätigt. Neben Sicherheitskriterien, Normung und Zertifizierungen fördern – wie schon erwähnt – Verbraucherverbände oder Experten- und Notfallteams wie das Computernotfallteam (CERT – Computer Emergency Response Team) die Vertrauensbildung aus institutioneller Sicht und stellen ebenfalls Systemvertrauen im Sinne Luhmannns und Giddens bezüglich Risikomanagement, Beherrschung und Erkennung von Bedrohungspotentialen und Sicherheitsvorfällen her.

Wir wollen nun die institutionelle Sichtweise auf die Vertrauensbildung verlassen und uns den Sicherheitsanforderungen und -maßnahmen, die von der Technik umgesetzt werden müssen, detaillierter widmen. Die Sicherheitskriterien, die bei der Zertifizierung und auch von Expertensystemen betrachtet werden, stehen in unmittelbarem Zusammenhang zu den bereits unter Vertrauen behandelten Sicherheitsaspekten Vertraulichkeit, Integrität, Authentizität, Nachweisbarkeit und Verfügbarkeit (vgl. Dittmann u.a. 2001). Im Wesentlichen nutzt man heute Sicherheitstechniken bzw. -mechanismen, die auf unterschiedlichen Ebenen der IT-Systeme wie dem Betriebssystem, dem Netzwerk oder der Anwendung angesiedelt sind, um die genannten Sicherheitsaspekte zu garantieren. Es handelt sich meist um Kombinationen aus technischen Verfahren wie:

(1) *Firewalls:* „Ein Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über den Firewall geführt werden muss. Auf dem Firewall sorgen Zugriffskontrolle und Audit dafür, dass das Prinzip der geringsten

7 Ein Online Shop, der das Trusted Shops-Siegel führen will, ist verpflichtet, während der gesamten Vertragslaufzeit mit der Trusted Shops GmbH die folgenden organisatorischen und technischen Voraussetzungen zu erfüllen: (1) Anbieterkennzeichnung, Vertragsschluss; (2) Allgemeine Geschäftsbedingungen, Vertriebs- und Marketingbeschränkungen; (3) Jugendschutz, Preistransparenz; (4) Zahlungsbedingungen, Bestellbestätigung; (5) nachverträgliche Informationen, Leistungserbringung; (6) Kundenservice, Widerrufs- oder Rückgaberecht und Kaufpreiserstattung, (7) Datenschutz, Daten- und Systemsicherheit.

8 Vgl. beispielsweise Department of Defense (1985), ITSEC (1991), NCSC (1991) oder NCSC (1987).

Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden“ (DFN CERT (2002). Eine Firewall übernimmt somit Zugriffsschutzmechanismen und kann das IT-System hinter der Firewall vor fremdem Zugriff schützen, kann aber auch sicherstellen, dass der Zugriff nach außen unterbleibt. Man findet Firewalltechniken beispielsweise zur Abgrenzung des Intranets zum Internet.

