

Adrian Rufener*

Cloud Computing

Stichworte: Cloud Computing, Sicherheit, Datenschutz, Outsourcing

Einführung

Immer mehr Unternehmer, Behörden und Institutionen lagern ihre bisher typischerweise intern erledigten Datenverarbeitungen an externe Unternehmen aus¹ und setzen dafür auf «Cloud Computing». Cloud Computing² ist ein Begriff aus der Informationstechnologie³. Er bedeutet, vereinfacht gesagt, dass Software, Speicherkapazitäten oder Rechnerleistung über ein Netzwerk, z.B. das Internet, oder innerhalb eines Virtual Private Network⁴ bedarfsorientiert bezogen, d.h. gemietet werden. Die ICT-Landschaft⁵ steht nicht mehr im Eigentum des Unternehmens oder der Behörde und wird nicht mehr von diesem bzw. dieser selbst betrieben, sondern von einem oder mehreren Cloud-Service-Anbietern als Dienstleistung⁶ gemietet. Die Anwendungen und Daten befinden sich nicht mehr im eigenen Netzwerk, sondern in der Cloud. Der Zugang zu Datenservices und Infrastruktur, die in der Cloud zur Verfügung gestellt werden, erfolgt mittels Fernzugriff⁷. Die verschiedenen Varianten zu Cloud Computing unterscheiden sich in Bezug auf Organisationsform und Servicemodell teilweise erheblich. Es werden drei Typen von Servicemodellen unterschieden: Infrastructure as a Service⁸, Platform as a Service⁹ sowie Software as a Service¹⁰.

Infrastructure as a Service

Der Cloud Service beinhaltet über das Internet genutzte ICT-Infrastruktur wie Platz, Klima, Netzwerk, Server, Speicher bis zum Betriebssystem und dem zugehörigen Betriebsmonitoring. Die Kunden können jeweils individuelle Middleware- und/oder Anwendungsumgebungen frei implementieren oder über das Internet nutzen.

Platform as a Service¹¹

Diese Dienstleistung ermöglicht es dem Kunden, seine benötigte Middleware¹² on demand zusammenzustellen. Die Nutzer können auf der Plattform für ihre Kunden oder ihre eigenen Bedürf-

nisse Anwendungssoftware entwickeln, betreiben und über das Internet nutzen.

Software as a Service¹³

Diese angebotene Dienstleistung bringt dem Anwender wohl den grössten Nutzen. Die Anwendungssoftware ist on demand abrufbar und kann von verschiedenen Standorten aus und von mehreren Usern gleichzeitig über das Internet genutzt werden.

Gründe für den Einsatz von Cloud Computing

Die Gründe für den Einsatz von Cloud Computing sind unterschiedlich. Sei es, dass der Service nur in der Cloud zur Verfügung steht¹⁴ oder aber, dass der Aufbau bzw. die Weiterführung einer eigenen Serverumgebung aus wirtschaftlichen Gründen¹⁵ nicht (mehr) von Vorteil ist.

Compliance/Risiken bei den Nutzern von Cloud Computing¹⁶

Beim Einsatz von Cloud Computing stellen sich verschiedene Compliance-Fragen. Da der Cloud-Anbieter meist nicht gleich wie ein Outsourcing-Dienstleister kontrolliert werden kann, fragt sich, ob die Bearbeitung und Speicherung von Daten bei externen Cloud-Anbietern rechtlich zulässig ist. Dies umso mehr, wenn sich der Dienstleister im Ausland befindet oder zumindest der Zugriff auf die Daten aus dem Ausland möglich ist.

Wer Cloud Services einsetzen und nutzen will, hat die für ihn geltenden gesetzlichen und branchenspezifischen Vorschriften¹⁷ einzuhalten. Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte¹⁸ bringt es in seinen Erläuterungen zum Cloud Computing vom Oktober 2011¹⁹ auf den Punkt: «Unternehmer und Behörden, die solche Dienste in Anspruch nehmen, sind sich oft zu wenig bewusst, dass die primäre Pflicht zur Einhaltung der Datenschutzregeln zunächst einmal bei ihnen selbst liegt und nicht beim Anbieter, der die Daten auf einem Cloud-Server speichert oder in der Cloud bearbeitet.»

Im Wesentlichen stellen sich die folgenden Fragen:

- Welche Daten sollen ausgelagert werden?
- Dürfen die Daten ausgelagert werden?

* Rechtsanwalt, St. Gallen.

1 Outsourcing.

2 Rechnen in der Wolke.

3 IT.

4 VPN.

5 Z.B. Rechenzentrum, Datenspeicher, Mail- oder Kooperationssoftware, Entwicklungsumgebungen oder Spezialsoftware, wie Customer Relationship Management (CRM).

6 Service.

7 Remote Access.

8 IaaS.

9 PaaS.

10 SaaS.

11 PaaS; PaaS baut auf IaaS auf.

12 Tool, Datenbanken etc.

13 SaaS; SaaS baut auf PaaS und IaaS auf.

14 iCloud von Apple zum Aufsuchen eines verloren gegangenen iPhones; E-Mail-Dienst bei einem Provider wie Bluewin etc.

