Vorschläge für ein datenschutzkonformes Cloud Computing

Durch Cloud Computing sind IT-Systeme über eine für den Anwender (in konsequenter Fortführung der Transparenzregeln verteilter Systeme) nicht näher spezifizierte und ggf. dynamisch skalierbare Verteilung interaktiv verwendbar. Dabei wird im Wesentlichen unterschieden zwischen einer verteilten Nutzung von Software (Applikationen), Plattformen (Datenbanken und Entwicklungsumgebungen) und Infrastrukturen (Hardware, Speicher- und Netzkapazitäten). Aus datenschutzbezogener Sichtweise sind darüber hinaus auch Unterscheidungen hinsichtlich der Verantwortungszuordnung (private/public/hybrid cloud) und dem zugrunde liegenden Automatisierungsgrad (und damit auch der Automatisierbarkeit technischer Kontrollsysteme) relevant.

Im Rahmen von Cloud Computing werden bisher häufig Datenschutz und Informationssicherheit gefährdet: Das anzuwendende Recht ist lokationsabhängig, so dass u.U. nicht alle Rechtsrisiken vollständig für Anwender abschätzbar sind, die Kontrollierbarkeit vereinbarter Leistungen ist durch die "Wolken"-Struktur i.d.R. beschränkt und schließlich ist für den Anwender der Umgang mit seinen Daten nicht in jedem Fall beherrschbar. Daher erfordert ein datenschutzkonformes Cloud Computing ein umfassendes Regelwerk, um dieses ausgleichen zu können.

Die sich zunehmend verbreitende, verteilte Bereitstellung entsprechender Ressourcen für Dritte gegen Entgelt kann dennoch nicht nur zu einer Kostenersparnis auf Seiten der Anwender führen, sondern sogar für alle Beteiligte lohnend sein, wenn nachstehende Vorschläge im Sinne mehrseitiger IT-Sicherheit berücksichtigt werden:

- Die Anwender sollten ihre Nutzung von Cloud Computing davon abhängig machen, ob die Einhaltung eines **Datenschutz– und Sicherheitskonzepts** zum angebotenen Cloud Computing mittels unabhängiger und qualifizierter Zertifizierung bestätigt wird. In diesem Konzept ist der Schutzbedarf aller Beteiligten (Betreiber, Anwender und Betroffene) im Zuge einer umfassenden IT-Risikoanalyse und –bewertung während des gesamten Lebenszyklus' eingesetzter IT-Systeme zugrunde zu legen und sind verbindlich die ergriffenen technischen und organisatorischen Maßnahmen auf aktuellem Stand der Technik zu beschreiben. Die Zertifizierung kann als Nachweis ausreichender Sorgfalt angesehen werden, so dass dies sowohl den Anwender als auch den Betreiber von Cloud Computing haftungsrechtlich entlastet. Allerdings sind die hierzu nötigen Zertifizierungsregelungen erst noch zu etablieren.
- Zwischen Anwender und Betreiber sind **Service Level Agreements** (SLAs) zu vereinbaren, in denen nicht nur wie üblich die Einhaltung einer ausreichenden Verfügbarkeit, sondern auch die Einhaltung weiterer Ziele der Informationssicherheit (wie zumindest eine ausreichende Vertraulichkeit, Integrität und Zurechenbarkeit) sowie der Zweckbindung der via Cloud Computing automatisiert verarbeiteten Daten vorgeschrieben wird. Zur datenschutzrechtlichen Verbindlichkeit benötigen diese SLAs der Anerkennung einer zuständigen Aufsichtsbehörde, um ein angemessenes Datenschutzniveau länderübergreifend gewährleisten zu können.

- Betreiber von Cloud Computing haben ihren Anwendern gegenüber im Rahmen ihrer **Aufklärungspflicht** darzulegen, wofür die angebotenen Leistungen geeignet sind und welche Risiken diese (z.B. durch ungewollte Einrichtung verdeckter Kanäle) ggf. hervorrufen. Ein IT-Verbund ist lediglich so sicher wie sein schwächstes Glied in der Kette. Daher sollten Anwender in die Lage versetzt werden, festzustellen, welchen Verwundbarkeiten sie ggf. durch die Nutzung des angebotenen Cloud Computings ausgesetzt sind.
- Für die Betroffenen ist ein besonderes **Auskunftsrecht** vorzusehen, mit dem diese erfahren dürfen, von welchem Betreiber welche Datenarten via Cloud Computing im Auftrag des Anwenders automatisiert verarbeitet werden, ob für diese Form des Cloud Computings beim Betreiber ein Zertifikat zur Einhaltung eines ausreichenden Datenschutz– und Sicherheitskonzepts vorliegt und ob zwischen Anwender und Betreiber von einer zuständigen Aufsichtsbehörde anerkannte SLAs getroffen wurden. Auf diese Weise kann der Grad der Vertrauenswürdigkeit in Cloud Computing deutlich erhöht werden.
- Zum Ausgleich für diese zusätzlichen Verpflichtungen soll das betreffende Cloud Computing trotz der fehlenden Weisungsbefugnis und unpräzisen Beschreibung detaillierter Vorgehensweisen als **Auftragsdatenverarbeitung** (unabhängig vom Erbringungsort!) qualifiziert werden dürfen. Faktisch sind viele Formen angebotener Cloud Computing Services dafür sogar prädestiniert.

Eine globale, allgegenwärtige und technikübergreifende Informationsverarbeitung benötigt eine globale und systemadäquate rechtliche Ausgestaltung. Die bisherigen Rechtsvorschriften bilden dies im Falle von Cloud Computing bisher nicht vollumfänglich ab. Zielvorgaben sind dabei zielführender als Detailregelungen. Obige Vorschläge sollen daher insbesondere auch der Fortentwicklung der EU-Datenschutz-Richtlinie und deren nationaler Umsetzung dienen.