Trust by design?

Vertrauen als zentrale Ressource für die Cloud

Michael Eggert und Daniel Kerpen

Beitrag zur Ad-hoc-Gruppe »Soziologische Perspektiven auf die Cloud« – organisiert von Michael Eggert und Daniel Kerpen

Von der Notwendigkeit einer Soziotechnik des Cloud-Computings

Cloud-Computing und darauf basierende Technologien stellen zweifellos eine der einschneidendsten Veränderungen in der jüngeren Geschichte der Informationstechnik (IT) dar. Dabei beschreibt der Begriff *Cloud-Computing* keine konkrete Technologie, sondern in einem sehr allgemeinen Sinn Modelle, in denen IT-Infrastrukturen, Plattformen und Dienste von den Nutzern nicht mehr selbst vorgehalten werden. Stattdessen werden diese als Dienstleistungen bezogen, die dynamisch, skalierbar und – räumlich wie organisatorisch – nicht mehr eindeutig zuordenbar sind.

Zur Alltagsubiquität des Cloud-Computings

Cloud-Technologien bieten Nutzungsmöglichkeiten, die über die Verlagerung und ubiquitäre Verfügbarmachung von Rechen- und Speicherkapazität im Rahmen typischer IT-Anwendungen hinausgehen: So wird bereits ein Großteil unserer täglichen Kommunikation über die Cloud abgewickelt. Weiter stellt die Nutzung cloud-basierter IT die notwendige Grundlage dar, die für die Entwicklung zu einem Internet der Dinge notwendigen Ressourcen effizient nutzen zu können (Atzori et al. 2010; Eggert et al. 2014a). Ebenso können realistischerweise nur über Cloud-Nutzung die für die vielfältigen Nutzungsmöglichkeiten des mobilen Internets erforderlichen Technologien bereitgestellt und die für Big-Data-Anwendungen benötigten Datenmengen erhoben, verwaltet und verarbeitet werden (Giese et al. 2011; Liu et al. 2011). Auch die unter dem Schlagwort Industrie 4.0 diskutierten Transformationen der industriellen Produktion gründen zu

weiten Teilen auf dem Einsatz von Cloud-Technologien (Hirsch-Kreinsen 2014; Ortmann, in diesem Band; Nof (Hg.) 2009).

Offensichtlich birgt dieses *Cloud-Paradigma* das Potential, (nicht nur) individuelle Arbeits- und Lebenswelten entscheidend zu verändern – man denke nur an mit Sensorik und Aktorik gespickte Wohn- und Arbeitsräume –, genauso wie sie neue Geschäftsfelder eröffnet, neue Beziehungen zwischen Personen und Unternehmen impliziert und neue Formen der Kooperation bedingt. Die Relevanz des Cloud-Computing für die Soziologie scheint also auf der Hand zu liegen.[1] Auf der anderen Seite ist die Cloud nicht nur ein Phänomen, das eine Vielzahl soziologisch motivierter Fragestellungen aufwirft, sondern soziologisches Wissen ist auch relevant für die (Weiter-)Entwicklung und Verbreitung von Cloud-Technologien und dahinter stehenden Ideen. Als Netzwerktechnologie im besten Sinne verknüpft Cloud-Computing nicht nur unterschiedliche technische Artefakte miteinander, sondern verbindet auch individuelle und kollektive soziale Akteure untereinander sowie mit der Technik und über diese. Cloud-Computing in seinen unterschiedlichen Ausprägungen ist offensichtlich von der Entwicklung bis zur Anwendung ganz elementar abhängig von den die Technologie umgebenden und begleitenden sozialen Prozessen – und damit von Problemstellungen, die sich nicht aus einer exklusiv technologischen Perspektive verstehen, geschweige denn lösen lassen.

Umso erstaunlicher scheint es uns, dass das Phänomen Cloud-Computing in seiner Breite bislang kaum Eingang in die soziologische Forschung gefunden hat. Ein Blick auf das Technologieprogramm *Trusted Cloud*[2] des Bundesministeriums für Wirtschaft und Energie (BMWi) offenbart die sehr technikgetriebene, anwendungsorientierte Herangehensweise zentraler Projekte in diesem Bereich: Gemeinsam ist ihnen die deutliche Betonung technischer Mechanismen zur Entwicklung und Gewährleistung von (Informations-)Sicherheit (mit Blick auf Integrität/Verfügbarkeit/Vertraulichkeit bzw. security/safety/privacy von Daten) sowie, damit zusammenhängend, der Einführung von Bewertungsmöglichkeiten solcher Cloud-Angebote aus ökonomischer oder rechtlicher Perspektive (BMWi 2014).

Eine solche Herangehensweise hat ihre Berechtigung – zumindest, so lange es um die Lösung grundlegender technischer Probleme geht –; sie bleibt aber ergänzungsbedürftig durch eine dezidiert soziologische Herangehensweise (Möllering 2011; Eggert et al. 2014b). Anknüpfend und explizit auf Cloud-Computing fokussierend stehen für unsere Auseinandersetzung insbesondere folgende Aspekte im Mittelpunkt: einerseits die Frage nach der Akzeptanz und Nutzbarkeit von Cloud-Anwendungen auf Seiten der Anwenderinnen und Anwender (zum Beispiel als hochskalierbare Plattform global vernetzter Sensoren und Aktoren sowie als cloudbasierte altersgerechte Assistenzsysteme[3]). Damit ist nicht nur das Anliegen formuliert, Mecha-

1 Die Ad-Hoc-Gruppe Soziologische Perspektiven auf die Cloud wurde für den Kongress mit dem Ziel beantragt, in ihr unterschiedliche soziologische Perspektiven auf das Cloud-Computing und/oder mit ihm verknüpfte Phänomene zusammenzubringen, um damit der Frage nach der Relevanz der Cloud für die Soziologie oder umgekehrt derjenigen der Soziologie für ein Verständnis der Cloud nachzugehen (vgl. auch Dukat, Caton; Reischauer; Petersen, Kollek, alle in diesem Band).

