Cloud-Lösungen

Datenschutz nicht vergessen

[24.02.2016] Die Datenverarbeitung in der Cloud hat handfeste Vorteile. Bei der Auswahl des Dienstleisters sollte geprüft werden, ob der Datenschutz berücksichtigt ist und Kriterien der IT-Sicherheit eingehalten werden.

Software in die Cloud zu verlagern, ist technisch kein Problem mehr. Bei Online-Speichern dient die Cloud quasi als Festplatte im Internet, Cloud Software geht noch einen Schritt weiter. Hier werden nicht nur die Daten in der Cloud gespeichert, sondern auch die Anwendungsprogramme. Sie werden beim Cloud-Dienstleister installiert und in dessen Rechenzentrum ausgeführt. Eine Cloud-Lösung beispielsweise für Bibliotheken bietet das Unternehmen datronic IT-Systeme an. Diese Art der Datenverarbeitung hat handfeste Vorteile. Zum Beispiel muss sich der Kunde nicht mehr um Wartung, Backups oder das Einspielen von Updates kümmern. Oft können auch die finanziellen und personellen Mittel nicht aufgebracht werden oder das nötige Know-how fehlt, um in Eigenregie die hochkomplexen Anforderungen an die IT-Sicherheit sowie Hard- und Software zu erfüllen. Entscheidet sich ein Kunde für eine Cloud-Lösung, obliegen die Anschaffung leistungsfähiger Hardware sowie die Sorge für die notwendigen Maßnahmen zur Verfügbarkeit und zur Sicherheit dem Cloud-Dienstleister. Er kümmert sich um alle Komponenten und sorgt dafür, dass alles nach neuestem Stand der Technik umgesetzt wird. Ein weiterer Vorteil: Der Nutzer kann von überall auf die Daten und Dienste zugreifen. Beim Cloud Computing gibt der Kunde ein erhebliches Maß an Kontrolle über seine geschäftlichen und privaten Daten sowie Anwendungen an den Dienstleister ab. Hier gilt es, die Vorteile mit dem Risiko abzuwägen. Es sollte überprüft werden, ob der Grad der Ausfallsicherheit beim Cloud-Dienstleister ausreichend hoch ist. Denn wenn die Internet-Leitung ausfällt, kann der Kunde nicht auf seine Daten zugreifen. Die Maßnahmen des Cloud-Dienstleisters zum Schutz vor Viren und Hackern sind ebenso zu hinterfragen.

Kriterien erfüllt?

Ferner sollten die Daten im Internet verschlüsselt übertragen werden und die Kundendaten vor dem unberechtigten Zugriff Dritter geschützt sein. Auch ist zu überprüfen, ob weitere Dienstleister in die Cloud-Lösung involviert sind. Die Erreichbarkeit des Supports gehört ebenfalls zur Risikoabwägung: Ist dessen Erreichbarkeit zu den Geschäftszeiten ausreichend oder ist ein 24-Stunden-Support notwendig? Nicht zuletzt sind passende Schnittstellen zur Rückübertragung oder zur Löschung der Daten bei Beendigung des Vertragsverhältnisses zu bedenken. Ein guter Cloud-Dienstleister beantwortet diese Fragen umfassend und legt seine Schutzmaßnahmen transparent dar. In der Praxis können Cloud-Dienstleister meist eine höhere Ausfallsicherheit oder ein deutlich höheres Sicherheitsniveau bieten, als es beispielsweise kleineren Bibliotheken normalerweise zur Verfügung steht. Datenschutz basiert nicht nur auf IT-Sicherheit. Sind bei der Verarbeitung in der Cloud personenbezogene Daten betroffen, müssen die Regeln des Bundesdatenschutzgesetzes (BDSG) und der Landesdatenschutzgesetze beachtet werden. Beispielsweise muss der Cloud-Dienstleister seine Mitarbeiter auf das Datengeheimnis verpflichten. Es sind schriftliche Vereinbarungen zu treffen, wie der Dienstleister mit den Kundendaten umgehen soll und darf. Die Daten dürfen auch nicht ohne weiteres in Drittländern außerhalb der EU gespeichert werden. Idealerweise sollte der Speicher- und Verarbeitungsort in Deutschland sein. Sind personenbezogene Daten betroffen, können deutsche Institutionen die Cloud-Angebote mit Datenverarbeitung in Drittländern wie den USA, Indien oder China, meist gar nicht oder nur sehr aufwendig datenschutzgerecht nutzen.

Schriftliche Vereinbarung

Diese und andere Vorgaben sind schriftlich in der Vereinbarung zur Auftragsdatenverarbeitung (ADV) festzuhalten. Welche Inhalte die Vereinbarung regeln muss, legt der Gesetzgeber im §11 BDSG und den entsprechenden Landesgesetzen fest. Die Verantwortung, eine passende ADV-Vereinbarung abzuschließen, liegt beim Cloud-Kunden als Auftraggeber. Fehlt eine solche und es werden dennoch personenbezogene Daten in die Cloud verlagert, kann das ein Bußgeld durch die Datenschutzaufsichtsbehörde für den Auftraggeber nach sich ziehen. Es lohnt sich überdies bei Cloud-Lösungen beim Dienstleister nach einer passenden ADV-Vereinbarung zu fragen. Gut vorbereitete Anbieter haben auf ihre Dienstleistung zugeschnittene Vereinbarungen vorformuliert. Der Kunde sollte dann prüfen, ob die darin enthaltenen Vorgaben seinen Ansprüchen genügen. Das Unternehmen datronic kommt den Anforderungen der IT-Sicherheit und des Datenschutzes nach, indem es für seine Cloud-Lösungen ein Server-Zentrum in Deutschland garantiert. Die Sicherheit der Kundendaten bei der Übertragung wird unter anderem durch die Verschlüsselung und den Einsatz von Firewalls gewährleistet. Empfehlenswert ist darüber hinaus, dass der Cloud-Dienstleister unabhängig von einer gesetzlichen Pflicht einen Datenschutzbeauftragten bestellt hat. Da er unabhängig agiert und im Unternehmen die Einhaltung des Datenschutzes kotrolliert, bedeutet der Datenschutzbeauftragte eine zusätzliche Kontrollinstanz beim Dienstleister vor Ort. Ebenso ist er Ansprechpartner für die Kunden, wenn sie Fragen zur datenschutzkonformen Verarbeitung personenbezogener Daten haben.

()

Dieser Beitrag ist in der Februar-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, BDSG, ADV