Vorschläge für ein datenschutzkonformes Cloud Computing

In den letzten Jahren hat sich bei der Bereitstellung von IT-Ressourcen ein Konstrukt etabliert: Das Cloud Computing. Darunter wird gemeinhin verstanden, dass IT-Systeme über eine für den Anwender nicht näher spezifizierte und ggf. dynamisch erfolgende Verteilung verwendbar sind; die IT-Systeme stehen für den Anwender in einer für ihn undefinierten "Wolke" zur Verfügung. Dieses Konstrukt ist zwar an sich nicht neu, da es beispielsweise schon seit vielen Jahrzehnten "verteiltes Rechnen" gibt, dennoch ist die Umsetzung und Bereitstellung für einen breiteren Nutzerkreis dieser Struktur konsequenter als frühere Ansätze. Beim Cloud Computing wird im Wesentlichen[1] unterschieden zwischen einer verteilten Nutzbarkeit von Software[2] (Applikationen), Plattformen[3] (Datenbanken und Run-Time-Environment) und Infrastrukturen[4] (Hardware, Speicher- und Netzkapazitäten). Das Konstrukt unterscheidet sich von einer ebenfalls seit geraumer Zeit häufig anzutreffenden Virtualisierungslösung durch die Verteiltheit der verwendeten IT-Ressourcen sowohl über Lokationen als auch über legale Entitäten hinweg.

Probleme und Chancen des Cloud Computings

Bei der Betrachtung des Cloud Computings aus Sicht des Datenschutzes und der Informationssicherheit treten folgende **Problemfelder** zutage[5]:

- Die nicht zwingend für den Anwender feststellbare Lokation der bereitgestellten IT-Ressourcen wirft Probleme des anzuwendenden nationalen Rechts auf, so dass die damit verbundenen Rechtsrisiken nicht vollständig beurteilt werden können.
- Die Durchsetzbarkeit und Kontrollierbarkeit vereinbarter Leistungen wird durch die "Wolken"-Struktur beschränkt.
- Da im Rahmen von Cloud Computing für den Anwender ggf. sensible bzw. geschäftskritische Daten außerhalb des eigenen Wirkungsbereichs automatisiert verarbeitet werden, stellen sich Fragen nach der Beherrschbarkeit der damit verbundenen Informationssicherheit.

Auf der Gegenseite stehen einige, durchaus erhebliche **Chancen** des Cloud Computings:

- Die Fortentwicklung der Informations- und Kommunikationstechnik verläuft rasant[6], so dass vor allem mittelständische Unternehmen kaum noch in der Lage sind, sich auf aktuellem Stand zu bewegen – sowohl aus finanziellen Gründen hinsichtlich der Anschaffung der Informations- und Kommunikationstechnik einerseits als auch der Betreubarkeit durch qualifiziertes und hochspezialisiertes Personal andererseits. Cloud Computing bietet hierfür einen Ausweg, da entsprechende IT-Ressourcen

[1] siehe auch [ENISA2009], S. 14f, sowie [CSA2009], S. 14
[2] unter dem Schlagwort "Software as a Service" (SaaS); eine Übersicht zu deren Chancen und Risiken liefert z.B. [Benlian+2010]
[3] unter dem Schlagwort "Platform as a Service" (PaaS)
[4] unter dem Schlagwort "Infrastructure as a Service" (IaaS)
[5] zu den rechtlichen Problemen siehe auch [Pohle+2009] sowie [Karger+2009] und [Reindl2009]
[6] siehe auch [Witt2010], S. 11ff

durch eine Stelle betrieben werden, die über beides dagegen verfügt. Das hierfür zu entrichtende Entgelt ist dagegen für den Anwender überschaubar und ausreichend skalierbar.

- Bestehende Grenzen eigener IT-Ressourcen im Rahmen des Kapazitätsmanagements können durch Cloud Computing durchbrochen werden, was einerseits zur Entlastung von Auslastungsspitzen und andererseits zu einer Reduzierung eigener IT-Ressourcen führt auf die auf Grundlage der Ergebnisse eines durchgeführten IT Risk Assessments bzw. zur besseren Umsetzbarkeit der Steuerung im Rahmen der IT Governance zwingend selbst zu betreibenden Verfahren und IT-Systeme.

