

# Daten in der Cloud

## Sensible Daten bei Online-Speicherdiensten immer selbst sichern

### Was ist eine Cloud?

Bei der Cloud (Englisch für Wolke) handelt es sich im Regelfall um ein IT-System, welches bestimmte Ressourcen von Rechnern bei Bedarf jederzeit und überall zur Verfügung stellt. Zu diesen Ressourcen zählen neben dem Speicherplatz etwa auch Programme und Zusatzanwendungen, die ein effizientes Arbeiten ermöglichen. Kennzeichnend für die Cloud ist außerdem der Aspekt, dass die Ressourcen variabel und ohne großen Aufwand hinzugebucht oder abgewählt werden können. Durch die Neuheit der Cloud variiert diese definierte Grundlage jedoch gegenwärtig noch geringfügig.

### Was kann ich mit der Cloud machen?

Die Einsatzmöglichkeiten der Cloud sind vielfältig und lassen sich nicht abschließend aufzählen. Grundsätzlich ist die Cloud für Privatpersonen als auch Unternehmen geeignet, um große Datenmengen zentral zu speichern, verfügbar zu machen und um bestimmte Anwendungen standortunabhängig zum Arbeiten zur Verfügung zu stellen. Die Cloud eignet sich also als überall und jederzeit verfügbarer PC, der sämtliche Aufgaben zentral erledigt und lediglich das Ergebnis überträgt und bereitstellt.

### Kann ich meine lokalen Dateien in der Cloud sichern?

Ja, die Cloud dürfen Sie sich wie ein gigantisches Rechenzentrum vorstellen. Dieses Rechenzentrum ist jedoch nicht dazu da, Webseiten oder dergleichen zu hosten. Die einzige Aufgabe besteht darin Ihre Inhalte sicher zu lagern und bei Bedarf bereitzustellen. Zahlreiche Cloud-Dienste bieten einen Synchronisierungsservice an. Dabei werden die Daten auf Ihrem PC mit denen in Ihrem Cloud-Account regelmäßig abgeglichen, sodass Sie online immer die aktuellste Version zur Verfügung haben. Egal, wo Sie sich gerade befinden.

### Kann die Cloud mit allen Betriebssystemen eingesetzt werden?

Ja, Sie können die Cloud mit jedem Betriebssystem nutzen. Egal, ob Sie Windows, Mac OS X oder Linux nutzen. Streng genommen ist die Cloud nämlich für sich genommen bereits eine Art Betriebssystem.

Zum Betrieb einer Cloud setzen Rechenzentren Software ein, die Ihnen überhaupt erst den Zugang zur Cloud oder Anwendungen möglich macht. Ihr PC oder Mac funktioniert also nur noch als "Darstellungsmedium". Die Berechnungen sowie alle weiteren Arbeitsschritte finden in der Cloud statt und belasten somit Ihren Computer nicht. Dadurch ist die Cloud vor allem für schwächere PCs sehr geeignet.

### Worauf muss ich bei der Auswahl eines Cloud-Anbieters achten?

Zuerst sollten Sie unbedingt mehrere Anbieter in die engere Auswahl nehmen, um vergleichen zu können. Eine Übersicht möglicher Anbieter finden Sie im Netz.

Erst danach sollten Sie sich um Detailfragen kümmern. Bei der Auswahl ist natürlich wichtig, welche Preise die einzelnen Anbieter präsentieren. Darüber hinaus sollten Sie aber auch Detailfragen klären.

Wie hoch ist die Verfügbarkeit des Anbieters? Meist wird dieser Wert in Prozent angegeben. Wer haftet bei einem kostspieligen Fehler in welchem Umfang? Alles Fragen, die Ihre Auswahl beeinflussen sollten.

## Sicherheit

### Ist die Cloud überhaupt sicher?

Grundsätzlich setzt die Mehrheit der Cloud-Anbieter auf eine Verschlüsselung. Diese ist jedoch mitunter mangelhaft, wie das Fraunhofer Institut herausgefunden hat.

