

Dr. Guido Möllering

Max-Planck-Institut für Gesellschaftsforschung, Köln

gm@mpifg.de

## **Vernebeltes Vertrauen?**

### **Cloud Computing aus Sicht der Vertrauensforschung**

– Vortragsmanuskript –

Es ist eine Ehre und auch eine Herausforderung, bei dieser Fachkonferenz, in deren Zentrum vor allem technische und technologische Fragen stehen, die Sichtweise der sozialwissenschaftlichen Vertrauensforschung zu vertreten und Ihnen näher zu bringen. Es spricht für sich – oder besser gesagt: es spricht für Sie, dass Sie das innovative Thema Cloud Computing mit einem Klassiker des menschlichen Zusammenlebens und Zusammenarbeitens verknüpfen, nämlich mit Vertrauen. Klingt dieser Begriff – Vertrauen – in Ihren Ohren nicht ein wenig verstaubt, altmodisch oder gar weltfremd? Brauchen wir ihn wirklich, wenn wir über die neuesten und fortschrittlichsten Informationstechnologien sprechen? Uns allen hier im Saal sollte klar sein, dass Cloud Computing nicht losgelöst von sozialen Kontexten und Beziehungen stattfindet und dass eben gerade auch im Internet die Bedingungen der Ungewissheit und Verwundbarkeit gegeben sind, die Vertrauen als Problem und zugleich als dessen Lösung ins Spiel bringen.

#### **Das Bild der Wolke**

„Cloud“ Computing, Informationsverarbeitung in der Internet „Wolke“. Inzwischen nimmt man vom Bild der Wolke vielleicht kaum noch Notiz. Man verwendet in Diagrammen ohne weiteres das Wolkensymbol für das Internet. Ich lade Sie ein, dieses Bild der Wolke einmal wieder ernst zu nehmen. Die Problematik des Vertrauens im Cloud Computing lässt sich nämlich damit schon sehr schön in einem ersten Zugang erschließen. Stellen Sie sich bitte vor, wie es ist, wenn man mit dem Flugzeug in eine Wolke fliegt, als Wanderer oder vielleicht auch als Skifahrer im Gebirge von einer Wolke eingeschlossen wird, oder wenn man mit dem Auto in den Nebel fährt. Man sieht dann kaum noch die anderen Akteure – also die anderen Flugzeuge, Wanderer, Skifahrer, Autos – und was sie tun. Man verliert gar die Orientierung und kann sich nur mit großer Vorsicht fortbewegen. Man sucht vor allem auch nach Orientierungspunkten. Mit Radar, GPS und Nebelscheinwerfern wird die Situation dank technischer Hilfsmittel um einiges ungefährlicher. Jedoch bleibt die Sorge, dass andere Akteure fahrläs-

sig oder gar böswillig im Nebel unterwegs sein könnten. Ohne Vertrauen, müsste man wohl auf der Stelle stehen bleiben und wäre selbst dann nicht in Sicherheit. Oder man müsste jede Wolke und jede Nebelbank meiden – und alle Chancen, die darin liegen, verpassen. Auch in der Internet Wolke haben wir vergleichsweise „schlechte Sicht“, können die anderen Akteure nur zum Teil kennen und kontrollieren und stoßen mit unseren technischen Hilfsmitteln immer wieder an Grenzen. Vertrauen macht Kooperation unter diesen Umständen möglich, ist selbst jedoch unter solchen Umständen schwerer aufzubauen und zu erhalten. Der Nebel kann nicht beseitigt werden und die Technologien sind nicht perfekt, aber wir können Orientierungspunkte für Vertrauen schaffen.