2 Das Technologieprogramm Trusted Cloud wurde vom BMWi im Herbst 2010 ins Leben gerufen und ist Kernbestandteil des Aktionsprogramms Cloud Computing sowie Element der IKT- und Hightech-Strategien der deutschen Bundesregierung. Eine Übersicht der bis Anfang 2015 laufenden Projekte bietet BMWi (Hrsg.) 2014.

3 Beispielsweise im Rahmen des BMWi-Projekts SensorCloud (http://www.sensorcloud.de/) sowie des RWTH-Exzellenzmittelprojekts IPACS: Intelligent privacy-aware cloud-based services (http://www.humtec.rwth-aachen.de/index.php?article_id=1034&clang=0).

nismen einer sich herausbildenden Mensch-Cloud-Interaktion zu beschreiben, sondern im Kontext konkreter FuE-Projekte auch die Aufgabe gestellt, technische, kulturelle, strukturelle und organisatorische Hemmnisse für den Einsatz von Cloud-Technologien frühzeitig in den Innovationsprozess zurückzuspiegeln, um eine partizipative nutzerorientierte Technikgestaltung zu gewährleisten (Eggert et al. 2014a; Henze et al. 2014). Andererseits besteht das Erkenntnisinteresse darin, den Innovationsprozess selbst kritisch zu begleiten und zu analysieren, um dadurch zu einem empirisch begründeten Verständnis des Cloud-Computing-Innovationsprozesses zu gelangen und künftige Entwicklungstrends auf diesem Gebiet abschätzen zu können (Eggert et al. 2014b).

Nach diesem kurzen Aufriss zur soziotechnischen Basis des Cloud-Computing werden wir aufzeigen, warum sich Cloud-Computing als soziale Technologie im besten Sinne darstellt und inwiefern Vertrauen aus unserer Perspektive als Schlüsselressource für das Funktionieren des Prinzips Cloud-Computing fungiert. Daraus leiten wir die Forderung nach *trust by design* als Gestaltungprinzip für Cloud-Technologien und Anwendungen ab und präsentieren abschließend ein Implementationsbeispiel dieses Prinzips.

Steigerung von technischer und sozialer Komplexität

Nimmt man somit – wenn man von Cloud-Computing spricht – nicht nur einzelne technische Artefakte und Dienstleistungen in den Blick, sondern versucht, sich die Cloud als Gesamtes zu vergegenwärtigen, so wird deutlich, dass sich die Nutzung cloud-basierter IT in zentralen Aspekten elementar von bisherigen Paradigmen der IT-Anwendung unterscheidet. Rechenleistung, Speicherplatz und technologische Plattformen werden nicht mehr von Verwenderinnen und Verwendern vorgehalten, sondern im Rahmen dynamischer Technik- und Angebotsstrukturen als Dienstleistung bezogen. Anstatt eigene IT-Infrastruktur aufzubauen und zu betreiben, greifen die Anwenderinnen und Anwender also auf Technik und Expertise spezialisierter Anbieter zurück. Cloud-Nutzung beinhaltet damit immer auch eine soziale Komponente: Wer die Cloud nutzt, delegiert einen beträchtlichen Teil ihres oder seines Umgangs mit eigenen Daten an Dritte, also andere soziale Akteure, nämlich den Anbieter der Cloud-Dienstleistung, und ist gleichzeitig auf die Leistungen weiterer Akteure angewiesen, wie etwa diejenigen Unternehmen, die die Infrastrukturen für den Datentransport bereitstellen. Wie diese Akteure allerdings die Ihnen zugeschriebenen Aufgaben erfüllen – beispielsweise durch einen Rückgriff auf unterstützende Dienstleistungen weiterer Unternehmen oder Ähnliches –, bleibt für die Anwender/-innen zumeist intransparent.

Einwenden ließe sich, dass die Fragen und Probleme, die sich daraus ergeben, keineswegs so neuartig sind, wie sie auf den ersten Blick erscheinen: schließlich ist IT-Outsourcing – zumindest in industriellen Kontexten – schon spätestens seit den 1970er Jahren eine gängige Praxis.

Mit zunehmender Nutzung von Cloud-Dienstleistungen gewinnen diese Fragen allerdings qualitativ wie auch quantitativ eine neue Dimension: In *quantitativer* Hinsicht, weil sich die potentielle Nutzendenschicht von IT-Dienstleistungen durch den Einsatz von Cloud-Technologien drastisch verbreitert. Während klassisches IT-Outsourcing eigentlich nur für große Organisationen eine Option darstellte, richtet sich eine Vielzahl der Cloud-Angebote auch an kleinere Orga-

nisationen und Privatanwender/-innen. In *qualitativer* Hinsicht führt die vermehrte Verbreitung von Cloud-Anwendungen und deren technische Weiterentwicklung dazu, dass IT-Services zunehmend ad-hoc zur Verfügung gestellt, unter verschiedenen Nutzer/-innen geteilt und im Endeffekt gar über technische Grenzen von Organisationen (beispielsweise über verschiedene Rechenzentren und Anbieter) hinaus skaliert und verteilt werden können. Die Anzahl der beteiligten Akteure und technischen Elemente wird also beträchtlich gesteigert, wodurch die Komplexität des gesamten Systems der Datenverarbeitung merklich zunimmt, und es für die einzelnen Anwenderinnen und Anwender zunehmend unüberschaubar wird, durch wen, wo und in welcher Form ihre Daten gespeichert und verarbeitet werden.

Ein Verständnis *der Cloud,* das einer allein technischen Perspektive verpflichtet ist, muss somit zwangsläufig lückenhaft bleiben. Mit der Vielzahl technischer und sozialer Elemente, die beim Einsatz relevant sind, präsentiert sich das Prinzip Cloud-Computing als sozio-technisches Netzwerk *par excellence.* Sein Funktionieren bestimmt sich nicht alleine über das gelingende Zusammenspiel seiner technischen Elemente. Als eher abstraktes Konzept eines komplexen Netzwerks aus technischen Elementen, sozialen Akteuren und organisatorischen Kontexten ist für ein Funktionieren des Prinzips Cloud-Computing die Integration und Kooperation dieser einzelnen Teile eine *conditio sine qua non.* Vor einer möglichen Realisierung der technischen, ökonomischen und ökologischen Vorteile, die Cloud-Computing verspricht, steht also immer das *soziale Funktionieren* des Prinzips vor dem Hintergrund der jeweils konkreten Anwendungssituation. Diese gegenseitige Angewiesenheit von technischen und sozialen Elementen macht Cloud-Computing zu einer sozialen Technologie im besten Sinne, bei der parallel zur Steigerung der technischen auch die soziale Komplexität der Technikverwendung zunimmt.