Sicherheit ist also wie immer relativ. Achten Sie im Vorfeld also darauf, welche Anbieter besonders sicher sind. Nur so sind auch Ihre Daten wirklich in Sicherheit.

### Welche Sicherheitssysteme kommen bei der Cloud zum Einsatz?

Hinsichtlich der Sicherheit kommen bei vielen Cloud-Anbietern verschiedene Dienste zum Einsatz.

Gute Cloud-Anbieter verschlüsseln nicht nur die Daten auf deren Servern, sondern auch bereits während der Übertragung. Dadurch sind sie besonders geschützt. Bevorzugt kommt hierbei ein Verschlüsselungsalgorithmus wie AES zum Einsatz. Einige Anbieter nutzen aber auch eigene, mangelhafte Lösungen.

### Ist die Datenübertragung auch gesichert?

Diverse Cloud-Anbieter legen besonderen Wert darauf, dass auch bereits die Übertragung der Daten von den Servern zu Ihnen und umgekehrt verschlüsselt ist.

Dabei kommt - wie erwähnt - häufig ein hochwertiger Algorithmus zum Einsatz, der als unknackbar gilt.

Vor allem wenn Sie sensible Daten übertragen, sollten Sie darauf achten, dass Ihr Anbieter eine verschlüsselte Datenübertragung ermöglicht

### Wie steht es um den Datenschutz allgemein?

Da Sie nur Ihre persönlichen Daten an die Cloud abgeben, geraten Sie mit keinem Gesetz in Konflikt. Dennoch sollten Sie detailliert prüfen, wie der Cloud-Anbieter mit dem Datenschutz verfährt.

**Solange die Anbieter in Deutschland sind, können Sie beruhigt sein. Für diese Anbieter gilt deutsches Recht.** Schwieriger wird es, wenn der Anbieter im Ausland sitzt. Hier sollten Sie sich vorab informieren, wie der Anbieter das Thema behandelt.

### Was ist, wenn der Anbieter in Insolvenz geht?

Das Horror-Szenario eines jeden Cloud-Kunden: Der Anbieter geht ruckartig in die Insolvenz. Was beunruhigend klingt, ist beim richtigen Anbieter kein echtes Problem.

Die Insolvenz führt nämlich nicht zum Löschen der Server. Im günstigsten Fall werden - je nach Vertrag - Ihre Daten schnell zu einem anderen Anbieter umgezogen. Im ungünstigsten Fall müssen Sie diesen Service-Schritt selbst vornehmen.

Ein Verlust Ihrer Daten ist jedoch äußerst unwahrscheinlich. Riskanter ist hier, dass im Zuge der Insolvenz Dritte Zugriff auf die Server erhalten. Bei guten Cloud-Anbieter spielt dies aber keine Rolle, da Ihre Daten dort verschlüsselt sind.

### Was ist bei einem Hackerangriff?

Ein heikles Thema, welches in der Vergangenheit rege diskutiert wurde. Cloud-Speicher sind natürlich für Hacker ein begehrtes Ziel. Im Gegensatz zu einer eigenen Lösung werden die Systeme jedoch von Experten überwacht.

Im Falle eines Angriffs ist somit kompetente Hilfe direkt zur Stelle. Diese kann gegen einen Großteil der Angriffe Maßnahmen ergreifen. Alles was darüber hinausgeht, wirft wieder die Frage der Datensicherheit auf. Deshalb sollten Sie auf Cloud-Anbieter achten, die Ihre Daten verschlüsselt lagern.

### **Kann ich auch urheberrechtlich geschützte Dateien hochladen?**

Grundsätzlich haben Sie die Möglichkeit, auch urheberrechtlich geschützte Dateien in Ihre Cloud zu laden. Hierbei müssen Sie jedoch die Nutzungsbedingungen des Dienstes beachten. Darüber hinaus dürfen Sie die Datei natürlich nicht öffentlich zugänglich machen.