### Vertrauensforschung

Bevor ich auf die Besonderheiten des Vertrauens im Cloud Computing eingehe, gestatten Sie mir noch einige Anmerkungen zur Vertrauensforschung im Allgemeinen. Die (eine) Vertrauensforschung als ein klar abgegrenztes, homogenes Feld gibt es gar nicht. Es handelt sich vielmehr um ein ausgesprochen heterogenes Feld, auf dem sich Wissenschaftler aus den verschiedensten Disziplinen tummeln und alle möglichen Forschungsfragen bearbeiten, die mit Vertrauen zu tun haben. Zwar gibt es auch gemeinsame Bezugspunkte – in Deutschland kommt man zum Beispiel kaum an dem kleinen, sehr scharfsinnigen Buch zu Vertrauen von Niklas Luhmann vorbei – doch oft widmen sich Forscher dem Thema eher ad hoc und improvisieren bei den theoretischen und methodischen Grundlagen, statt auf eine Art Kanon zurückzugreifen. Den gibt es schlichtweg noch nicht, auch wenn hier und da schon Handbücher zu Vertrauen herausgegeben wurden (vgl. Literaturhinweise hinten).

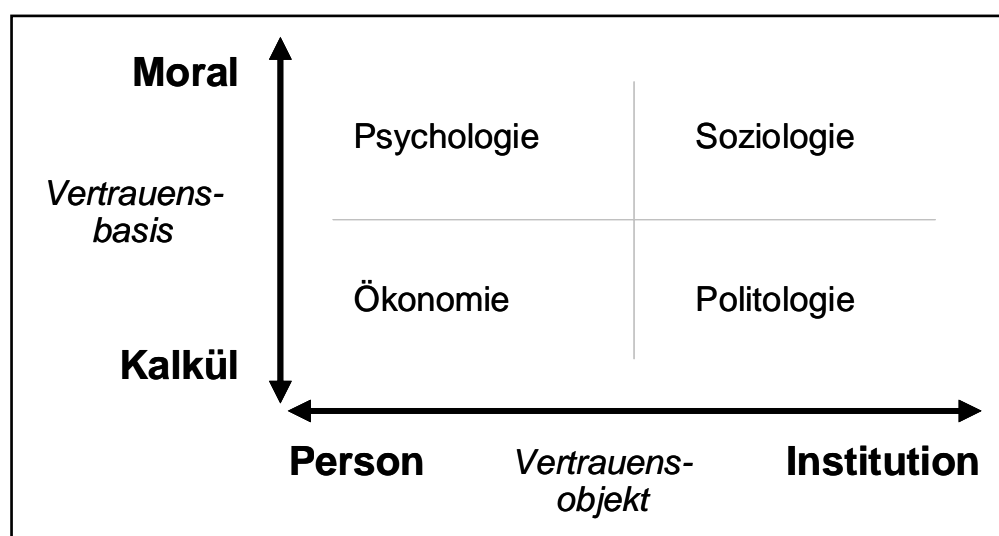


Abbildung 1 – Sozialwissenschaftliche Vertrauensforschung

Vertrauen ist vor allem eine soziale Kategorie – zumindest auch, wenn man vom Alltagsverständnis des Begriffes ausgeht. Es geht um Beziehungen zwischen Akteuren, die sich gegenseitig wahrnehmen und dies in ihrem Handeln berücksichtigen. Und so ist es kaum verwunderlich, dass sich vor allem die Sozialwissenschaften mit diesem Thema befassen. Hier wiederum kann man stark vereinfachend die in Abbildung 1 dargestellte Systematik beobachten. Ein Teil der Forscher – insbesondere in der Ökonomie und der Politikwissenschaft – sieht als Basis des Vertrauens vor allem ein Kalkül, während andere Wissenschaftler – vor allem Psychologen und Soziologen – moralische und emotionale Grundlagen von Vertrauen betonen. In einer zweiten Dimension kann man unterscheiden, ob es um Vertrauen in Personen oder Vertrauen in Institutionen geht. Hier stehen sich die Ökonomie und die Psychologie nahe, weil sie meist Interaktionen zwischen konkreten Akteuren vor Augen haben, während die Politologen und Soziologen eher abstrakte Vertrauensobjekte betrachten.