Während es an der datenschutzrechtlichen Zulässigkeit von Tätigkeiten mittels Cloud Computing keine Zweifel bestehen[7], werden aus juristischer Sicht vor allem Defizite bei der Rechtsdurchsetzung gesehen[8]. Typische **Lösungsszenarien** setzen bisher im Wesentlichen darauf auf, dass ein Generalunternehmer als Schnittstelle zwischen Anwender und Anbieter vermitteln soll[9], sofern der Anbieter nicht selbst aus einem EU-Land stammt. Damit sollen vor allem die Probleme umgangen werden, die sich aus einem Datentransfer jenseits des Schutzraums aus der EU-Datenschutzrichtlinie ergeben. Das etablierte Vorgehen zum IT Risk Management nach der ISO/IEC 27005:2008 lässt sich aus Sicht des Anwenders nicht direkt übertragen, sondern erfordert in Anlehnung an das Vorgehensmodell zur Auftragsdatenverarbeitung nach § 11 BDSG eine Abwandlung[10]. Die praktischen Probleme lassen sich auf diese Weise einigermaßen in den Griff kriegen.

Vorschläge für ein datenschutzkonformes Cloud Computing

Dennoch lohnt sich ein Blick darüber hinaus in einen neuen, noch zu schaffenden Rechtsrahmen, der bestehende Schwierigkeiten, die mit einer globalen, allgegenwärtigen und technikübergreifenden Datenverarbeitung wie Cloud Computing zusammen hängen, effektiv lösen könnte[11]. Zwar ist das Problem, wie derartige technische Entwicklungen angemessen innerhalb der Rechtsdogmatik abgebildet werden können[12], damit keineswegs abschließend gelöst und noch viele Detailfragen offen, doch könnte eine verstärkte Orientierung an Zielvorgaben besser als die bestehende Detailregelungsstrategie geeignet sein[13], um gerade solche Fälle global und systemadäquat lösen zu können.

Die nachstehenden Vorschläge sind dabei lediglich als ein erster Schritt in eine entsprechende Fachdiskussion anzusehen, sollen aber im Sinne mehrseitiger IT-Sicherheit für alle Beteiligten (Betreiber, Anwender und Betroffene) dabei helfen, Cloud Computing datenschutzfreundlicher zu gestalten. Einige Aspekte lassen sich bereits jetzt durchführen, bedürfen aber zur besseren Wirksamkeit einiger datenschutzrechtlicher Gesetzesänderungen, sowohl national als auch zumindest auf europäischer Ebene.

[7] siehe [Reindl2009], S. 448
[8] siehe [Karger+2009], S. 436f sowie [Obenhaus2010]
[9] siehe [Karger+2009], S. 429f, und [Bierekoven2009]
[10] siehe [Faber2009]
[11] im Sinne der Gewährleistung von Transparenz, Steuerbarkeit, Datensparsamkeit und Zweckbindung, die bei einer Datenverarbeitung mittels Ubiquitous Computing bereits zu adressieren sind (siehe [Witt2010], S. 208f)
[12] siehe auch [Witt2009]
[13] wie bereits in [Roßnagel+2001] angeregt

1. Verpflichtung des Anbieters zur Erstellung eines Datenschutzkonzepts

Die Betreiber einer Cloud sollten durch gesetzliche Anreize dazu verpflichtet werden, ein Datenschutzkonzept für das angebotene Modell zu erstellen. In diesem Datenschutzkonzept sind verbindlich die ergriffenen technischen und organisatorischen Maßnahmen auf aktuellem Stand der Technik und auf Basis eines umfassenden IT Risk Assessments unter Annahme eines hohen Schutzbedarfs für den gesamten Life Cycle zu beschreiben.

Das Datenschutzkonzept muss von unabhängiger Seite zertifiziert worden sein, um als Nachweis ausreichender Sorgfalt gewertet werden zu können. Ein entsprechender Nachweis brächte etwa bei der Abwehr von Schadensersatzansprüchen (z.B. nach § 7 BDSG) Rechtssicherheit für die Betreiber einer Cloud. Da Cloud Computing i.d.R. eben nicht an Ländergrenzen halt macht, sollten entsprechende Regelungen nicht auf Deutschland beschränkt bleiben[14].