### **Wer kann auf meine Dokumente zugreifen / Kann ich den Zugriff individuell regeln?**

Der Zugriff auf Dateien und Dokumente innerhalb der Cloud lässt sich individuell regeln. So stellen Sie sicher, dass nur die Personen Zugriff auf eine Datei erlangen, die dazu berechtigt sind.

### **Dropbox →ältester Anbieter (seit 2007)**

Für wen eignet sich der Cloud-Anbieter Dropbox?

Dropbox gehört mit zu den bekanntesten Cloud-Anbietern für Privatkunden und hat sich auch für diese Zielgruppe aufgestellt. Wenn Sie erste Schritte in der Cloud unternehmen wollen, ist Dropbox eine gute Wahl. Der Dienst bietet Ihnen nämlich auch eine geringe Menge an kostenlosem Speicherplatz. Vor allem unerfahrene Nutzer können hier erst mal ausgiebig testen

### **Welche Pakete gibt es bei Dropbox?**

Dropbox bietet drei unterschiedliche Paketstufen an. Hierzu zählen Kostenlos, Pro sowie Team. Diese Stufen sind wiederum mit unterschiedlichen Speicherplatzmengen bestückt.

**Kostenlos:** Hier erhalten Sie zu Beginn 2 Gigabyte Speicherplatz. Sie können insgesamt bis zu 18 Gigabyte erhalten. Dafür müssen Sie Dropbox lediglich an Freunde empfehlen.

### **Was ist „Cloud-Computing“ technisch und rechtlich?**

Bei „Cloud-Verträgen“ handelt es sich rechtlich gesehen **nicht** um einen Vertrag, der sich einem konkreten Vertragstypus des BGB zuordnen lässt. Hier muss bei jedem Anbieter im Einzelfall geprüft werden, wie das konkrete Nutzungsverhältnis vertraglich ausgestaltet wurde. In aller Regel wird es sich um einen so genannten gemischten Vertrag handeln, der - je nachdem, welche Leistungen vom Anbieter erbracht werden - schwerpunktmäßig als Mietvertrag, Werkvertrag oder Dienstvertrag behandelt wird.

Wird beispielsweise Speicher zur Verfügung gestellt, der gegen ein kostenpflichtiges Upgrade auch noch erweitert werden kann (z.B. wie im Fall von Dropbox), so handelt es sich schwerpunktmäßig um einen Vertrag mit Mietcharakter nach den §§ 535ff. BGB. Je nachdem, wie der Nutzungsvertrag eingeordnet wird, unterscheiden sich dann die Rechte und Pflichten des Nutzers, etwa bei auftretenden Mängeln.

### **Cloud-Anbieter und der Datenschutz: Wie sicher sind Ihre Daten?**

Das Deutsche Datenschutzrecht findet auf „Cloud-Dienste“ grundsätzlich dann Anwendung, wenn es sich bei den in der Cloud gespeicherten Daten um sogenannte „personenbezogene Daten“ gem. § 3 Nr. 1 BDSG handelt. Dies sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“, also die Daten eines Menschen.

Gerade nicht vom deutschen Datenschutzrecht erfasst sind damit Daten über juristische Personen (wie GmbH, AG, etc.) sowie anonyme Daten. Etwas anderes gilt jedoch für pseudonymisierte Daten nach § 3 Nr. 6a BDSG, bei denen zwar kein unmittelbarer Personenbezug besteht, dieser Personenbezug aber hergestellt werden kann (z.B. wenn eine Person eine bestimmte Ziffer trägt und sie über die Ziffer identifiziert werden kann). Je nachdem, ob Dateien in der Cloud Personenbezug aufweisen oder nicht, sind diese folglich vom Schutz des Datenschutzgesetzes erfasst oder nicht.