Man muss natürlich hinzufügen, dass die Grenzen zwischen den Disziplinen hier auch fließend sind. Ich selbst habe mich von Anfang an einem interdisziplinären Ansatz verschrieben. Es bringt wenig, sich darüber zu streiten, in welcher der vier Ecken das „echte“ Vertrauen steckt. Vielmehr geht es in dem ganzen Feld darum, positive Erwartungen trotz Ungewissheit und Verwundbarkeit zu erklären. Also sollte man auch Erkenntnisse aus allen Disziplinen nutzen. Vielleicht kommt hier zum Ausdruck, dass ich ein Organisationsforscher aus der BWL bin. Leute wie ich beschäftigen sich eben meist mit Organisationen auf einer mittleren Ebene zwischen Mikro- und Makroebene und analysieren vor allem auch das Zusammenspiel von Mikro und Makro. Und die BWL als anwendungsorientierte Wissenschaft kann es sich gar nicht leisten, die reine Theorie zu pflegen, sondern muss realitätsnah für alle Einflussfaktoren offen sein, auch wenn sie in einer ungewohnten Disziplin entdeckt wurden.

Diese Offenheit gilt grundsätzlich auch gegenüber den Natur- und Ingenieurwissenschaften, die ebenfalls etwas zu Vertrauen zu sagen haben. In den Naturwissenschaften ist dies vor allem die neurowissenschaftliche Forschung, die viel Aufmerksamkeit erhält und durchaus interessant ist. Allerdings muss ich gestehen, dass mir zum Beispiel Studien darüber, welche Hirnareale in simulierten Vertrauenssituationen besonders aktiv sind, noch keine Erklärungen für Vertrauen geliefert haben, auf die man nicht auch schon mit anderen Methoden gekommen wäre. Das gilt auch für die Studien über sogenannte Vertrauenshormone. Hier sehe ich es sogar mit Sorge, dass man einmal auf die Idee kommen könnte, Oxytocin-Sprays zu verteilen. Momentan ist es noch schwer, den Oxytocin-Spiegel bei Menschen künstlich zu erhöhen, doch die Pharmaforschung kann da bestimmt helfen. Aber wollen wir das Vertrauen im Internet mit Drogen steigern? Oder durch Aufrufe, wie sie zumindest halbernst aus den USA kommen, die Leute müssten einfach mehr kuscheln, weil sie dann mehr Hormone im Blut haben, die Vertrauen bewirken?

In den Ingenieurwissenschaften gibt es Beiträge zur Vertrauensforschung gerade auch im Bereich der neuen Informationstechnologien. Man beschäftigt sich hier – nah an der Ökonomie – zum Beispiel mit Zertifizierungssystemen und Reputationsmechanismen. Außerdem gibt es Studien – näher an der Psychologie – die vereinfacht gesagt analysieren, wie Vertrauensbereitschaft mit Webdesign zusammenhängt. Zuletzt erwähnt seien hier noch die vielfältigen Forschungen darüber, wie man gefälschte Daten automatisch erkennen kann, was sicherlich auch für das Thema Cloud Computing relevant ist. Diese Art der Forschung macht sehr viel Sinn, jedoch muss ich aus einer allgemeinen Perspektive der Vertrauensforschung kritisieren, dass hier häufig nicht zum Kern der Vertrauensproblematik vorgedrungen wird, sondern man an der technischen Oberfläche bleibt. Was aber ist der Kern der Vertrauensproblematik? Was macht Vertrauen aus? Vor allem: Wie kann man es definieren?

### **Definition von Vertrauen**

Ich beanspruche selbstverständlich keine Allgemeingültigkeit, jedoch schlage ich vor, von folgender allgemeinen Definition auszugehen: Vertrauen bedeutet, trotz Ungewissheit und Verwundbarkeit zu erwarten, dass andere ihre Freiräume kompetent und verantwortungsvoll nutzen. Diese kurze Definition hat es in sich. Schauen wir uns das einmal genauer an. Beim Vertrauen geht es also um positive Erwartungen. Die anderen, in die die Erwartungen gesetzt werden, können sehr spezifische Personen oder aber eher abstrakte Akteure sein. Das spielt hier zunächst noch keine große Rolle, darauf komme ich aber noch zurück.