Die Zertifizierbarkeit von Datenschutzkonzepten auf der Grundlage eines Datenschutzauditgesetzes sind bisher an der Konstruktion gescheitert, dass eine Zertifizierung des Einhaltens datenschutzrechtlicher Vorschriften schwerlich den Aufwand für ein Zertifizierungswesen rechtfertigen könne. Wenn sich daraus jedoch haftungsrechtliche Vergünstigungen nachweislich ergeben könnten, führt dies zu einer erhöhten Bereitschaft bei Anbietern und Sinnhaftigkeit des Zertifizierungswesens bei Aufsichtsbehörden. Entscheidend ist in diesem Zusammenhang jedoch, dass sich die Datenschutzkonzepte am tatsächlichen best practice orientieren. Als Referenz eines adäquaten IT Risk Assessments können die Szenarien[15] aus [ENISA2009] Verwendung finden.

2. Vereinbarung verbindlicher Service Level Agreements

Anwender müssen sicher sein können, dass ihre Anforderungen im Rahmen genutzten Cloud Computings eingehalten werden. Vertragstechnisch lässt sich dies am besten absichern, indem beide Seiten miteinander Service Level Agreements (SLAs) vereinbaren. Damit die Rechtsdurchsetzung gewährleistet ist, müssen diese über eine ausreichende Verbindlichkeit verfügen.

Die via SLAs gegebenen Garantien sollten dabei nicht nur eine ausreichende Verfügbarkeit, sondern auch (in Abhängigkeit zum Gegenstand des Cloud Computings) zumindest eine ausreichende Vertraulichkeit, Integrität und Zurechenbarkeit zusichern. Ferner ist die Zweckbindung der via Cloud Computing automatisiert verarbeiteten Daten zu gewährleisten. In diesen SLAs sind außerdem die Vorgaben einschlägiger internationaler Standards (wie z.B. bei der Bereitstellung von Speicherkapazitäten der ISO/IEC 24762:2008) zu berücksichtigen.

Diese Garantieerklärung hat rechtsverbindlich selbst in den Staaten ohne angemessenes Datenschutzniveau im Sinne von Binding Corporate Rules zu erfolgen.

[14] einige Vorschläge an die Gesetzgeber formuliert auch [ENISA2009], S. 81 – 83
[15] siehe [ENISA2009], S. 21 – 62

3. Regelung einzelner Detailfragen zu Betroffenenrechte und Auftragsdatenverarbeitung

Für die Betroffenen erbringt ein Einsatz eines Cloud Computings u.U. Unklarheiten, wie seine personenbezogenen Daten durch die verantwortliche Stelle tatsächlich verwendet werden. Selbst wenn der Anbieter ausreichende Vorkehrungen getroffen hat und der Anwender mit dem Anbieter ausreichende Vereinbarungen getroffen hat, müssen Betroffene sicher sein können, dass ihre Rechte geeignet durchgesetzt werden.

Die Konstruktion des Cloud Computings dürfte in den meisten Fällen datenschutzrechtlich als Auftragsdatenverarbeitung (nach § 11 BDSG) zu qualifizieren sein. Hilfsweise lässt sich auch eine Legitimation aus § 28 Abs. 1 Nr. 2 BDSG herleiten, da im Regelfall das Betroffeneninteresse die Risiken aus der Übermittlung an den Anbieter aufgrund der Art der outgesourcten Tätigkeit nicht überlagern dürfte.

In beiden Fällen würde nach derzeitigem Stand der Betroffene keine Mitteilung erhalten, dass eine entsprechende Aufgabe mittels Cloud Computing erfüllt wird. Der Betroffene sollte in den Zyklus des Cloud Computings insoweit partizipieren, dass er im Rahmen seines **Auskunftsrechts** auch erfahren können soll, welcher Anbieter welche Daten des Betroffenen via Cloud Computing automatisiert verarbeitet. Auf den Umstand des Vorliegens eines zertifizierten Datenschutzkonzepts und der Vereinbarung wirksamer SLAs sollte der Betroffene ebenfalls hingewiesen werden, um das Cloud Computing mit einer höheren Vertrauensstellung versehen zu können.

