# Nachhaltiges Computing in Clouds

DOI 10.1007/s11576-011-0273-3

## Die Autoren

**Prof. Dr. Günter Müller** (✉)
Institut für Informatik und Gesellschaft
Abteilung Telematik
Universität Freiburg
Friedrichstr. 50
79098 Freiburg
Deutschland
mueller@iig.uni-freiburg.de

**Prof. Dr. Noboru Sonehara**
**Prof. Dr. Isao Echizen**
**Dr. Sven Wohlgemuth**
National Institute of Informatics (NII)
2-1-2 Hitotsubashi, Chiyoda-ku
Tokyo 101-8430
Japan
Sonehara@nii.ac.jp
iechizen@nii.ac.jp
wohlgemuth@nii.ac.jp

Online publiziert: 2011-04-15

This article is also available in English via http://www.springerlink.com and http://www.bise-journal.org: Müller G, Sonehara N, Echizen I, Wohlgemuth S (2011) Sustainable Cloud Computing. Bus Inf Syst Eng. doi: 10.1007/s12599-011-0159-3.



Cloud-Computing verspricht Kosteneffizienz und Flexibilität, vor allem aber einen unbegrenzten Zugang zu potenziell wirtschaftlich relevanten Diensten. Diese hohe Abstraktionsebene von Diensten und ihre jederzeitige Verfügbarkeit verändert nicht nur die Entwicklung sondern auch das Computing von Informationssystemen. Man lagert das Rechnen in eine unbekannte „Wolke“ (Cloud) aus und bezieht von dort die gewünschten Dienste und orchestriert sie z. B. zu höherwertigen Geschäftsprozessen. Im Privaten geschieht dies bereits millionenfach durch die Smartphones, die einen weltweiten Boom erleben und die alle auf die Telefonie beschränkten Geräte verdrängen werden. Die Unternehmen werden diesem Vorbild folgen und dadurch sowohl die betriebswirtschaftlichen Funktionen vereinheitlichen und das Rechnen globalisieren. Solche Veränderungen erzeugen Widerstände, die gegenwärtig vor allem durch den Zweifel am Schutz kritischer Informationen genährt werden. Ein wenig diskutierter Aspekt spielt vor allem in Japan eine wichtige Rolle, indem sie dort die Cloud als überlebensverbessernde Infrastruktur im Falle von Katastrophen interpretieren.

Nachhaltigkeit in der IT ist ein werbewirksames Schlagwort geworden, wobei vor allem eine irgendwie geartete ökologische Auswirkung gemeint ist. Der ursprüngliche, nicht-IT bezogene Begriff der Nachhaltigkeit betont die Notwendigkeit, Abhängigkeiten zwischen der vergangenen, aktuellen und zukünftigen Entwicklung zu berücksichtigen und ist ein Synonym für Moderne. IT wird im Allgemeinen vor allem in zwei Bereichen mit Nachhaltigkeit in Verbindung gebracht. Zum einen soll Hardware nachhaltig zu erzeugen sein und betrieben werden. Dies ist das Ziel der „Green-IT“. Dabei soll der momentan teilweise noch immense Energieverbrauch z. B. für den Betrieb und die Kühlung von Rechneranlagen reduziert werden. „Green-IS“ hingegen sieht Cloud-Computing als wichtiges Mittel bei der Lösung von Nachhaltigkeit, damit das „produziere und konsumiere“ Paradigma durch eine ökologischere Variante der Produktion ersetzt werden kann. Das aktuelle Green-IS-Thema sind die durch Cloud ermöglichten Skaleneffekte, welche durch individuelle Unternehmen oder ausgelagerte IT-Anbieter nicht erzielbar sind und die zugleich über eine optimale Ressourcenplanung die regenerative Produktion fördern. Unternehmen aller Art profitieren dabei von dem in globalen Maßstab durchgeführten Benchmarking und der Standardisierung von Diensten. Die IT-Kosten fallen.