(2) *Kryptographische Verfahren:* Kryptographische Mechanismen basieren auf mathematischen Verfahren, auch Kryptosysteme genannt, die meist zur Verschlüsselung der Daten benutzt werden, um Vertraulichkeit zu garantieren oder mittels digitaler Signaturen zum Nachweis der Unversehrtheit und Authentizität dienen. Nach Dittmann u.a. (2000) bestehen Kryptosysteme aus zwei Mengen an Funktionen, einer Menge an Schlüsseln, durch die diese Funktionen parametrisiert werden, und aus Mengen, auf denen diese Funktionen operieren. Man unterscheidet zwischen symmetrischen Kryptosystemen (oder Private-Key-Kryptosystemen) und asymmetrischen Kryptosystemen (oder Public-Key-Kryptosystemen). „Die Kryptographie beruht neben der Annahme über die Berechenbarkeiten von Funktionen auf der Voraussetzung, dass Daten, die für kryptographische Mechanismen eingesetzt werden, authentisch sind (beispielsweise durch ihre Veröffentlichung) oder ihre Authentizität geprüft werden kann. Ein Datum oder eine Partei gilt dann als echt, wenn ein Prüfer einen Beweis akzeptiert, in dem ein Geheimnis verwendet wird, bei dem der Prüfer davon ausgeht, dass dieses Geheimnis nur dem rechtmäßigen Besitzer oder den rechtmäßigen Besitzern bekannt ist. Jeder andere, der das Geheimnis kennt, also auch ein Betrüger, kann das Geheimnis ebenfalls für einen entsprechenden Beweis einsetzen. Es ist Aufgabe der Sicherheitsstrategie (Security Policy) der jeweiligen Anwendung festzulegen, ob ein Prüfer einen Beweis akzeptieren kann. Die Sicherheitsstrategie muss definieren, wie hoch das Sicherheitsniveau der Anwendung zu setzen ist, beispielsweise: wie streng die Auflagen an die Sicherheit von Geheimnissen (wie Größe, Anzahl aber auch Aufbewahrungsort) sind und mit welchem Verfahren der Sicherheitsmechanismus realisiert wird, damit er als sicher im Sinne der Sicherheitsstrategie gilt. Hier müssen Kosten, die durch den Einsatz von Sicherheitsmechanismen entstehen, und Kosten, die durch Schäden ohne oder von in nur geringem Maße eingesetzten Sicherheitsmechanismen aufkommen, gegeneinander abgewogen werden.“ (Dittmann 2002, S. 110).

(3) *Steganographische Verfahren:* Die Steganographie hat den Zweck, Nachrichten in anderen Nachrichten zu verstecken, um die bloße Existenz einer geheimen Botschaft zu verbergen (vgl. Schneier 1996). Die Steganographie nutzt zur geheimen Kommunikation die Präsenz anderer Kommunikation und bietet Mechanismen zur Gewährleistung der Vertraulichkeit. Derzeit verbreitet sind Verfahren, die in digitalem Bildmaterial, das auf zugänglichen Quellen wie der Webseite Nachrichten in den Farbwerten verbirgt, die vom menschlichen Auge nicht wahrgenommen

werden können. Nur bei Kenntnis von geheimen Schlüsseln kann die Nachricht zugänglich gemacht werden.

(4) *Digitale Wasserzeichen:* Mit digitalen Wasserzeichen kann die Authentizität der Urheber und die Herkunft des Datenmaterials und/oder die Integrität nachgewiesen werden, indem Informationen direkt in das Datenmaterial eingefügt werden. Unter einem digitalen Wasserzeichen versteht man nach Dittmann (2000) ein transparentes, nicht unmittelbar wahrnehmbares Muster, welches in das Datenmaterial (Bild, Video, Audio, 3D-Modelle) mit einem Einbettungsalgorithmus unter Verwendung eines geheimen Schlüssels eingebracht wird und mit einem Schlüssel wieder ausgelesen werden kann, um die Authentizität bzw. Integrität zu verifizieren.

Einschlägige Diskussionen zu heutigen Verfahren und dem damit zu erzielenden Sicherheitsniveau findet man beispielsweise in Bishop (2003) und Pfleeger u.a. (2003). Weitergehende vertrauenbildende technische Verfahren sind etwa Verfahren zur Anonymisierung oder Pseudonymisierung. Welchen Einfluss hat nun die Wahl von technischen Sicherheitsmechnismen auf die Vertrauensbildung? Klar ist, dass das Vertrauen durch die Gesamtheit der einzelnen Sicherheitsmechnismen beeinflusst wird. Die institutionelle Vertrauensbildung mittels Zertifizierung filtert nach anerkannten Verfahren. Die Praxis zeigt aber, dass ein zertifiziertes System institutionelles Vertrauen aufweisen kann, es jedoch in der Praxis trotz Zertifizierung nicht angenommen wird, da Sicherheitsmechnismen verwendet werden, die nur unter Vorbehalt akzeptiert werden. Ein Beispiel dafür ist die Überprüfung der Microsoft Produktaktivierung durch TÜViT (2001)[9]. Obwohl keinerlei Anhaltspunkte gefunden wurden, dass irgendwelche personenbezogenen Daten über das Internet übertragen werden, bestehen bei Anwendern Bedenken, auf Windows XP umzurüsten. Für die Vertrauensbildung bedeutet dies, dass neben dem institutionellen Vertrauen auch Vertrauen in die einzelnen technischen Komponenten vorhanden sein muss, allgemeines Systemvertrauen reicht also nicht aus.