Den Vorteilen auf Seiten der Anwender/-innen im Sinne reduzierter – oder im Extremfall vollständig vermiedener – Investitions- und Betriebskosten stehen damit aber auch Herausforderungen gegenüber, die sich aus der Steigerung sozio-technischer Komplexität ergeben. Für Cloud-Computing heißt das konkret, dass die Anwendenden die faktische Kontrolle über die Infrastruktur der Datenübertragung, -verarbeitung und -speicherung aus den Händen geben. Stattdessen liegt dieser relevante Anteil des Umgangs mit den Daten der Anwender/-innen bei Dritten, die den Anwendenden bestenfalls nicht näher bekannt sind und die sie daher nicht einschätzen können – sofern sie überhaupt davon Kenntnis haben, dass solche Dritte involviert sind.[4] Die Kehrseite der Cloud-Vorteile besteht auf Nutzer/-innenseite also darin, dass Handlungen im IT-Kontext einem höheren Maß an Unsicherheit unterliegen – bestehende Risiken werden verstärkt, neue Unsicherheiten werden geschaffen.

4 Cloud-Angebote lassen sich einer von drei Klassen von Dienstleistungen zuordnen: (1) *Software as a Service (SaaS),* (2) *Platform as a Service* oder (3) *Infrastructure as a Service (IaaS).* Durch diese auf unterschiedlichen Ebenen angesiedelten Dienste kann es zu der – nicht ungewöhnlichen – Situation kommen, dass der/die Anbieter/-in einer Cloud-Dienstleistung für Endanwender/-innen seinerseits wiederum auf andere Cloud-Dienste zurückgreift, um die Nutzer/-innendaten abzulegen und zu verarbeiten. So wissen Nutzende des Dienstes *Dropbox* in der Regel, dass sie eine Cloud-Anwendung nutzen. Dass *Dropbox* zur Realisierung des Dienstes seinerseits auf Infrastrukturangebote von *Amazon* zurückgreift und ihre Daten damit in einem Rechenzentrum des letztgenannten Unternehmens liegen, dürfte den Anwendenden andererseits nur in den seltensten Fällen bekannt sein.

Zum Umgang mit Unsicherheit und Komplexität

Der Umgang mit Komplexität und daraus resultierenden Risiken und Unsicherheiten ist im Sozialen alltäglich und ein umfassend bearbeitetes Feld soziologischer Forschung (Endreß 2002). Eine zentrale Fragestellung der soziologischen Auseinandersetzung besteht darin, wie diese soziale – bzw. in unserem Kontext sozio-technische – Komplexität reduziert werden kann, um Handlungen und Sachverhalte erwartbarer und handhabbarer zu machen und damit Kooperation unter den Bedingungen von Risiko und Unsicherheit zu ermöglichen beziehungsweise zu erreichen, dass diese weniger unwahrscheinlich wird (Luhmann 1989). Für den Bereich des Cloud-Computing ist die Frage nach der Kooperation von besonderer Relevanz, da jede Anwendung von Cloud-Technologien immer auch auf die Leistungen anderer Akteure zurückgreift und damit auf deren Kooperation angewiesen ist. Handlung und Kooperation fallen beim Cloud-Computing ineinander. Insbesondere zwei Phänomene lassen sich dabei als wirksame Mechanismen identifizieren, um diesem Ziel näher zu kommen: *Kontrolle* einerseits und *Vertrauen* andererseits.

Kontrolle und Vertrauen

Kontrolle als erste der beiden Möglichkeiten, das Handeln des Gegenübers erwartbarer zu machen, bedeutet, Handlungs- oder Kooperationshemmnisse mit Hilfe von Wissen zu beseitigen oder zumindest zu minimieren. Dazu ist allerdings erforderlich, dass die Konsequenzen sämtlicher Aktivitäten vollständig transparent sind. Eine Situation zu kontrollieren bedeutet also, aufgrund vollständiger Informationen um die Konsequenzen möglicher Handlungen oder Verfahren zu wissen und über geeignete Mittel zu verfügen, den Verlauf nach jeweils eigenen Vorstellungen zu gestalten und die weiteren Beteiligten zur Kooperation zu bewegen. Kooperation unter den Bedingungen von Kontrolle erweist sich damit als höchst voraussetzungsreiche Option, deren Anforderungen an vollständige Information und die gegenseitige Transparenz der Handlungskalküle der Beteiligten – wenn überhaupt – nur in sehr begrenztem Rahmen erfüllt werden können.

Bezogen auf die Kontrolle im Umgang mit Technik zeigt sich ein ähnliches Problem: Bei simplen technischen Artefakten, wie es etwa Werkzeuge oder einfache Maschinen sind, können die Folgen einer Handlung abgesehen und mithin kontrolliert werden. Wer einen Hammer benutzt, *weiß,* was passiert, wenn er mit diesem auf einen Nagel einschlägt. Auch das in feste Strukturen gegossene technische Funktionsprinzip eines Verbrennungsmotors kann *kontrolliert* werden. Beim Cloud-Computing ist aber eine solche vollständige Kontrolle nicht mehr möglich. Die Technologie weist hier ein Komplexitätsniveau auf, das es den Anwender/-innen nahezu unmöglich macht, ihr Funktionieren zu durchschauen. Ebenso komplex wie die Technik ist auch das dahinter stehende sozio-technische Netzwerk, das bei der Nutzung von Cloud-Anwendungen aktiv ist. Spätestens mit dem Zusammenfallen dieser beiden Aspekte entsteht bei der Nutzung von Cloud-Computing somit eine Kontrolllücke, die den Einsatz von Cloud-Technologien als hochriskantes Unterfangen erscheinen lässt.