Generell werden weltweit die ähnlich lautenden Einwände gegen Cloud in der mangelnden Fähigkeit zum Schutz kritischer Daten gesehen. Dieser ist mit einem Kontrollverlust und der Furcht der Nutzer vor Regelverletzungen verbunden, welche die Reputation, das Verhältnis zu Partnern und Kunden oder die Compliance beschädigen können. Wie gut ungewollte Informationsflüsse und Datenmissbrauch vermieden werden können, wird in diesem Sonderheft der WIRTSCHAFTSINFORMATIK als Trennlinie zwischen nachhaltigem und nicht-nachhaltigem Cloud-Computing betrachtet. Da missbrauchte Daten keinen Weg zurück erlauben, ist ein System dann nicht nachhaltig, wenn solcher Datenmissbrauch zu wirtschaftlich relevantem Schaden führt. Neben Green-IT und Green-IS gibt es einen dritten, weit weniger häufig bearbeiteten Nachhaltigkeitsaspekt. Japanische Planungen zu Cloud-Computing betonen die Schutzfunktion, die das Überleben und den Neubeginn nach Katastrophen fördern soll.

Ironischerweise ist ausgerechnet die Branche, die dem Cloud-Computing am nächsten steht, am weitesten davon entfernt. Merill Lynch (Chow et al. 2009) zufolge gibt es bisher nur ein IT-Unternehmen, nämlich die Softwarefirma „Salesforce.com“, das komplett Cloud-basiert arbeitet. Dieselbe Studie besagt ferner, dass die Top-Fünf-Softwarefirmen (gemessen am Umsatz) nur wenig Gebrauch von der Cloud machen und ihre sensitiven Daten nicht in eine Umgebung verlagern möchten, die sie als nicht zuverlässig und unkontrollierbar einstufen. Diese Furcht geht soweit, dass sogar die allgemein verwendeten Kommunikationsdienste wie soziale Netze für Mitarbeiter teilweise verboten werden. Entgegen der ursprünglichen Cloud-Vision, dass Nutzer sich nicht darum kümmern sollten, wo die Dienste faktisch ausgeführt bzw. ausgerechnet werden, ist nun genau die Unkenntnis des Ortes der Datenspeicherung und -bearbeitung

zum Haupthindernis für die Verbreitung geworden. Die Mehrheit der börsennotierten Unternehmen lagert deswegen meist unwichtige Prozesse oder statistische, also keine direkt für das operative Geschäft relevanten Daten aus. Hinzu kommt die Sorge, Cloud-Anbieter könnten Schlussfolgerungen oder Inferenzen aus der Dienstenutzung ihrer Kunden ziehen und damit Einblick in deren Pläne erhalten bzw. Profile der Geschäftsmodelle bilden. Solche Sorgen werden auch durch die Visionen, z. B. der IBM,[1] mit ihrem Vorhaben wie *smarter Planet* oder die Pläne der EU mit dem Forschungsprogramm *Internet of Services*[2] nicht aufgehoben, da dabei vor allem die Kommunikationsfähigkeit im Vordergrund steht. Um jedem Misstrauen zu begegnen, dass die Cloud-Anbieter Daten und Prozesse nicht hinreichend schützen können, muss Transparenz zur Datenverwendung und -verarbeitung geschaffen werden. Eine solche Transparenz aber wird bei allen Betreibern noch sehr klein geschrieben, dies auch deshalb weil geeignete Mechanismen fehlen, um das Vertrauen zu erhöhen. Während z. B. die Vorratsdatenspeicherung der Telekom Anbieter ein halbes Jahr gesetzlich vorschreibt, hat sich Google im Rahmen einer Selbstverpflichtung auf eine 18-monatige Speicherung der Benutzerdaten festgelegt. Da alle kooperativen Dienste auf dem Austausch von attraktiven Diensten gegen private Daten beruhen, ist das Vertrauensdefizit von Unternehmen durchaus nachvollziehbar, wenn auch die private Akzeptanz von Cloud-Diensten ein anderes Bild gibt. Regelkonforme Informationsflüsse sind folgerichtig eine technische Anforderung zur Nachhaltigkeit der Cloud.