15 Beschaffung, Wartung, Betrieb etc.

16 Zum Thema: Leitfaden zum Cloud Computing der Euro Cloud Swiss; im Internet abrufbar unter www.eurocloudswiss.ch.

17 Standesregeln.

18 EDÖB.

19 Im Internet abrufbar unter www.edoeb.admin.ch.

- Dürfen die Daten ins Ausland ausgelagert werden?
- Sind die Daten sicher und jederzeit verfügbar?
- Sind die Daten auch sofort verfügbar, wenn der Provider in Konkurs fällt?
- Ist im Konkurs des Providers sichergestellt, dass keine unberechtigten Dritten Einsicht bzw. Zugriff in bzw. zu den Daten erhalten?

Die sich stellenden rechtlichen Fragen des Cloud Computing sind ähnlich gelagert wie jene bei anderen Outsourcing-Projekten. Rechtliche Rahmenbedingungen können ein Cloud-Projekt stark beeinflussen bzw. verunmöglichen, obwohl der Nutzen einer Auslagerung in die Cloud möglicherweise gross wäre. Im Wesentlichen ist sicherzustellen, dass:

- es nicht zu einem Kontrollverlust über die Daten kommt;
- der Datenschutz und die Datensicherheit gewährleistet ist;
- ausländische Behörden keinen Zugriff auf die Daten haben;
- es nicht zu einer Abhängigkeit gegenüber dem Provider kommt, d.h. dass sichergestellt ist, dass auch im Falle eines Providerwechsels die Daten auf eine neue Plattform migriert werden können;

- die Daten auch im Konkurs des Anbieters sofort verfügbar sind und nicht von unberechtigten Dritten eingesehen werden können;
- das Anwaltsgeheimnis gewahrt bleibt.

In diesem Sinne hat sich auch der Conseil des barreaux européens (CCBE)²⁰ gegenüber der Europäischen Kommission vernehmen lassen und gefordert, dass europaweit Standards zum Einsatz von Cloud Computing definiert werden.

Wie weiter?

Cloud Computing ist nicht des Teufels; ohne klare Regelungen und die notwendigen Vereinbarungen mit dem Provider²¹ stellt Cloud Computing jedoch einen Verstoß gegen geltendes Recht und die Standesregeln dar.

20 CCBE; www.ccbe.eu

21 Geheimhaltungsvereinbarung, Regelung über die Datensicherheit, Datenherausgabe etc.

Adrian Rufener*

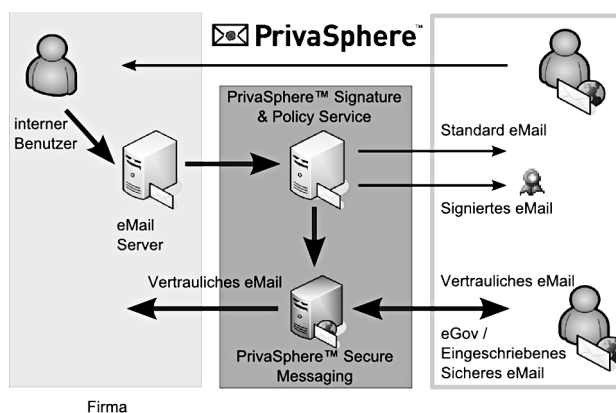
«Durchklick» – Integration der Zustellplattform in die E-Mail-Infrastruktur

Stichworte: Durchklick, Zustellplattform, Integration in E-Mail-Infrastruktur

In der Anwaltsrevue 4/2009, S. 191 ff., wurde ausführlich dargestellt, wie der Mailverkehr abgesichert werden kann, namentlich auch unter Verwendung der Zustellplattformen von PrivaSphere und bzw. oder IncaMail.

Seit dem 1. Januar 2011 können Eingaben der Parteien an Gerichte, an die Staatsanwaltschaft sowie an die SchKG-Behörden in elektronischer Form eingereicht werden (Art. 130 Abs. 1 ZPO, Art. 110 Abs. 2 StPO und Art. 33a SchKG). Neben anderen Formvorschriften ist erforderlich, dass die Eingabe über eine vom Bund zugelassene Zustellplattform eingereicht wird.

Die vom Bund zum elektronischen Rechtsverkehr zugelassenen Zustellplattformen ermöglichen es, die eigene Mail-Domain an die Zustellplattform anzubinden. Im Falle einer Domainanbindung wird der gesamte ausgehende Mailverkehr ab dem firmeninternen Mailserver über eine geschützte Verbindung¹ auf die Zustellplattform gesandt. Je nach «Codierung»² versendet in der Folge die Zustellplattform das Mail als ungeschütztes, signiertes, sicheres, eingeschriebenes oder eGov-Mail. Für den Anwender



hat die Domainanbindung erhebliche Vorteile, kann er doch in seinem Mailprogramm mit dem Anklicken entsprechender Schaltflächen bestimmen, wie das Mail von der Zustellplattform weitergeleitet werden soll. Über die Zustellplattform eingehender Mailverkehr wird dem Empfänger über die verschlüsselte Verbindung direkt in seinen Mailclient zugestellt. Handelt es sich um eingeschriebene bzw. eGov-Sendungen, erhält der Benutzer eine Mail mit einem eingebetteten Link, da für ihn eine «Abholungs-

* Rechtsanwalt, St. Gallen.

1 TLS-Verschlüsselung mittels SSL-Zertifikat.

2 Mittels Anklicken einer Schaltfläche im Mailclient.