Um diese Lücke zu schließen und damit erfolgreiche Kooperationsbeziehungen zu initiieren und aufrechtzuerhalten, bedarf es des zweiten Mechanismus: *Vertrauen.* Als »mittlerer Zustand zwischen Wissen und Nichtwissen« (Simmel 1992: 393) ermöglicht es die Initiierung einer Kooperation durch eine Vorleistung eines der Beteiligten – im Falle des Cloud-Computing der Anwenderin oder des Anwenders. Hätten diese vollständigen Informationen über das Handlungsrepertoire der anderen Beteiligten, so wäre kein Vertrauen nötig und sie könnten kontrollieren, was mit ihren Daten geschieht. Nicht möglich wäre Vertrauen andererseits, wenn die/der Vertrauensgeber/-in keinerlei Einblick in die Motive und Handlungskalküle der potentiellen Vertrauensnehmer/-innen hätte. Information und Unsicherheit sind also gemeinsam konstitutiv für Vertrauen.

Kontrolle und Vertrauen ergänzen sich folglich bei der Herstellung von Erwartbarkeit, und je weniger es möglich ist, Kontrolle auszuüben (zum Beispiel wegen zunehmender Undurchschaubarkeit), desto größere Anforderungen werden an das komplementäre Vertrauen gestellt. Die Unmöglichkeit einer vollständigen Information über die Konsequenzen der Cloud-Nutzung führt zwangsläufig dazu, dass die Rationalität von Entscheidungen grundsätzlich gewissen Beschränkungen unterliegt (Simon 1972) und somit immer ein bestimmtes Maß an Vertrauen notwendig ist, um eine Kooperation einzugehen. Der Einsatz von Cloud-Computing ist folglich immer auf ein gewisses Maß an Vertrauen angewiesen. Vertrauen stellt also eine zentrale Ressource für das Funktionieren der Cloud dar. Ausmaß und konkrete Ausprägung dieser Ressource, die nötig sind, um eine dauerhafte und ertragreiche Kooperationsbeziehung in Gang zu bringen, bestimmen sich dabei über die konkreten Charakteristika des sozio-technischen Netzwerks der jeweiligen Anwendung.

Vertrauen als Basis für erfolgreiche Kooperationen ist allerdings immer mit Unsicherheit bzw. mit Risiko in der Form behaftet, dass die Vertrauensgebenden – in unserem Fall die Anwender/-innen – von der/dem Vertrauensnehmer/-in *hintergangen* wird, sich diese/-r also nicht an die impliziten oder auch expliziten Vereinbarungen hält. Die Vertrauensgebenden treten also in eine »riskante Vorleistung« (Luhmann 1989: 23), indem sie ihre eigene Verwundbarkeit steigern. Allerdings ist dies erst »das Instrument, mit dem eine dauerhafte und wechselseitig ertragreiche Kooperationsbeziehung in Gang zu bringen versucht wird (Preisendörfer 1995: 264). Je höher dieses Risiko – und damit der Grad des erforderlichen Vertrauens – ist, desto geringer ist die Chance, dass sich die Akteure auf das riskante Vorgehen einlassen. Ein Mangel an Vertrauen – in die Technik, in die Anbieter etc. – geht dabei mit einem Überschuss an Misstrauen einher, der sich beim Cloud-Computing aus zwei Quellen speist: einerseits einer »Skepsis gegenüber der [.] Unbedenklichkeit der technischen Sachen und zum anderen [.] Zweifel an der Glaubwürdigkeit der technischen Experten« (Ropohl 2010: 117), wobei diese beiden Dimensionen sich auch gegenseitig aufeinander beziehen können.

Beide Ebenen adressieren zwei grundlegende Dimensionen von Vertrauen, die in der soziologischen Vertrauensforschung häufig unterschieden werden: Auf der einen Seite steht das *habituelle* Vertrauen, das sich auf Vertrautheit, Gewohnheit, Intuition und selbstverständliche Gewissheit stützt und in seiner Unmittelbarkeit den dominierenden Vertrauenstypus vormoderner Gesellschaften darstellt. Im Zuge der Modernisierung und den damit einhergehenden Prozessen der Rationalisierung und (funktionalen) Differenzierung gewinnt das *reflexive* Vertrauen zunehmend an Bedeutung, das insbesondere auf Annahmen der Vertrauensgebenden über die Motive und Handlungsrationalitäten der Vertrauensempfangenden basiert.

Zwar steht das habituelle Vertrauen primär für interpersonelles Vertrauen, mit seiner grundlegenden Unterscheidung zwischen Vertrautheit und Fremdheit (Strasser, Voswinkel 1997: 220) kann es jedoch auch auf eine Betrachtung der Beziehung zur technischen Seite der Cloud angewendet werden. Wie jede Innovation provozieren auch Cloud-Technologien Irritationen bestehender Alltagsroutinen; es mangelt ihnen an Integration in die alltägliche Lebenswelt, die potentiellen Anwender/-innen sind noch nicht mit diesen vertraut. Darüber hinaus sind sie aufgrund ihrer Komplexität in ihrer Funktionsweise für Laien nahezu undurchschaubar (Ropohl 2010: 124). Der Vertrauensmangel, der sich daraus für die technische Basis der Cloud ergibt, ist ein Problem des Umgangswissens *(tacit knowledge),* das nur durch einen alltäglichen Umgang mit Cloud-Technologien bearbeitet werden kann (Irrgang 2010: 341) und daher an dieser Stelle nicht weiter verfolgt wird.

Zentraler für das Funktionieren des Cloud-Computing ist allerdings das Vorhandensein generalisierten Vertrauens in das sozio-technische Gebilde, das die Cloud trägt. Hierbei handelt es sich um die reflexive Spielart von Vertrauen, welche dieses als Ressource ausmacht. Mit dem Einsatz dieser Ressource gehen die Akteure eine Wette auf das kontingente Verhalten der anderen Involvierten ein, die eine gewisse Chance auf Erfolg aufweisen muss, damit die Akteure bereit sind, Vertrauen in die Technik bzw. das Geflecht aus technischen Artefakten und sozialen Akteuren zu investieren.