Auf der Gegenseite sollte diese zusätzliche Auskunftspflicht entlohnt werden, indem das betreffende Cloud Computing trotz der fehlenden Weisungsbefugnis und unpräzisen Beschreibung detaillierter Vorgehensweisen als **Auftragsdatenverarbeitung** (unabhängig vom Erbringungsort!) datenschutzrechtlich eingestuft wird. Bereits jetzt sieht beispielsweise der neue § 11 Abs. 2 Nr. 9 BDSG vor, dass im zugrunde liegenden Vertrag der Umfang der Weisungsbefugnisse zu beschreiben und damit limitierbar ist. Die Vorgaben eines Auftraggebers sind üblicherweise bereits jetzt nur selten in letzter Konsequenz ausformuliert, da sich Auftragsarbeiten im Laufe der Gültigkeitsdauer auch in kleinen Details ohne Auswirkung auf die inhaltlichen Beschränkungen fortentwickeln[16].

Insofern wäre es nur konsequent, Tätigkeiten via Cloud Computing, die auf der Grundlage eines zertifizierten Datenschutzkonzepts (unter obigen Auflagen) und verbindlicher SLAs (unter obigen Vorgaben) angeboten werden, datenschutzrechtlich als Auftragsdatenverarbeitung zu klassifizieren. Dies ist bereits jetzt nach der EU-Datenschutzrichtlinie in vielen Fällen möglich[17].

[16] der Auftragnehmer ist nicht als "Sklave" des Auftraggebers anzusehen

[17] dennoch schlägt auch hierzu [ENISA2009], S. 83, Präzisierungen in einer überarbeiteten EU-Datenschutz-Richtlinie vor

Literatur

[Benlian+2010] Alexander Benlian, Thomas Hess und Peter Buxmann: Chancen und Risiken des Einsatzes von SaaS – die Sicht der Anwender. Wirtschaft & Management 02.2010, S. 23 – 32.

[Bierekoven2009] Christiane Bierekoven: Die Neuerungen / Herausforderungen des / durch Cloud Computing. Vortrag im Rahmen von [SECMGT2009]

[CSA2009] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf (Abruf vom 25.04.2010 13:40)

[ENISA2009] European Network and Information Security Agency: Cloud Computing – Benefits, risks and recommendations for information security, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (Abruf vom 25.04.2010 13:44)

[Faber2009] Eberhard von Faber: IT als Fremdleistung: Risikomanagement und Strategien für Anwender. Vortrag im Rahmen von [SECMGT2009]

[Karger+2009] Michael Karger und Frank Sarre: Wird Cloud Computing zu neuen juristischen Herausforderungen führen?, in: [Taeger+2009], S. 427 – 439.

[Obenhaus2010] Nils Obenhaus: Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft. Neue Juristische Wochenschrift, 10/2010, S. 651 – 655.

[Pohle+2009] Jan Pohle und Thorsten Ammann: Über den Wolken… - Chancen und Risiken des Cloud Computing. Computer und Recht 5/2009, S. 273 – 278.

[Reindl2009] Martin Reindl: Cloud Computing & Datenschutz, in: [Taeger+2009], S. 441 – 454.

[Roßnagel+2001] Alexander Roßnagel, Andreas Pfitzmann und Hansjürgen Garska: Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Inneren, 2001

[SECMGT2009] GI-Fachgruppe Management von Informationssicherheit: Workshop zur Informationssicherheit beim Cloud Computing vom 20. November 2009, http://www1.gi-ev.de/gliederungen/fachbereiche/sicherheit/fg-secmgt/workshops/2009-11-20/ (Abruf vom 25.04.2010 13:48)

[Taeger+2009] Jürgen Taeger und Andreas Wiebe (Hrsg.): Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Edewecht, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009, Tagungsband zur 10. Herbstakademie der Deutschen Stiftung für Recht und Informatik

[Witt2009] Bernhard C. Witt: Unsicherheit im Recht?. <kes> 2009#3, S. 31

[Witt2010] Bernhard C. Witt: Datenschutz kompakt und verständlich, Wiesbaden, Vieweg+Teubner Verlag, 2010, 2. Auflage