Wichtiger ist mir hier zunächst, erstens, dass Vertrauen sich auf die Freiräume der anderen bezieht. Diese Freiräume werden also vorausgesetzt oder, anders ausgedrückt: Wenn andere keine Freiräume haben, dann braucht man ihnen auch nicht zu vertrauen. Dann hat man ja vollkommene Sicherheit. Wenn Sie meinen, dass Cloud Computing nur dann funktioniert, wenn die Beteiligten gar keine Freiräume haben, um eventuell in irgendeiner Weise unkooperativ zu handeln, dann reden wir einseitig von Kontrolle und haben es eigentlich gar nicht mehr mit Vertrauen zu tun. Wenn wir allerdings davon ausgehen, dass immer Freiräume bleiben werden und dass dies sogar sehr wünschenswert ist, denn wir schätzen am Internet ja gerade auch seine Offenheit und Flexibilität, dann sehen wir unmittelbar wieder die Notwendigkeit des Vertrauens.

Zweiten ist Vertrauen als positive Erwartungshaltung nicht naiv oder bedingungslos. Die Definition verweist auf Kompetenz und Verantwortungsbereitschaft. Diese will der Vertrauensgeber beim Vertrauensnehmer sehen. Erweist sich der Vertrauensnehmer als inkompetent oder übernimmt er beim Auftreten von Problemen und Fehlern keine Verantwortung oder

erfüllt er ganz allgemein die positiven Erwartungen nicht, dann kann Vertrauen natürlich auch wieder entzogen werden. Doch zunächst gibt Vertrauen dem anderen die Chance, sich freiwillig als vertrauenswürdig zu erweisen, indem er seine Freiräume nicht missbraucht.

Drittens steckt im Phänomen des Vertrauens noch eine ganz spezielle Eigenheit, geradezu eine Zumutung: Vertrauen ist eine positive Erwartung trotz Ungewissheit und Verwundbarkeit. Vertrauen wird erst unter den Bedingungen der Ungewissheit und Verwundbarkeit relevant und setzt sich dann quasi über diese hinweg. Der Vertrauende weiß also nicht mit Sicherheit, wie der andere seine Freiräume nutzen wird, und ein Missbrauch würde dem Vertrauenden auch schaden. Aber er nimmt dennoch das Beste an und gibt der Kooperation eine Chance. Er tut dies nicht blind, hat dafür gute Gründe, aber eben keine perfekten Gründe. Es bleibt eine Lücke, die mit Vertrauen überbrückt wird. Es bleibt der Nebel, man bleibt vorsichtig, aber man bewegt sich trotzdem. Man handelt, als ob man wüsste, dass alles gut gehen wird. Und schon wieder wirkt Vertrauen naiv und weltfremd, doch ich sage Ihnen: Nein, Vertrauen dieser Art macht handlungsfähig und ist außerdem ganz alltäglich.

Ich bin gerne bereit, dieses Vertrauensverständnis mit Ihnen weiter zu diskutieren. Für die heutige Fachkonferenz möchte ich an dieser Stelle folgende Anregung festhalten: Denken Sie darüber nach, welchen Status die Freiräume der Akteure im Cloud Computing haben. Und machen Sie sich stets bewusst, ob es in Ihren Diskussionen um die Begrenzung oder Ausweitung dieser Freiräume geht. Oder ob es um die Akzeptanz der Freiräume und um deren kompetente und verantwortungsvolle Nutzung geht. Verwechseln Sie also nicht Kontrolle mit Vertrauen und vergessen Sie nicht, dass Kontrolle und Vertrauen beide nötig sind.

### **Generalisiertes Vertrauen**

Ich komme nun zu einigen Besonderheiten des Vertrauens im Cloud Computing und werde mich dabei im Wesentlichen auf zwei Hauptpunkte beschränken: Zum einen ist im Cloud Computing das generalisierte Vertrauen besonders wichtig, da spezifisches Vertrauen schwer aufzubauen ist. Zum anderen geht es vor allem um Vertrauen in ein abstraktes System und weit weniger um Vertrauen in individuelle Akteure. Gerade dieses diffuse Vertrauen im Cloud Computing ist eine Art Kollektivgut, zu dem die Einzelnen beitragen müssen. Dabei geht es nicht so sehr um „Anbieter gegen Nachfrager“ als um eine Koalition der Verantwortungsvollen gegen Betrüger und Trittbrettfahrer.