Mechanismen der Vertrauensgenerierung

Somit stellt sich die Frage, wie die Erfolgschancen dieser Wette so weit gesteigert werden können, damit die Akteure – im Falle der Cloud die Anwender/-innen – sich auf diese einlassen. Wie also entweder der Umfang der notwendigen Vertrauensinvestition verringert oder wie die Investition gegen einen Verlust *abgesichert* werden kann. Neben der Möglichkeit einer rechtlichen Verregelung der Beziehung zwischen den Akteuren, also der Substitution der direkten Vertrauensbeziehung durch ein Verhältnis, das durch staatliche Macht vermittelt wird, bieten sich aus der Perspektive der Vertrauensforschung insbesondere zwei Strategien an, wie das für das Funktionieren der Cloud notwendige Vertrauen generiert werden kann.

Risikostreuung

Eine erste Möglichkeit besteht darin, das Risiko zu streuen (Preisendörfer 1995: 265). Das Risiko für den einzelnen Akteur wird dadurch verringert, dass andere das gleiche Risiko tragen oder einen Teil des Risikos übernehmen. Nachahmung etwa ermöglicht eine solche Risikoübertragung, indem Erfahrungen früherer Anwender/-innen in die Risikokalkulation einbezogen werden. Die Reputation eines Anbieters oder einer Technologie, die auf diese Art und Weise generiert wird, macht für neue Anwender/-innen das Risiko weniger unberechenbar, ob ihre Investition von Vertrauen und anderen Ressourcen möglicherweise ein Verlustgeschäft wäre.

Ein weiterer Mechanismus der Risikostreuung ist die Übertragung von Vertrauen an Vertrauensagenturen und damit die Verlagerung der Vertrauensproblematik auf eine andere Ebene.

Diese »Vertrauensagenturen« bzw. »Vertrauensintermediäre« (Strasser, Voswinkel 1997: 224ff.) ermöglichen eine Form generalisierten Vertrauens, indem sie dem Umstand Rechnung tragen, dass Vertrauen auch immer einen Rückgriff auf Misstrauen enthalten muss, um nicht *blind* zu sein. Indem sie das dem Vertrauen komplementäre Misstrauen institutionalisieren, ermöglichen sie paradoxerweise die institutionelle Vermittlung von Vertrauen (Endreß 2002: 78f.). Beispiele für solche Agenturen sind etwa die *Stiftung Warentest*, der *TÜV, Verbraucherzentralen* oder auch *Zertifizierungsinstanzen.* Allerdings müssen diese Agenten nicht unbedingt in Form neutraler Dritter auftreten – auch Selbstverpflichtungen der Industrie können beispielsweise diese Rolle übernehmen.

Kalkulierbarkeit von Handlungsweisen

Während Risikominimierung durch Risikostreuung primär darauf abzielt, die Wahrscheinlichkeit zu verringern, dass das Vertrauen enttäuscht wird, kann auch versucht werden, das Ausmaß des zu investierenden Vertrauens zu verringern. Dies kann erreicht werden, indem das Verhalten der Vertrauensempfangenden in gewissem Maß kalkulierbar gemacht wird. Die Erzeugung bspw. von Verhaltensgleichförmigkeit schafft in dieser Hinsicht Wiedererkennbarkeit und damit Verlässlichkeit der Handlungsweisen der Vertrauensempfangenden. Hinzu kommt die Annahme, dass sich die Vertrauensempfangenden – insbesondere im Fall von Organisationen – rational an ihrem Eigeninteresse orientieren. Zusammen reduzieren diese Aspekte aus Sicht der Vertrauensgebenden die Kontingenz des Verhaltens der Vertrauensnehmenden und können somit die Bildung des notwendigen Vertrauens erleichtern (Strasser, Voswinkel 1997: 224).

Im Kontext der Cloud stellt sich hier allerdings auch die Frage, wer jeweilige Vertrauensnehmer/-innen sein könnten. Vertrauen ist immer ein Element einer Beziehung von zwei oder mehr Akteuren. Der Cloud als solcher zu vertrauen, dürfte also kaum möglich sein. Vielmehr sind es die an der Cloud beteiligten Akteure und Artefakte, die als potentielle Vertrauensnehmer/-innen fungieren. Eine herausragende Rolle kommt dabei denjenigen Instanzen zu, die als *Gatekeeper* die Schnittstelle der Cloud zu den Anwender/-innen darstellen – also Anbieter, die in direkter Beziehung zu den Anwenderinnen und Anwendern stehen sowie die Technologien, die an dieser Stelle eingesetzt werden und die Cloud den Nutzer/-innen gegenüber repräsentieren. Das Vertrauen, das Anwenderinnen und Anwender diesen Gatekeepern entgegenbringen, stellt also die entscheidende Dimension für den Einsatz von Cloud-Technologien dar.

Trust by Design – Cloud-Entwicklung als System-Building zur Vertrauensermöglichung

Dass diese Schnittstelle zwischen der Cloud und den Nutzer/-innen und das an dieser Stelle vorhandene Vertrauen die relevanten Größen für den erfolgreichen Einsatz von Cloud-Technologien sind, zeigen auch empirische Untersuchungen im Rahmen des Projekts *Sensor Cloud*. In leitfadenunterstützten Interviews sowie einer Zukunftswerkstatt mit Nutzer/-innen und

Entwickler/innen zur Frage der Akzeptanz cloud-basierter intelligenter Objekte zeichnete sich auf Nutzer/-innenseite ein offensichtlicher Vertrauensmangel gegenüber Cloud-Technologien ab. Dieser wird zwar auch auf die Undurchschaubarkeit der Cloud zurückgeführt, in erster Linie allerdings an der konkret vorliegenden Technik sowie einer mangelnden Vertrauenswürdigkeit der Anbieter festgemacht (Rüssmann, Eggert 2014).