Abschließend sei ein Aspekt erwähnt, der in anderen Zusammenhängen sicherlich noch eine eingehendere Erörterung verdient: Die bisherige Thematisierung von Vertrauen, insbesondere die modernitätstheoretische Sicht nach Giddens und die Perspektive des Rational-Choice-Ansatzes, geht von einem einseitigen Modell der Betrachtung der Vertrauensbeziehung wie bei der Arzt-Patienten-Beziehung aus. Rein technisch gesehen finden wir im Internet jedoch auch Ansätze eines zweiseitigen Modells: Vor allem ist hier das HTTPS-Protokoll zu nennen (vgl. Details beispielsweise in Pfleeger u.a. 2003), bei dem beim Zugang auf eine Webseite eine Serverauthentifzierung vorgenommen wird und nach erfolgreicher Prüfung des Servers die Kommunikation vertraulich über Verschlüsselung erfolgt. In den technischen Sicherheitskonzepten findet man beim HTTPS-Protkoll aber auch eine sogenannte Client-

9 TÜVIT (2002): Microsoft Produktaktivierung durch TÜViT geprüft!, http://www.tuvit.de/XS/ASP/content.050300/sprache.DE/EID.25/SX/

Authentifzierung, die, bevor die Kommunikation stattfindet, auch die Clientauthentizität überprüft und somit ein zweiseitiges Vertrauensmodell darstellt.

### *3.3 Identität als Bedingung von Vertrauen und Technik*

Die Diskussion der sozialwissenschaftlichen Thematisierung von Vertrauen hat gezeigt, dass die Identifizierung der Person (formale Identität) eine grundlegende Voraussetzung für Vertrauensmodelle darstellt. Communties mit ihren Akteuren in der digitalen Welt sind virtuell, woraus sich zusätzliche Problemstellungen der Identifizierung der Nutzer hinter den Akteuren ergeben, auf die wir jetzt eingehen wollen. Wir bearbeiten in diesem Aufsatz also nicht die Aspekte der persönlichen Identität und der Rollenidentität in virtuellen Communities (vgl. dazu u.a. Döring 1998, Turkle 1995, Marotzki 1997).

Die eBay Geschäftsbedingungen umreißen prägnant die Problemlage: „(1) Beim Handel über das Internet bestehen Risiken, die in der Natur des Mediums liegen. Da die Identifizierung von Nutzern im Internet schwierig ist, kann eBay nicht zusichern, dass jeder Nutzer die natürliche oder juristische Person ist, für die er sich ausgibt. Trotz unterschiedlicher Maßnahmen durch eBay ist es möglich, dass ein Nutzer falsche Adressdaten gegenüber eBay angegeben hat. Der Nutzer hat sich deshalb selbst von der Identität seines Vertragspartners zu überzeugen“ (eBay AGBn § 4).