Die Notwendigkeit des Cloud-Computings zur Aufrechterhaltung von lebensnotwendigen Infrastrukturen erfordert neben der Kontrollfrage zusätzliche Sicherheitseigenschaften. In Japan sieht man die Nachhaltigkeit durch den Einsatz von Cloud in den mit 5 E's (*Energy, Education, Employment, Environment, Elderly*) bezeichneten sozialen Infrastrukturen gewährleistet (Government of Japan 2011). Bei dem in diesem Heft im Vordergrund stehenden Katastrophenmanagement muss die Sicherheit und Transparenz dazu durch Redundanz und Verfügbarkeit ergänzt werden. Die von Aoyama et al. beschriebenen japanischen Bemühungen, eine Naturkatastrophen trotzende IT-Infrastruktur aufzubauen, stellen ein überzeugendes Beispiel dar, um nicht nur Cloud-, sondern sogar Inter-Cloud-Computing zu fordern. In zahlreichen Projekten, anhand derer Japan eine Verbesserung der sozialen Infrastrukturen anstrebt, sind die Sicherheitsprobleme tendenziell nachrangig zu den Eigenschaften Verfügbarkeit und Flexibilität gereiht. Watanabe betont in dem Interview in der vorliegenden Ausgabe der WIRTSCHAFTSINFORMATIK, dass für die japanische Regierung eine alle Aspekte umfassende Nachhaltigkeit der Maßstab für die Cloud-Computing-Strategie Japans sei.

Viele der Nachhaltigkeitsprobleme bei Cloud-Computing erscheinen als „alter Wein in neuen Schläuchen", werden sie doch oft nur als ein Aufguss schon früher bekannter Probleme dargestellt, auch wenn sie aus ökonomischen Überlegungen heraus jetzt drängender sein mögen. Die Preise für Rechnerleistung fallen angesichts bereits jetzt bestehender Überkapazitäten und der weltweiten Vernetzung so stark, dass einzelne Firmen ohne den Einsatz von Cloud-Diensten nicht mehr wettbewerbsfähig sind. Ganz gleich, ob es früher um Auslagerung an externe Unternehmen oder die direkte Zusammenarbeit mit Partnern ging, weltweit stellen sich die gleichen Fragen nach Vertrauen und der Einhaltung von Gesetzen und Vereinbarungen sowie um die Gewährleistung einer umfassenden Verfügbarkeit in hoher Qualität. Zur Einschätzung der Problemkomplexität liegt der Vergleich zum Aufkommen von Open-Source-Software nahe, da diese bei reduzierten Kosten und in Kombination mit internationaler Standardisierung Start-Ups und IT-Abteilungen in die Lage versetzte, schnell Anwendungen zu entwickeln und einzusetzen. Genau wie beim Cloud-Computing blieb dabei vielfach die Kontrolle auf der Strecke, wie man an den von Schwachstellen geplagten heutigen Web Services noch erkennen kann. Die Parallelen zu den „alten" Softwareproblemen geben aber gleichzeitig auch Anlass zu der Hoffnung, dass die Fundamente zu Lösungen der „neuen" Cloud-Probleme vorhanden sind.

Sicherheit und Privatsphäre im Cloud-Computing können in der Tat auf die etablierten Forschungsergebnisse der „alten" Netzwelt setzen und diese weiterentwickeln. Die theoretische Beschränkung der Nachhaltigkeit liegt in der Vollständigkeit bzw. realen Unvollständigkeit des gültigen Angreifermodells. Gegen einen unbekannten Angreifer kann keine Sicherheit erreicht werden, weil ja zwangsläufig unvollständig bleiben

[1] http://www.ibm.com/smarterplanet/us/en/.
[2] http://ec.europa.eu/information_society.