Das Funktionieren der Cloud hängt also zu einem großen Anteil davon ab, dass nicht nur die technischen Artefakte die ihnen zugedachte Funktion zuverlässig erfüllen, sondern das gesamte Zusammenspiel der unterschiedlichen Elemente und Akteure von den Anwenderinnen und Anwendern als funktionierend eingeschätzt wird, was diese wiederum überwiegend an den Technologien und den Anbietern festmachen. Für die Entwickler/-innen und Anbieter/-innen von Dienstleistungen ergibt sich damit die Herausforderung, dass die Entwicklung von Technologien und Dienstleistungen für die Cloud nicht als rein technische Entwicklungsaufgabe verstanden werden kann, sondern auch immer die sozialen Bedingungen der Cloud-Nutzung reflektieren muss. Dazu ist es notwendig, dass die Entwicklerinnen und Entwickler eine Rolle als *system builder* einnehmen, deren zentrale Aufgabe auch darin besteht, Vertrauen sowohl in die einzelnen Dienste und Artefakte als auch in das System als Ganzes zu generieren und damit das Funktionieren des Systems Cloud-Computing zu ermöglichen. Dies bedeutet eine Übersetzung der Vertrauensanforderungen in technische Elemente und sozio-technische Prozeduren, die bereits in frühen Phasen der Entwicklung grundlegend stattfinden muss. Der erfolgreiche Einsatz von Cloud-Technologien erfordert es also, dass die Herstellung von Vertrauen von Anfang an eines der entwurfsleitenden Prinzipien darstellen muss – analog zu *privacy by design* lässt sich beim Cloud-Computing also das Erfordernis eines *trust by design* feststellen.

IPACS – beispielhafte Implementierung von TbD

Die Umsetzung dieses Prinzips kann dabei unterschiedliche Dimensionen fokussieren: Nämlich erstens diejenige der Einbettung der Technik in organisationale Zusammenhänge wie Zertifizierung und Monitoring (um das Risiko zu streuen). Eine Sonderrolle nimmt hierbei noch die technische Normung ein, wie Wagner (1994) ausführt. Die zweite Ebene ist diejenige der Technik, wo die Erwartbarkeit und Berechenbarkeit des Verhaltens der Cloud, ihrer Akteure und Artefakte dadurch gesteigert werden kann, dass transparente Regeln implementiert werden, denen die sozio-technischen Prozesse unterworfen werden.

Vor allem an dieser Stelle setzt unser nachfolgendes Beispiel an, das diesen Gedanken illustrieren soll, *Trust by Design* als Gestaltungsprinzip schon in frühen Entwicklungsschritten zu implementieren. Es entstammt einem laufenden interdisziplinären Projekt, in welchem es um die nutzerzentrierte Entwicklung technischer Grundlagen für cloud-basierte Assistenzsysteme geht (RWTH-Exzellenzmittelprojekt IPACS[5]). Zwar bezieht sich das Beispiel auf ein konkretes Szenario aus dem Bereich altersgerechter Assistenzsysteme (Ambient Assisted Living, AAL), letztlich liegt

5 IPACS steht für *intelligent privacy-aware cloud-based services*; es sollen Grundlagen für umfassende, sichere sensor- und cloud-basierte Lösungen geschaffen werden (zum Beispiel für tragbare Geräte als interaktive Hilfe in öffentlichen Räumen und im privaten Wohnumfeld).

dieser Konzeption aber die Annahme zugrunde, dass die Übersetzung der Vertrauensanforderungen in die nachfolgend dargestellten technischen Elemente und sozio-technischen Prozeduren über das konkrete Szenario hinaus verallgemeinerbar sind.

Nun zu dem konkreten Implementierungsbeispiel (vgl. nachfolgende Abbildung): Wir gehen davon aus, dass jede Nutzerin oder jeder Nutzer eine mehr oder weniger große Zahl an vernetzten Geräten im alltäglichen Gebrauch hat: Hierbei kann es sich beispielsweise um die inzwischen ubiquitären Smartphones oder Tablet-PCs handeln; genauso kann es sich allerdings um avanciertere Gerätschaften wie körpernah getragene Sensorik oder intelligente Wohnraumausstattung handeln. Jedes dieser Geräte ist vernetzt, das heißt letztlich in und mit verschiedenen Netzwerken (vom WAN, Wide Area Network, bis hin zum WBAN, Wireless Body Area Network) online. Alle diese technischen Artefakte, somit letztlich Netzwerke, formen die Privatsphäre (privacy sphere) der Nutzer/-in mit, wobei wir davon ausgehen, dass diese(r) in ihr die jeweiligen Komponenten mehr oder weniger habituell verwendet. Jedes dieser Netzwerke ist mit der Cloud über ein spezifisch ausgelegtes Gateway verbunden (GW; hier PEP genannt; dazu vgl. weiter unten); und Daten dieser Netzwerke werden über das GW in der Cloud gespeichert und für den Zugriff verschiedener Dienste/Services (S) und Notfallservices (emergency services, ES) vorgehalten. Diese verschiedenen Dienstangebote (welche ganz unterschiedliche aus dem Bereich des Ambient Assisted Living sein können) werden von Dienste-Entwicklern (service developer, SD) entwickelt und mit Blick auf ihre Funktionalität (zum Beispiel lastabhängiger Skalierung) implementiert.

Zentrale Herausforderung ist nun, dass potentiell persönlichkeitssensitive Daten möglicher Nutzerinnen und Nutzer Dritten natürlich nicht zugänglich sein sollen. Da jede Person nur ihre jeweiligen Daten sehen und ändern können soll, geschieht dies mittels der sogenannten privacy enforcement points (PEPs) am gerade bereits eingeführten Gateway. Die technische Funktionalität dieser Instanz lässt sich vereinfachend dahingehend zusammenfassen, dass die PEPs einerseits die sichere wechselseitige Authentifizierung zwischen den vernetzten Geräten und der Cloud garantieren, und es andererseits dem Nutzer erlauben, den Datentransfer mittels (semantischer) Annotationen (A) zu restringieren (zum Beispiel Metadaten im Sinne wer wann auf welche Daten zugreifen darf; Henze et al. 2014). Auf Entwickler/-innenseite werden durch die Benutzung einer vereinheitlichten Modellierungssprache (Unified Modeling Language, UML; Rumpe 2011) service-spezifische Teilspezifikationen (hier privacy policies, PP genannt) und genau solche gerade erwähnten Metamodellierungen (M) festgelegt, die dann wiederum durch einen vertrauenswürdigen Dritten (hier trusted third party, TTP genannt, zum Beispiel das Bundesamt für Sicherheit in der IT, BSI) begutachtet und in Form von privatsphäreschützenden Einstellungen (privacy configuration, PC) gegenüber den Nutzerinnen und Nutzern als vertrauenswürdig verifiziert werden.