Die von Bishop (2003) definierte Identität als eine Computerrepräsentation einer Entität ist eine Form dessen, was wir oben *formale Identität* genannt haben. Formale Identitäten (im Sinne der eindeutigen Identifizierung eines Nutzers) legen die Basis für die Zuordnung von Privilegien und sind integrale Voraussetzung für die Bestimmung und Benennung von Schutzdomänen in der IT-Sicherheit. Die Authentifizierung bindet eine Entität an eine interne Repräsentation der Identität im Computersystem, wobei jedes Computersystem seine eigene Art und Weise der Repräsentation von formaler Identität hat. Alle Entscheidungen, wie Zugriffe und Ressourcenfreigaben, nehmen an, dass die Bindung von Entität und zugeordneter Identität korrekt sind.

Diese formale Identität hat verschiedene Zwecke, zwei wesentliche sind Zurechenbarkeit und Zugriffskontrolle. Die Zurechenbarkeit erfordert eine Identität, die alle Aktionen eindeutig einer Entität zuordnen lassen. Zugriffskontrolle erfordert eine Identität, die Zugriffskontrollmechanismen nutzen können, um zu entscheiden, ob ein Zugriff erlaubt ist oder nicht. Zurechenbarkeit knüpft somit an die Möglichkeit an, mittels Identitäten Protokollierungen und Auditierungen durchzuführen, und erfordert eine eindeutige Identifizierung der Entität. In vielen Systemen ist dies schwer oder nicht möglich, deshalb wird die protokollierte Identität abgebildet auf ein Nutzerkonto (user account). Die meisten Systeme bestimmen die Zugriffsrechte auf der Grundlage der Identitäten der Entität, die eine bestimmte Aktion ausführt.

In der IT-Sicherheit finden wir nach Bishop (2003) Identitäten für alle Entitäten eines Computersystems: Diese reichen von Identiäten von einzelnen Nutzern und Gruppen von Nutzern, bis hin zu Identitäten von Dateien und Objekten. Im allgemeinen werden Identitäten durch *Bezeichner* (Identifier) eindeutig unterschieden. Probleme, die bei einer eindeutigen Zuordnung von Entitäten und Identitäten auftreten können, sind zum Beispiel die Wahl von eindeutigen Bezeichnern bei gleichen Namen von Nutzern, statische oder dynamische Bezeichner, Gewährleistung von Anonymität von den Identitäten zugeordneten Nutzern (vgl. Bishop 2003).

Im Folgenden wollen wir untersuchen, welche technischen Mechanismen es gibt, Nutzern (Offline-Personen) eine formale Online-Identität zuzuordnen und diese zu überprüfen. Im ersten Schritt wird eine Authentifizierung der Nutzer vorgenommen, d.h. einem Nutzer wird im System eine Identität zugeordnet. Dabei kann überpüft werden, ob der Benutzer überhaupt berechtigt ist, eine formale Identität zu erhalten, wie es zum Beispiel auch auf den Meldestellen bei der Passausfertigung erfolgt. Im zweiten Schritt kann dann der Nutzer mit der erhaltenen Identität (im übertragenen Sinne also mit seinem Pass) sich gegenüber dem System authentifizieren.

Um eine Authentifizierung vornehmen zu können, muss der Nutzer Informationen bereitstellen, um das System in die Lage zu versetzen, dass es die Identität prüfen und bestätigen kann. Als hinterlegte Informationen zur Authentifizierung und Identifizierung der Nutzer kommen in der Regel Folgende in Frage: (1) *Wissen:* Passwörter, geheime Information; (2) *Besitz:* Chipkarten, Schlüssel; (3) *Sein:* biometrische Merkmale wie Fingerabdruck, Retina oder Stimme. Die wohl gängigste Form der Authentifizierung und Überprüfung von Identitäten ist das Password (Wissen). Meist wird auch eine Kombination benutzt, beispielsweise werden geheime Informationen auf einer Chipkarte (Besitz) freigeschaltet über ein Password (Wissen) und/oder ein biometrisches Merkmal (Sein). Das System, das den Nutzer identifiziert und seine Identität überprüft, muss nicht unbedingt die komplette Information über Wissen, Besitz und Sein hinterlegt haben. Oft werden Abstraktionen im System aufbewahrt, um Angreifern zu erschweren, die Authentifizierungsinformation auszuspähen, um eine Identität vorzutäuschen. Authentifizierungsmechanismen können des Weiteren bei der Identifizierung eine örtliche und/oder zeitliche Überprüfung einbeziehen, beispielsweise, wo der Nutzer sich befindet (vor dem Terminal oder in einem bestimmten Gebäude) und zu welcher Zeit er sich dort befindet.