muss, gegen wen, was und wie geschützt werden soll. Nicht erfasste Bedrohungen stellen Schwachstellen dar, anhand derer als sicher bezeichnete Protokolle gebrochen werden können. Die Entwicklung von Sicherheitsmechanismen erfolgt generell unter dem Paradigma des „idealen" Modells für die Zugangskontrolle; d. h. die beteiligten Parteien sind vollständig erfasst und senden ihre Eingaben an eine als vertrauenswürdig definierte dritte Partei, welche die Ergebnisse ohne eigene Interessen berechnet und zurücksendet. Wäre dieses Ideal technisch erreichbar, gäbe es die Diskussionen um die vom Nutzer unbemerkte Nutzung von persönlichen Daten bei den sozialen Diensten nicht. Auch bei Cloud-Anbietern ist ein Übereinklang von „ideal" und „real" nicht zu erwarten. Von Sonehara, Echizen und Wohlgemuth wird zu diesem Problem eine Übersicht der aktuellen Forschung gegeben, die unter dem sehr originellen Aspekt zusammengestellt ist, dass die Methoden zur Aufrechterhaltung der Privatsphäre auch in der Cloud Anwendung finden können. Es ist nicht der Zugang zu den Daten und Diensten, der neu geregelt werden muss, sondern die Sicherstellung der „vereinbarten" Nutzung. Die Autoren diskutieren dazu die Nutzungskontrolle und führen die bislang wenig beachtete Delegation von Rechten als Grundlage von individueller Vertragsgestaltung für Cloud-Dienste ein. Mit solchen Mechanismen können das „ideale" und das „reale" Sicherheitsmodell leichter miteinander verschmelzen. Neuartig ist der Audit-basierte Ansatz von Accorsi, Lowis und Sato, die Nachhaltigkeit mithilfe von aus Log-Aufzeichnungen abgeleiteten Mustern verbessern wollen. Bei einem Audit lassen sich so zwar neue Angriffe nicht ausschließen bzw. abwehren, aber nach ihrem ersten Auftreten erkennen und dann durch Anpassung des realen Sicherheitsmodells in Zukunft verhindern. Ein solches System lernt. Die Qualität des Schutzes vor Kontrollverlust erfolgt daher erst „nach" der Transaktion. Sollten sich aus den Angriffen „Muster" oder „Klassen" ergeben, können diese schon zum Entwurfszeitpunkt – also „vor" der Transaktion – verwendet werden. Genügt ein Dienst einem solchen Sicherheitsmodell, kann ein Zertifikat vergeben werden, um nicht bei jeder Transaktion eine teure Prüfung vornehmen zu müssen. Einen Beitrag zur nachhaltigen Zusammenarbeit mehrerer Parteien in der Cloud liefert Kerschbaum, der nicht nur den sicheren Austausch, sondern auch die sichere Berechnung gemeinsamer Ergebnisse anstrebt, ohne dabei Informationen preiszugeben, die nicht erforderlich sind. Aufbauend auf der von Yao im Jahr 1987 vorgestellten Theorie der Nicht-Unterscheidbarkeit für sicheres Mehrparteienrechnen lautet die Annahme, dass ehrliche Parteien die Protokollschritte genau einhalten und ihre Ausgabe nach einer vereinbarten Vorgabe erzeugen. Authentifizierte Kanäle können ja schon heute anhand von digitalen Signaturen in der Public-Key-Infrastruktur gekennzeichnet werden. Die Herausforderung und das Qualitätskriterium für Sicherheit bestehen nun darin, eine Abfrage an die Cloud zu stellen, ohne dass dabei die Abfrage selbst erkennbar wird. Die Privatsphäre und Sicherheit wird selbst dann gewahrt, wenn ein „böswilliger" Server in der Cloud beteiligt ist. Kerschbaum schlägt ein Verfahren zum Schutz vor ungewollten Informationsflüssen bei der Cloud-Benutzung vor und zeigt, dass eine Abfrage A aus Sicht der Cloud nicht von einer Abfrage B zu unterscheiden ist.

Dieses Schwerpunktheft der WIRTSCHAFTSINFORMATIK hat durch die Katastrophen, die im März 2011 über Japan hereingebrochen sind, eine schreckliche Aktualität erhalten. Neben dem anlaufenden Wiederaufbau bitten wir auch die Überlebenden nicht zu vergessen, die vielfach bei „Null" beginnen und auf Unterstützung angewiesen sind. Wir danken allen denen, die dabei auf ihre Weise in ihrem Wirkungskreis helfen.

## Literatur

Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on cloud computing security, CCSW'09, S 85–90

Government of Japan (2011) Highlighting Japan, vol 4, February 2011. The cabinet office. http://www.gov-online.go.jp/eng/publicity/book/hlj/