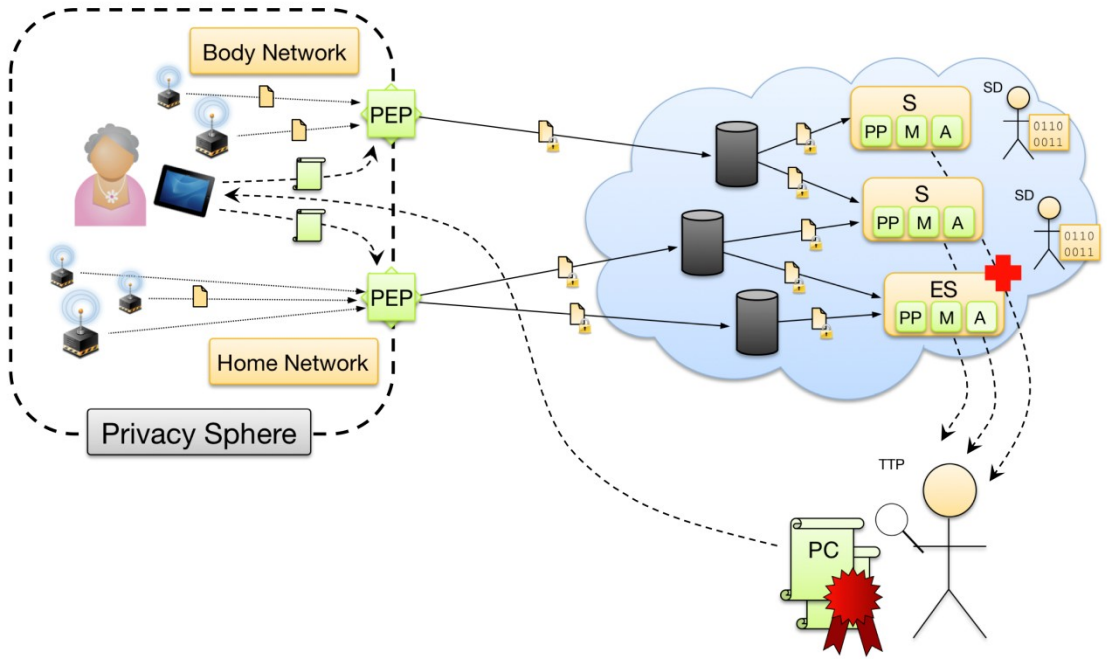

Abb. 1: technisches Schema der vorgestellten TbD-Implementierung (Henze et al. 2014)

Zusammenfassung und Ausblick

Für den aktuell bereits umfassenden und zukünftig weiter zunehmenden Einsatz vernetzter IT bietet Cloud-Computing ein Konzept an, um die dafür notwendigen technischen Kapazitäten und Dienstleistungen ressourceneffizient vorhalten und verlässlich zur Verfügung stellen zu können. Ob das hinter der Cloud stehende Konzept allerdings funktioniert, ist keine ausschließlich technisch beantwortbare Frage. Die Vielzahl der technischen Elemente und sozialen Akteure, die an der Cloud beteiligt sind, machen aus dieser ein hochgradig komplexes sozio-technisches Netzwerk, das für die Nutzerinnen und Nutzer nahezu unüberblickbar ist. Eine Anwendung von Cloud-Computing ist also immer mit einem gewissen Risiko verbunden, das kompensiert werden muss, wenn Cloud-Technologien eingesetzt werden sollen. Ob dieses Risiko eingegangen werden kann, können die Akteure nur im unwahrscheinlichen Fall vollständiger Information alleine aufgrund des verfügbaren Wissens entscheiden. Daher ist der Einsatz von Cloud-Technologien und -Anwendungen immer auf das Vorhandensein von Vertrauen als investierbarer und investierter sozialer Ressource angewiesen.

Dieses Erfordernis einer Ermöglichung von Vertrauensinvestitionen in Cloud-Technologien und -Anbieter/-innen muss bereits während des gesamten Cloud-Entwicklungsprozesses reflektiert und im Entwurf der technischen Artefakte und Dienstleistungen berücksichtigt werden. Die Aufgabe, Anwendungen und Technologien für die Cloud zu entwickeln, kann damit nicht auf technische Entwicklungen reduziert werden. Cloud-Entwickler/-innen müssen darüber hinaus die Rolle von *system builders* einnehmen, deren Aufgabe auch darin besteht, geeignete Mechanismen zur Ermöglichung von Vertrauen in die einzelnen Anbieter und Techniken sowie in das

gesamte System Cloud-Computing zu implementieren und damit ein Prinzip von *trust by design* bei ihrer Entwicklungstätigkeit umzusetzen.

Das abschließend dargestellte Beispiel illustriert, wie eine Ebene der Forderung nach *trust by design* in der Entwicklung von Cloud-Technologien implementiert werden kann. Dabei erscheint der in diesem Kontext gewählte Implementierungsansatz als eine geeignete Möglichkeit, Vertrauen beziehungsweise das diesem komplementäre Misstrauen anhand des PEPs und der Vertrauensintermediäre (trusted third parties) zu institutionalisieren. Darüber hinaus verdeutlicht es, wie auch auf Seiten der Cloud-Entwickler/-innen mittels einer modellbasierten Herangehensweise, die soziologische Expertise einbezieht, versucht werden kann, die Eigenschaften und Verhaltensweise des Vertrauensempfangenden, also des cloud-basierten Systems, erwartbarer zu gestalten, um dadurch den beteiligten Akteuren die Aufnahme einer Kooperationsbeziehung zu erleichtern. Allerdings bezieht sich das hier vorliegende Beispiel lediglich auf einen Teil der Vertrauensfragestellungen. Im Sinne einer vertrauens- und nutzer/-innenorientierten Entwicklung von Cloud-Technologien und -Anwendungen besteht nun die weitere Herausforderung darin, Möglichkeiten des *trust by design* für die unterschiedlichen Dimensionen der cloud-relevanten Vertrauensproblematik zu formulieren und diese Prinzipien bei der Entwicklung cloud-basierter Technologien und bei deren sozialer Kontextualisierung zu implementieren.