Hinsichtlich der Vertrauensbildung spielt die Überprüfung einer Identität und die Zuordnung zu einer Person (einem Nutzer) eine wesentliche Rolle, da die vertrauensbildenden Maßnahmen die eindeutige Identifizierung der Person voraussetzen. Bei formalen Identitäten ist der Authentifizierungsprozess, die Zuordnung einer Person zu einer formalen Identität, ein kritischer und vertrauensbeinflussender Vorgang. Will man sichergehen, dass eine Identität einer realen Person beweisfähig zugeordnet ist, wie man es beispielsweise bei notariellen Vertragsabschlüssen vorfindet, wird man bei der

Authentifizierung die Zuordnung von Name und Anschrift über den Personalausweis durch persönliche Überprüfung der Ausweisdaten vornehmen müssen. Dieses Vorgehen findet man beispielweise im Rahmen der elektronischen Signatur, bei dem ein öffentlicher Schlüssel eindeutig einer Person mit Namen zugeordnet wird. Auf der Grundlage des Erscheinens der Person bei einer zentralen Vertrauensinstanz (Trusted Third Party) und der Vorlage des Ausweises wird über ein Zertifikat der öffentliche Schlüssel der Person zugeordnet. In weniger sicherheitsrelevanten Bereichen, wie der privaten oder firmeninternen Kommunikation, findet man auch dezentrale Authentifizierungsverfahren, bei denen sich Nutzer untereinander authentifizieren. Ein Beispiel dafür ist das „Pretty Good Privacy" (PGP) Email Verschlüsselungswerkzeug, bei der ebenfalls ein öffentlicher Schlüssel einem Email-Nutzer zugeordnet wird. Im PGP bescheinigen die Nutzer untereinander, den anderen zu kennen, wodurch dezentrale Vertrauensbildung erfolgt.

Zur Vertrauensbildung in virtuellen Communities können die bekannten Mechnismen von *Besitz-Wissen-Sein* genutzt werden, um Identitäten festzustellen. Wichtig ist jedoch, dass es in der digitalen Welt und somit in virtuellen Communities möglich ist, mehrere formale Online-Identitäten zu haben, die auf *eine* Offline-Identität abgebildet werden, ohne dass dies für andere Nutzer transparent ist. Des weiteren ist es möglich, die Online-Identitäten an andere Offline-Identitäten weiterzugeben, sei es zeitweise oder unbeschränkt, um beispielweise positive Reputationsmechanismen auszunutzen[10]. Weiter können zu einer Offline-Identität ständig neue Online-Identitäten entstehen oder ausgelöscht werden, um beispielweise negative Reputationen abzustreifen. Ebenso kann hinter einer Online-Identität eine ganze Gruppe von realen Nutzern stehen.

Wichtig für die Vertrauensbildung erscheint uns, die digitalen Online-Identitäten mit Attributen zu versehen, die anzeigen, inwieweit die Zuordnung zu einer realen Person oder zu einem realen Personenkreis möglich ist und ob ein Wechsel der Online-Identität vorgenommen wurde. Abgestufte und ausgewogene technische Authentifizierungsmechanismen (auf der Basis von Besitz, Wissen und Sein) sowie organisatorische Authentifizierungsmechanismen (zentraler und/oder dezentraler Überprüfungen realer Identitäten), die einerseits Identitäten für die Vertrauensbildung nachvollziehbar machen, andererseits auch die Privatspäre und Anonymität berücksichtigen, stellen vielversprechende Lösungskonzepte in virtuellen Communties dar und werden in den nächsten Jahren mit Sicherheit weiterentwickelt werden.