Bei der Frage, welches Datenschutzrecht Anwendung findet, ist ein genauere Blick auf Anbieter und Nutzer des Cloud-Dienstes notwendig. Befindet sich der Cloud-Anbieter innerhalb der EU und hat ein Cloud-Kunde seinen Wohnsitz in Deutschland, kann in der Regel davon ausgegangen werden, dass deutsches Datenschutzrecht Anwendung findet. Nach der Europäischen Datenschutzrichtlinie (RL 95/46/EG) stellt eine grenzüberschreitende Datenverarbeitung innerhalb der EU nämlich kein rechtliches Hindernis mehr dar (vgl. Art. 1 Abs. 2 EU-DSRL)- Deutsches Datenschutzrecht ist also immer anwendbar, wenn personenbezogene Daten einer Person mit Wohnsitz in Deutschland von einem Cloud-Anbieter mit Niederlassung in der EU verarbeitet werden.

### **Datenschutzprobleme bei Cloud-Anbietern außerhalb Europas?**

Insbesondere bei außer-europäischen Anbietern von Cloud-Diensten (z.B. Google-Drive) bestehen aus rechtlicher Sicht o Bedenken. Da diese Länder oft über ein Datenschutzniveau verfügen, das nicht den europäischen Gesetzen entspricht, werden viele der dort geltenden Regelungen von europäischen Datenschützern oft als unzulässig eingestuft. Eine Pauschallösung für die Behandlung der datenschutzrechtlichen Probleme im Zusammenhang mit ausländischen Cloud-Anbietern gibt es aber bisher nicht. Grundsätzlich wird die Übermittlung von Daten per Cloud an einen ausländischen Anbieter als unzulässig angesehen, da es hierfür keine datenschutzrechtliche Legitimation gibt und in der Regel **kein angemessenes Datenschutzniveau besteht.** Will man dennoch einen außereuropäischen Anbieter für einen Cloud-Dienst nutzen, empfiehlt es sich, das Übermitteln von personenbezogenen Daten in die Wolke zu vermeiden und ausschließlich nicht-personenbezogene Daten zu verwenden. Was den praktischen Nutzen der Dienste dann aber stark einschränkt.

### **Datenverlust und Hackerangriffe: Wann haftet der Cloud-Anbieter?**

Für Nutzer von Cloud-Speicher- Diensten stellt sich natürlich die Frage, ob der Anbieter haftet, wenn er einem Hackerangriff zum Opfer gefallen ist und die Daten des Nutzers betroffen sind. Entscheidend für einen zivilrechtlichen Schadensersatzanspruch bei gehackten Cloud-Daten ist also die Frage, ob dem Anbieter die Verletzung von Sorgfaltsanforderungen, also ein Verschulden (Vorsatz oder Fahrlässigkeit) nachgewiesen werden kann. Dies ist beispielsweise dann der Fall, wenn der Anbieter anerkannte Sicherheitsstandards nicht einhält und aufgrund dessen der Hacking-Angriff erst ermöglicht wurde.

Bisher ist jedoch kein Urteil eines Gerichts in der deutschen Rechtsprechung bekannt, dass einen solchen Schadensersatzanspruch gewährt hätte oder über einen solchen Fall zu entscheiden gehabt hätte.

### **Das Kleingedruckte: Die Nutzungsbedingungen der Cloud-Computing im Vergleich**

Entscheiden Sie sich dazu, Ihre Daten in die Cloud auszulagern, sollten Sie vor der Nutzung die Nutzungsbedingungen (AGB, terms and conditions) des jeweiligen Anbieters genau ansehen.

### *Nutzungsbedingungen von Dropbox*

**Auch im Fall von Dropbox bleibt der Nutzer alleiniger Inhaber der Rechte an den Dateien.** Trotzdem ist zu beachten, dass auch bei der Nutzung von Dropbox zumindest die für das Betreiben des Services notwendigen, eingeschränkten Rechte auf den Betreiber übertragen werden. Insbesondere sollen laut dem Betreiber des Cloud-Dienstes dadurch Backups auf rechtlicher Ebene abgedeckt werden.