Beim Cloud Computing sind natürlich viele Varianten vorstellbar, aber lassen Sie uns intertypisch von einem relativ offenen System ausgehen. Die Teilnehmer begeben sich also in die besagte Wolke mit vielen anderen Teilnehmern. Soweit man im Cloud Computing nicht

genau wissen kann, welche Akteure an dem System beteiligt sind und welche individuellen Anreize ihr Handeln bestimmen, so kann man Vertrauen nicht kalkulierend und fallweise produzieren, sondern braucht eine vertrauensvolle Grundeinstellung, die auch als generalisiertes Vertrauen bezeichnet wird. Damit ist die Annahme gemeint, dass andere Akteure im Allgemeinen vertrauenswürdig sind und man sich im Zweifel eher für als gegen Kooperation entscheidet.

Das Konzept des generalisierten Vertrauens wird bereits seit den späten 1940er Jahren in der empirischen Forschung eingesetzt und zwar inzwischen weltweit. Man stellt in den entsprechenden Erhebungen zumeist folgende Frage: „Manche Menschen sagen, dass man den meisten Menschen trauen kann. Andere meinen, dass man nicht vorsichtig genug sein kann im Umgang mit anderen Menschen. Was ist Ihre Meinung dazu?“ Fragen Sie sich bitte einmal, welche Antwort Sie geben würden: Man kann den meisten Menschen vertrauen? Oder: Man kann nicht vorsichtig genug sein? – In Deutschland antworten übrigens gut 30%, dass man vertrauen kann, und etwa 60% sind lieber vorsichtig. Damit liegt Deutschland im Mittelfeld, gehört aber schon zu den Ländern mit eher hohem generalisiertem Vertrauen.

Im Cloud Computing würde generalisiertes Vertrauen also bedeuten, dass die Teilnehmer meinen, dass man den meisten anderen Teilnehmern in diesem System vertrauen kann. Ein solches generalisiertes Vertrauen ist vor allem moralisch fundiert und wird durch gute Erfahrungen bestätigt. Diese Art des Vertrauens gründet sich wohlgerne nicht darin, dass man die anderen Teilnehmer durchschauen und kontrollieren kann. Natürlich ist es auch nicht schädlich, wenn man zu einigen Teilnehmern bereits eine engere Beziehung hat, die gut funktioniert. Dies darf jedoch nicht verhindern, dass man auch eher unbekannte Teilnehmer in das System hineinlässt, die sich dann natürlich als vertrauenswürdig erweisen müssen, denen man jedoch einen Vertrauensvorschuss gewährt.

Jeder Teilnehmer sichert durch sein vertrauenswürdiges Verhalten nicht nur seinen eigenen Zugang zu dem System, sondern reproduziert und stärkt auch das generalisierte Vertrauen der anderen. Und damit der Vertrauensmissbrauch einzelner Teilnehmer nicht das generalisierte Vertrauen zerstört, müssen Vertrauensbrecher auch konsequent aus dem System wieder ausgeschlossen werden oder – falls das nicht so ohne weiteres möglich ist – unter besondere Beobachtung gestellt werden, bis sie die Erwartungen wieder erfüllen. Generalisiertes Vertrauen fällt also nicht vom Himmel, sondern muss gepflegt werden.

Entwicklungspsychologisch gesprochen steht das generalisierte Vertrauen dem sogenannten Urvertrauen nahe, das sich im Kleinkindalter entwickelt. Diese „Früherziehung zum Vertrauen“ ist aus der Sicht des Cloud Computing recht weit weg. Aber sie ist doch in sofern noch

übertragbar, dass gerade in der frühen Phase in der Etablierung eines System – und gerade in Bezug auf Neueinsteiger in das System – besonders in Vertrauen investiert werden muss. Das bedeutet: in die Etablierung eines Musters, wonach Freiräume selbstverständlich gewährt, aber ebenso selbstverständlich auch nicht missbraucht werden. Verstöße müssen in dieser Phase unbedingt geahndet werden, aber nicht direkt zum Ausschluss führen. Gerade das Zugestehen einer zweiten Chance kann nämlich Vertrauen fördern.