10 Spieler von Online-Computerspielen, die in bestimmten Spielen mit ihrem Avatar eine bestimmte Punktzahl erreicht haben, verkaufen (oder versteigern) gelegentlich ihren Avatar. Der Käufer kann dann mit diesem Avatar, der dann „seiner" ist, mit einer hohen Reputation (= hohe Punktezahl) in das Spiel einsteigen.

## 4. Schlussbemerkung

Interessant für die weitere Forschung erscheint die Tatsache, dass in virtuellen Communities „digital lebende“ Avatare existieren können, die aus ihren sozialen Erfahrungen lernen und beispielsweise aufgrund dieser Erfahrungen ihre Identity-Card verändern, gleichsam ihre digitale Biographie umschreiben, ohne dass dieses von der Offline-Person veranlasst und vielleicht auch bemerkt wird. Die Avatare (Online-Personen) können auf diese Weise sich von der Offline-Person gleichsam ablösen und ein eigenes Leben führen. Das wären Themen, die genauer zu untersuchen sind, wenn man sich Fragen von persönlicher Identität und Rollenidentität zuwendet, wie sie sich in virtuellen Communities entwickeln.

Auch wenn wir uns in dieser Arbeit nur auf die formale Identität bezogen und deren Bedingungsverhältnis zu Vertrauen und Technik erörtert haben, dürfte doch deutlich geworden sein, dass ein Framework zur Vertrauensbildung für virtuelle Communities ein umfassendes Spektrum an Maßnahmen erfordert, um die wesentlichen Beziehungen des Verhältnisses Identität, Technik und Vertrauen abzudecken.

## Literatur

*Abdul-Rahman, A./Heiles, St.:* Supporting Trust in Virtual Communities, HICSS, [citeseer.nj.nec.com/article/abdul-rahmanOOsupporting.html] 2000.

*Bishop, M.:* Computer Security – Art and Science. Boston 2003.

*Brinkmann, U./Seifert, M.:* “Face to Interface”. Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. In: Zeitschrift für Soziologie 30 (2001), S. 23-47.

*BSI – Bundesamt fur Sicherheit in der Informationstechnik:* Grundschutzhandbuch. [http://www.bsi.de/gshb/index.htm] (30.3.2003).

*Coleman, J. S.:* Grundlagen der Sozialtheorie. Bd. 1: Handlungen und Handlungssysteme. München 1991.

*Department of Defense:* Department of Defense Trusted Computer System Evaluation Criteria (Orange Book). DOD 5200.28-STD, Dec 1985

*DFN CERT:* Zentrum für sichere Netzdienste GmbH, [http://www.cert.dfn.de] (20.3.2003). 2002.

*Diekmann, A./Wyder, D.:* Vertrauen und Reputationseffekte bei Internet-Auktionen. In: Kölner Zeitschrift für Soziologie und Sozia1psycho1ogie.4/2002, S. 674-693.

*Dittmann, J:* Digitale Wasserzeichen. Berlin 2000.

*Dittmann, J./Wohlmacher, P./Nahrstedt, K:* Multimedia and Security – Using Cryptographic and Watermarking Algorithms, IEEE MultiMedia, October-December 2001, Vol. 8, No. 4, pp. 54-65.

*Döring, N:* Sozialpsychologie des Internet – Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen. Göttingen 1998.
*Eggs, H./Sackmann, St./Eymann, T./Müller, G.:* Vertrauen und Reputation in P2P-

Netzwerken. In: Peer-to-Peer-Ökonomische, technologische und juristische Perspektiven. Berlin 2002, S. 229-254.

*Endress, M.:* Vertrauen. Bielefeld 2002.

*Giddens, A.:* Konsequenzen der Moderne. Frankfurt a.M.1996.