### **DMCA-Richtlinien von Dropbox**

Dropbox, nachfolgend Dropbox genannt, respektiert die gewerblichen Schutzrechte Dritter und erwartet, dasselbe von seinen Nutzern. Gemäß dem Digital Millennium Copyright Act aus dem Jahr 1998, dessen Wortlaut Sie auf der Website des U.S. Copyright Office unter <http://www.copyright.gov/legislation/dmca.pdf> finden, reagiert Dropbox unverzüglich auf Mitteilungen über Urheberrechtsverletzungen bei der Nutzung des Dropbox-Dienstes bzw. der Dropbox-Website, nachfolgend Website genannt, wenn solche Rechtsverletzungen dem in der untenstehenden Beispielbenachrichtigung genannten Urheberrechtsbeauftragten von Dropbox gemeldet werden.

Wenn Sie Urheberrechtsinhaber sind oder bevollmächtigt sind, im Namen eines Urheberrechtsinhabers oder aufgrund eines ausschließlichen Rechts im Rahmen des Urheberrechts zu handeln, so teilen Sie uns bitte mutmaßliche Verstöße gegen Urheberrechte mit, die auf der Website oder über die Website begangen wurden, indem Sie die folgende DMCA-Benachrichtigung ausfüllen und dem zuständigen Urheberrechtsbeauftragten von Dropbox zukommen lassen. Nach Erhalt der unten beschriebenen Benachrichtigung ergreifen wir nach eigenem Ermessen die Maßnahmen, die wir für angemessen erachten. Eine solche Maßnahme kann beispielsweise das Entfernen des betroffenen Inhalts von der Website sein.

### **Nutzungsbedingungen von Google Drive**

Im Fall von Google Drive ist zunächst zu erwähnen, dass sich Google in Deutschland weit weniger Rechte einräumen lässt als es dies im englischsprachigen Raum macht. So stellt Google zunächst klar, dass der Nutzer alle Urheberrechte und bestehenden gewerblichen Schutzrechte behält. Allerdings wird durch die Einstellung von Daten in die Cloud Google ein unentgeltliches, nicht ausschließliches, aber weltweites und zeitlich unbegrenztes Recht eingeräumt, die Inhalte ausschließlich zum Zweck der Erbringung des Dienstes und in dem nötigen Umfang zu nutzen. So wird Google unter anderem das Recht eingeräumt, die Inhalte technisch zu vervielfältigen und die Daten öffentlich zugänglich zu machen, sofern eine öffentliche Zugänglichmachung durch den Nutzer beabsichtigt wird oder ausdrücklich eine solche Zugänglichmachung bestimmt wurde.

### **Nutzungsbedingungen von Microsoft SkyDrive**

Wie bei Dropbox erhebt auch Microsoft SkyDrive keine Eigentumsansprüche an den in die Cloud eingestellten Daten. Allerdings erklärt man sich durch Nutzung von SkyDrive ebenfalls damit einverstanden, dass Microsoft die Cloud-Inhalte „in dem für die Bereitstellung des Services erforderlichen Umfangs innerhalb des Services verwendet, ändert, kopiert, vertreibt und veröffentlicht, jedoch nur, um den Vertrag mit ihnen zu erfüllen.“

### **Fazit**

Bei allen Vorteilen aus technischer Sicht ist bei der Nutzung von Cloud-Computing Diensten aus rechtlicher Sicht Vorsicht geboten: durch die unbestimmten Formulierungen in den Nutzungsbedingungen wird den Cloud-Anbietern ein weiter Spielraum eingeräumt, die

eigenen Daten zu nutzen. **Aus datenschutzrechtlicher Sicht ist dabei vor allem Zurückhaltung geboten, wenn außereuropäische Cloud-Services genutzt werden sollen.** Will der Nutzer daher auf Nummer sicher gehen, so sollte die Devise heißen: so viele Daten wie nötig, so wenig Daten wie möglich.