Literatur

Atzori, L., Iera, A., Morabito, G. 2010: The Internet of Things: A survey. Computer Networks, 54. Jg., Heft 15, 2787–2805.

Bundesministerium für Wirtschaft und Energie (BMWi) (Hg.) 2014: Trusted Cloud. Innovatives, sicheres und rechtskonformes Cloud Computing, akt. Neuauflage (Februar 2014). Berlin: Bundesministerium für Wirtschaft und Energie.

Dukat, C., Caton, S.: »Social Cloud« – Spezifika dieses Cloud-Konzepts unter Berücksichtigung von Kompetenz und Vertrauen. In diesem Band.

Eggert, M., Kerpen, D., Rüssmann, K., Häußling, R. 2014a: SensorCloud: Sociological Contextualization of an Innovative Cloud Platform. In H. Krcmar, R. Reussner, B. Rumpe (Hg.), Trusted Cloud Computing. Cham et al.: Springer International Publishing, 295–313.

Eggert, M., Häußling, R., Henze, M., Hermerschmidt, L., Hummen, R., Kerpen, D., Navarro Pérez, A., Rumpe, B. Thißen, D., Wehrle, K. 2014b: SensorCloud: Towards the interdisciplinary development of a trustworthy platform for globally interconnected sensors and actuators. In H. Krcmar, R. Reussner, B. Rumpe (Hg.), Trusted Cloud Computing. Cham et al.: Springer International Publishing, 203–218.

Endreß, M. 2002: Vertrauen. Bielefeld: transcript.

Giese, H., Rumpe, B., Schätz, B., Sztipanovits, J. 2011: Science and Engineering of Cyber-Physical Systems (Dagstuhl Seminar 11441). Dagstuhl Reports, 1. Jg., Heft 11, 1–22.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., Wehrle, K. 2014: User-Driven Privacy Enforcement for Cloud-Based Services in the Internet of Things. 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014), 27–29 August 2014, Barcelona, Spain.

Hirsch-Kreinsen, H., 2014: Wandel von Produktionsarbeit – Industrie 4.0. Soziologisches Arbeitspapier Nr. 38/2014 (Januar). Dortmund: Wirtschafts- und sozialwissenschaftliche Fakultät der TU Dortmund, http://www.wiso.tu-dortmund.de/wiso/de/forschung/gebiete/fp-hirschkreinsen/forschung/soz_arbeitspapiere/AP-SOZ-38.pdf (letzer Aufruf 31.05.2015).

Irrgang, B. 2010: Technikvertrauen und autonom-intelligente Technologie. Ethica, 18. Jg., Heft 4, 339–363.

Liu, Z., Yang, D.-S., Wen, D., Zhang, W.-M., Mao, W. 2011: Cyber-Physical-Social Systems for Command and Control. IEEE Intelligent Systems, 26. Jg., Heft 4, 92–96.

Luhmann, N. 1989: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart: Enke.

Möllering, G. 2011: Vernebeltes Vertrauen? Cloud Computing aus Sicht der Vertrauensforschung. In A. Picot, U. Hertz, T. Götz (Hg.), Trust in IT. Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an? Berlin, Heidelberg: Springer, 39–47.

Nof, S. Y. (Hg.) 2009: Springer handbook of automation. Berlin, Heidelberg: Springer.

Ortmann, U.: »Was bedeutet Industrie 4.0 für unser Unternehmen?« Partizipative Technikfolgenabschätzung im Industriebetrieb. In diesem Band.

Pantelopoulos, A., Bourbakis, N. G. 2010: A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 40. Jg., Heft 1, 1–12.

Petersen, I., Kollek, R.: Digitale Forschungskulturen in der Systemmedizin. In diesem Band.

Preisendörfer, P. 1995: Vertrauen als soziologische Kategorie. Möglichkeiten und Grenzen einer entscheidungstheoretischen Fundierung des Vertrauenskonzepts. Zeitschrift für Soziologie, 24. Jg., Heft 4, 263–272.

Reischauer, G.: Über den Wolken? Zur Grenzenlosigkeit von Cloud Computing aus der Perspektive des organisationalen Lernens. In diesem Band.

Ropohl, G. 2010: Das Misstrauen in der Technikdebatte. In: M. Maring (Hg.), Vertrauen – zwischen sozialem Kitt und der Senkung von Transaktionskosten. Karlsruhe: KIT Scientific Publishing, 115–132.

Rumpe, B. 2011: Modellierung mit UML. Sprache, Konzepte und Methodik, Berlin, Heidelberg: Springer.

Rüssmann, K., Eggert, M. 2014: Cloud-Computing im Kontext Smart Home: Akzeptanzbarrieren und Anforderungen. Aachen: Publikationsserver der RWTH Aachen University. urn:nbn:de:hbz:82-opus-52552.

Simmel, G. 1992: Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Frankfurt am Main: Suhrkamp.

Simon, H. A. 1972: Theories of bounded rationality. In: C. B. MacGuire, R. Radner (Hg.), Decision and organization. A volume in honour of Jacob Marschak. Amsterdam et al.: North-Holland Publishing Co, 161–176.

Strasser, H., Voswinkel, S. 1997: Vertrauen im gesellschaftlichen Wandel. In M. Schweer (Hg.), Interpersonales Vertrauen. Theorien und empirische Befunde. Opladen: Westdeutscher Verlag, 217–236.

Wagner, G. 1994: Vertrauen in Technik. Zeitschrift für Soziologie, 23. Jg., Heft 2, 145–157.