*Grimm, R.:* Sicherheit für offene Kommunikation, Mannheim 1994.

*Henslin, J. M.:* Trust and the Cab Driver. In: Truzzi, M. (Hrsg.): Sociology and Everyday Life. Englewood Cliffs NJ 1968, S. 139-159.

*Horster, P. (Hrsg.):* DACH Security. Erfurt (syssec IT Security & IT Management). Erfurt 2003

*Intern.de:* Wie zuverlässig ist eBays Bewertungssystem? In: Intern.de Fachinformationsdienst Ausgabe 13/2003 vom 31.2.2003 (http://www.intern.de/news/4105.htm1 [31.3.2003]).

*ITSEC (Information Technology Security Evaluation Criteria):* Provisional Harmonised Criteria. Version 1.2, Juni 1991.

*Joy, B.:* Warum die Zukunft uns nicht braucht. In: Frankfurter Allgemeine Zeitung Dienstag, 6. Juni 2000. Nr. 130, S. 49.

*Luhmann, N:* Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. 4. Auflage 2000. Stuttgart 1968.

*Marotzki, W:* Digitalisierte Biographien? Sozialisations- und bildungstheoretische Perspektiven virtueller Welten. In: Lenzen, D.;/Luhmann, N. (Hrsg.): Bildung und Weiterbildung im Erziehungssystem. Lebenslauf und Humanontogenese als Medium und Form. Frankfurt a.M. 1997, S. 175-198.

*Moravec, H.:* Robot: Mere Machine to Transcendent Mind. Oxford 1999.

*NCSC (National Computer Security Center):* Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (Red Book). NCSC-TG-005, Version 1, Jul 1987.

*NCSC (National Computer Security Center):* Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria. NCSC-TG-021, Version 1, Apr 1991.

*Pfleeger, C. P./Pfleeger, S. L:* Security in Computing, 3rd Edition, New Jersey 2003. *Preisendörfer, P.:* Vertrauen als soziologische Kategorie. Möglichkeiten und Grenzen einer entscheidungstheoretischen Fundierung des Vertrauenskonzepts. In: Zeitschrift für Soziologie 24. 1995, S. 263-272.

*Reimer, H.:* TeleTrust: Informationssicherheit als interdisziplinäre Aufgabe, In: Horster (Hrsg.): DACH Security. Erfurt 2003. S. 1-15.

*Reitenspiess, M.:* IT-Sicherhit – Quo Vadis? In: Horster, P. (Hrsg.): DACH Security. Erfurt 2003, S. 16-32.

*Richards, J. u.a.:* Are we Spiritual Machines? Ray Kurzweil vs. the Critics of Strong A.I. Seattle, Washington 2002.

*Rössler, P./Wirth, W. (Hrsg.):* Glaubwürdigkeit im Internet. Fragestellungen, Modelle, empirische Befunde. München 1999.

*Schädler, M.:* Institutionelle Aspekte der Vertrauensbildung bei Zahlungssystemen im Internet, Diplomarbeit, [http://www.ub.uni-konstanz.de/kops/volltexte/2000/407/.] 1999.

*Schneier, B.:* Angewandte Kryptographie. München 1996.

*Sztompka, P.:* Vertrauen: Die fehlende Ressource in der postkommunistischen Gesellschaft. In: Nedelmann, B. (Hrsg.): Politische Institutionen im Wandel. Sonderheft 35 der Kölner Zeitschrift für Soziologie und Sozialpsychologie. 1995, S. 254-276.

*Turkle, S.:* Life on the Screen. Identity in the Age of the Internet. London 1995.

*Winkel O.:* Die Förderung von Vertrauen, Glaubwürdigkeit und Verläßlichkeit. Welchen Beitrag kann die elektronische Verschlüsselung dazu leisten? In: Rössler/Wirth (Hrsg.) 1999. S. 193-208.