Ich frage mich – und ich frage Sie, ob es vorstellbar ist, die Cloud Computing Systeme grundsätzlich „kooperationsfreundlich“ zu programmieren. Dazu würde dann eben auch eine gewisse Fehlertoleranz gehören sowie eine Kultur des konstruktiven Problemlösens. In der Vertrauensforschung hat sich immer wieder gezeigt, dass Vertrauen durch gemeinsames Problemlösen gestärkt wird. Und es wird mithin nicht schon dadurch zerstört, dass ein Problem auftritt, sondern erst dadurch, dass die betreffenden Akteure das Problem nicht lösen, sondern sich als inkompetent erweisen oder sich gar ihrer Verantwortung entziehen. Anbieter von Cloud Computing Diensten sollten also besonderen Wert auf ihren User Support und Kundenservice legen. Und die Kunden sollten nicht gleich beim ersten Problem den Anbieter wechseln, sondern ihrerseits konstruktiv zur Problemlösung beitragen. Wenn diese Grundeinstellung weit verbreitet ist, dann steht es um das generalisierte Vertrauen bereits gar nicht schlecht. Wohlgermerkt geht es ja nicht nur darum, dass man selbst Wechsel- oder Neuanwerbungskosten sparen kann, sondern dass man mit seinem kooperativen Verhalten auch die Vertrauenskultur in dem System pflegt.

### **Vertrauen in abstrakte Systeme**

Das System der Internet Cloud ist zudem ein abstraktes System, in dem einzelne Akteure zumeist nur einen kleinen Teil der Leistung beitragen und verantworten können. Das System als Ganzes darf man sich wiederum nicht als einen Akteur vorstellen, der sich schlüssig und konsistent entscheidet, das in ihn gesetzte Vertrauen zu honorieren oder zu brechen. Die Vertrauensforschung weist vielmehr darauf hin, dass Vertrauen in ein abstraktes System dadurch aufgebaut und gepflegt wird, dass die Repräsentanten an den Zugangspunkten und die das System kontrollierenden Experten vertrauenswürdig sind. Das Vertrauensobjekt bleibt nach wie vor das System, doch die Vertrauenswürdigkeit des Systems macht der Vertrauensgeber am Verhalten bestimmter Akteure fest.

Ich beziehe mich hierbei insbesondere auf Überlegungen von Anthony Giddens und Niklas Luhmann. Giddens betont die Bedeutung von sogenannten Zugangspunkten zu abstrakten Systemen. Und diese Zugangspunkte sind eben oft Personen. Beim Gesundheitssystem ist es etwa das medizinische Personal, beim Luftverkehrssystem sind es unter anderem die

Flugbegleiter und bei unserem Regierungssystem sind es die Bundeskanzlerin und die Minister. In allen Fällen beobachtet der Vertrauensgeber diese Repräsentanten, um zu sehen, ob das abstrakte System noch vertrauenswürdig ist. Entsprechend legen diese Repräsentanten besonderen Wert auf ihr Auftreten. Bleiben wir bei Giddens, der das Beispiel der Stewardessen anführt: Durch ihr freundliches Lächeln, ihre Kleidung, die Selbstverständlichkeit, mit der sie den Flug vorbereiten, signalisieren sie uns – ganz bewusst – dass alles in Ordnung ist mit dem Flugzeug und dem ganzen Drumherum. Stellen sie sich einmal vor, dass Sie eine schlecht gekleidete, unfreundliche und unsichere Person im Flugzeug begrüßt und etwas über die widrige Witterung und die komischen Geräusche am Fahrwerk murmelt. Wir durchschauen das System nicht, aber an diesem Zugangspunkt wollen wir die Bestätigung, dass alles gut geht, und keine Erinnerung an die verbleibende Ungewissheit und Verwundbarkeit.

Bei Luhmann, der ansonsten in vielen Punkten Vertrauen anders versteht als Giddens, finden sich einige Überlegungen zum Systemvertrauen, die den vorigen Gedanken unterstützen und erweitern. Luhmann verweist darauf, dass Vertrauen in ein System vor allem durch Vertrauen in die in das System eingebauten Kontrollen gestützt wird. Das ist interessant, weil hier Vertrauen durch Kontrolle produziert wird, aber man achte auf die Feinheiten. Der Vertrauende ist keineswegs in der Lage, das System selbst zu kontrollieren. Er muss ihm nach wie vor vertrauen. Er weiß jedoch, dass in das System Kontrollen eingebaut wurden. Nun kann sich sein Vertrauen darauf konzentrieren, dass diese Kontrollen funktionieren. Ich würde sagen, dass dies auf einen besonderen Typus eines Zugangspunktes zum System verweist, nämlich auf die Kontrolleure. Man vertraut dem System, weil man den Kontrolleuren des Systems vertraut, die aber doch selbst Teil des Systems sind.

