

Pro & Contra

Ist die Cloud wirklich sicher?

Cloud Computing ist das Topthema der IT-Branche im Moment. Wer daran bislang noch zweifelte, brauchte sich nur auf der vergangenen CeBIT umzusehen. Doch fragt sich inzwischen so mancher IT-Verantwortliche: Ist die Sache denn auch wirklich sicher?



Dr. Walter Kirchmann, Vorsitzender der Geschäftsleitung bei Finanz Informatik Technologie Service (FI-TS).
geschaeftsfuehrung@f-i-ts.de



Das Thema Cloud Computing wird derzeit viel diskutiert. Die IT-Experten sind begeistert. Die Unternehmen sind noch etwas zwiespalten. Die positiven Fakten liegen auf der Hand: erhöhte Flexibilität, schnelle und einfache Anpassung individueller IT-Kapazitäten und Kosteneinsparungen. Mit Vorteilen sind inhärent auch Nachteile verbunden – das liegt in der Natur der Sache. Doch wenn Finanzinstitute einige Eckpunkte beachten, können auch sie von der Cloud profitieren. Für die Finanzbranche eignet sich nicht jede Form des Cloud Computings. **Banken sollten auf eine Branchencloud setzen, die speziell auf die hohen Anforderungen des Finanzsektors zugeschnitten ist, und auf einen IT-Servicepartner vertrauen, der unabhängige Zertifizierungen und einschlägige Branchenerfahrung vorweisen kann.** Zudem muss der Fokus beim Cloud Computing ganz klar auf den Aspekten Sicherheit und Vertrauen liegen. Und dabei geht es nicht nur darum, ob die Cloud selbst und die darin angebotenen Services sicher sind. Vielmehr müssen die rechtlichen Rahmenbedingungen und die Sicherheitsanforderungen erfüllt sein. Es gilt zu klären: Wo liegen die Unternehmensdaten physisch – im In- oder Ausland? Wo liegen die personenbezogenen Daten? Wo die Bilanz- und steuerrechtlich relevanten Daten? Wer ist der Vertragspartner? Kann er die rechtlichen Vorgaben des Bankensektors einhalten? Greift er seinerseits auf Subunternehmen zu, die letztlich nicht mehr greifbar sind? Zudem sollten Finanzinstitute zunächst erste Erfahrungen sammeln und das Konzept Cloud Computing ausprobieren. Das können sie durch die Verlagerung einzelner, nicht geschäftskritischer Anwendungen oder von Test- und Entwicklungsumgebungen in die Cloud. So können sie konkrete Erkenntnisse sammeln, bei Bedarf interne Prozesse anpassen und Maßnahmen für die Integration von Cloudanwendungen in die herkömmliche Unternehmens-IT angehen. Bei der Auswahl des richtigen Cloud-Servicepartners liefern Merkmale wie „made in Germany“, Herstellerzertifizierungen wie „SAP Cloud Service Partner“ sowie unabhängige ISO-Zertifizierungen zum Beispiel nach ISO 27001 wichtige Anhaltspunkte. ■



„Pack's in die Cloud und alle Probleme sind gelöst!“ – die Public Cloud als Rundumsorglos-Paket? Jederzeitige Verfügbarkeit ist ein Versprechen von Cloudanbietern. Doch dies wird nicht immer eingelöst, wie die Fälle Sidekick (2009) oder Flickr (2011) zeigen, in denen Daten plötzlich nicht mehr auffindbar waren. Datensicherheit bedeutet ohnehin mehr: **Kann der Cloudanbieter garantieren, dass kein Unbefugter auf die dort gespeicherten Daten zugreift? Nein.** Neue Angriffe auf die Virtualisierungssoftware, zum Beispiel durch Kompromittieren des Hypervisors, ermöglichen den Zugriff von Cloudnutzern auf die Daten anderer. Natürlich kann die Gefahr auch vom Cloudanbieter selbst oder seinen Mitarbeitern ausgehen – rein technisch ist ein Zugriff nämlich möglich. Außerdem können Cloudanbieter im Einklang mit ihrer heimischen Jurisdiktion rechtlich verpflichtet werden, den Zugriff Dritter auf die Daten zu erlauben: zur Strafverfolgung, zur Fahndung nach Urheberrechtsverstößen oder gar zur Wirtschaftsspionage. Einige Cloudanbieter behalten sich vor, auf Daten der Kunden zuzugreifen und sogar „anstößige“ Inhalte zu löschen oder Accounts zu sperren. Anwender sollten sich überlegen, ob sie beim Cloudangebot auf einer „Regionalgarantie“, das heißt Beschränkungen des Computing auf den nationalen oder europäischen Rechtsraum, bestehen, was ohnehin für die Verarbeitung personenbezogener Daten geboten sein kann. Zudem sollten sie ihre Daten verschlüsseln, und zwar so, dass sie die Kontrolle über das Schlüsselmanagement behalten. Mangelnde Transparenz für die Anwender ist ein weiteres Problem, denn Aussagen der Cloudanbieter über Sicherheitsgarantien und verbleibende Risiken bleiben oft wolkig. Es ist jedoch Bewegung im Cloudmarkt: Mit mehr Datensicherheit sowohl in der Cloud als auch auf Seiten der Anwender kann sich Cloud Computing zu einem wichtigen Element in vielen Anwendungen mausern. „Rundum sorglos“ geht aber nicht – die Verantwortung für die Daten lässt sich nicht an die Cloudanbieter wegdelegieren. ■



Marit Hansen ist Diplom-Informatikerin und seit 2008 stellvertretende Datenschutzbeauftragte des Landes Schleswig-Holstein. Sie setzt sich für datenschutzfördernde Technik ein, unter anderem im EU-Projekt „TClouds – Trustworthy Clouds“. marit.hansen@datenschutzzentrum.de