Zusammenfassend finde ich hier zwei Aspekte für die weiteren Diskussionen besonders wichtig. Erstens: Beim Vertrauen in abstrakte Systeme handelt es sich nicht um ein indirektes Vertrauen vermittelt durch spezifische Personen. Ich muss die Ärztin, die Stewardess oder die Lebensmittelkontrolleurin nicht persönlich kennen, aber ihr persönliches Verhalten gibt mir wichtige Signale über das System. Es geht also, wie auch beim generalisierten Vertrauen, nicht nur um konkrete Beziehungen, sondern um das Vertrauen darüber hinaus.

Zweitens: Eingebaute Kontrollen können vertrauensförderlich sein und sie sind zweifelsohne auch im Cloud Computing nötig. Jedoch wird man Opportunismus und Fehler wohl niemals völlig ausschließen können. Und die Betonung der Vertrauenswürdigkeit der Kontrolleure bedeutet ja vor allem eine teilweise Verschiebung der Vertrauensproblematik vom System zu den Kontrolleuren. Und wer kontrolliert bitte die Kontrolleure?

**Fazit: Verantwortung zeigen**

So wird es auch im Cloud Computing über alle Bemühungen um fehlerfreie Technologien, lückenlose Rechtsapparate, konsequente Aufsichtsinstanzen und vorsorgliche Versicherungen hinaus immer nötig sein, dass die Beteiligten signalisieren, dass sie Verantwortung für das System tragen wollen – auch über ihre individuellen Verpflichtungen hinaus. Geschieht dies, werden sich viele weitere Akteure in die Wolke hineinwagen. Ich habe in meinem Vortrag herausgestellt, dass es in der Internet Cloud vor allem auf generalisiertes Vertrauen und Vertrauen in abstrakte Systeme ankommt. Wo technische Sicherungsmechanismen an Grenzen stoßen, müssen die verbleibenden Lücken durch soziale Mechanismen geschlossen werden. Daher gilt es, Gelegenheiten zu schaffen und zu nutzen, bei denen die das System tragenden Akteure in Erscheinung treten, ihre Verantwortungsbereitschaft beweisen und auch gegen die vorgehen, die verantwortungslos handeln – egal, ob diese auf der Seite der Anbieter, der Nachfrager oder der Behörden stehen. Es geht nicht um absolute Sicherheit, sondern um den guten Willen. Der allein reicht wiederum auch nicht aus – das wäre ja weltfremd – aber er muss stets erkennbar sein, wenn Cloud Computing mit Vertrauen effizienter oder überhaupt erst in der Breite möglich werden soll.

**Der Autor**

Dr. Guido Möllering ist Wissenschaftlicher Mitarbeiter am Max-Planck-Institut für Gesellschaftsforschung in Köln. Er wurde 2003 an der Universität Cambridge promoviert und forscht über Vertrauen, Unternehmenskooperation und Marktconstitution. Weitere Informationen: [www.mpifg.de/people/gm](http://www.mpifg.de/people/gm).

**Literaturhinweise**

Bachmann, Reinhard / Zaheer, Akbar (Hrsg.), 2006: Handbook of Trust Research. Cheltenham: Edward Elgar.

Giddens, Anthony, 1999. Konsequenzen der Moderne. 3. Aufl., Frankfurt/M.: Suhrkamp.

Latusek, Dominika / Gerbasi, Alexandra, 2010: Trust and Technology in a Ubiquitous Modern Environment. Hershey, PA: Information Science Publishers.

Luhmann, Niklas, 2000: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität. 4. Aufl., Stuttgart: UTB.

Möllering, Guido, 2006: Trust: Reason, Routine, Reflexivity. Oxford: Elsevier.

Zak, Paul, 2009. Die Neurobiologie des Vertrauens. In: Spektrum der Wissenschaft, Heft 04/09 (April), S. 40-46.