### **LaCie Wuala Cloud**

Wuala ist ein sicherer Online-Speicher aus der Schweiz. Wuala ist das Schweizer Taschenmesser unter den Online-Speichern und deckt alle wichtigen Funktionen ab: Mit der Wuala Software können Sie Ihre Dateien sicher online ablegen, anderen zur Verfügung stellen, von überall darauf zugreifen, automatische Backups Ihrer Daten einrichten, oder auch ganze Ordner synchronisieren. Wuala bietet ein einzigartiges Sicherheitskonzept (client-side-encryption). Alle Daten werden direkt auf dem Computer des Benutzers verschlüsselt bevor sie hochgeladen werden. Das Kennwort verlässt den Computer nie. Ohne Berechtigung kann niemand – nicht einmal Wuala/LaCie als Anbieter – auf Ihre Dateien zugreifen. Wuala's Rechenzentren stehen in Europa (Schweiz, Deutschland, Frankreich).

Wuala existiert seit 2007 und wird von der LaCie AG in Zürich entwickelt und betrieben. Wuala schloss sich im März 2009 mit LaCie, dem französischen Hersteller von externen Festplatten, zusammen, um gemeinsam die Welt der Datenspeicherung voranzubringen.

### **Wuala sorgt für Datenschutz**

Wuala verfügt über die besten Datenschutz- und Sicherheitssysteme seiner Kategorie. Alle Dateien werden vor dem Versand in die Cloud auf Ihrem Computer verschlüsselt. Ihr Kennwort verlässt niemals Ihren Computer, sodass weder nicht berechtigte Benutzer noch Mitarbeiter von LaCie auf Ihre Daten zugreifen können.

### **Verschlüsselung auf Kundenseite**

Da die Verschlüsselung stattfindet, bevor die Dateien Ihren Computer verlassen, errichtet Wuala praktisch Schutzwand um Ihre in der Cloud gespeicherten Daten. Die Mitarbeiter von LaCie haben nur sehr beschränkten Zugriff auf Ihre Daten. Sie können ausschließlich sehen, wie viele Dateien Sie gespeichert haben und wie viel Speicherplatz diese belegen. Die Daten selbst sowie alle Metadaten (Ordernamen, Dateinamen, Kommentare, Bildvorschauen, etc.) sind verschlüsselt.

### **Preise**

Sie starten kostenlos mit 5 GB. Damit können Sie ca. 1500 Bilder oder 500 Musik-Dateien speichern. Aber das muss noch nicht alles sein - mit Wuala können Sie Ihren Speicherplatz beliebig erweitern.

### **Sicherheit & Privatsphäre**

Wuala sichert Ihre Daten und schützt Ihre Privatsphäre. Um Ihre Privatsphäre zu schützen, werden alle Dateien auf Ihrem Computer verschlüsselt, bevor sie hochgeladen werden. Beim Hochladen werden Ihre Dateien in kleine Stücke (Fragmente) aufgeteilt und an verschiedenen Orten abgelegt. Somit wird sichergestellt, dass Sie nie eine Datei verlieren. Ihr Passwort wird niemals übertragen, so dass niemand - nicht einmal wir als Anbieter - Zugriff auf Ihre Dateien hat.

In der Zeitschrift „Stiftung Warentest 8/2013 wurden die verschiedenen Cloud-Dienste getestet. Hierbei schnitt u.a. der Cloud-Dienst Google-Drive auf Grund seiner Datenschutzrechtlichen Bedenken mit „mangelhaft“ ab.

Die Cloud-Dienste.,DropBox, La-Cie Wuala, Sky Drive schnitten mit „befriedigend“ ab. Auch das WDR hat sich des Themas „Cloud-Dienste“ angenommen und kam zu selben Ergebnis, wie die Zeitschrift „Stiftung Warentest“

**Getestet wurden folgende Online-Speicherdienste:** Box, Deutsche Telekom Mediacenter, Dropbox, GMX Media-Center, Google Drive, LaCie Wuala, Microsoft SkyDrive, Mozy MozyHome, Pro Softnet, IDrive, Strato HiDrive Free, Sugar-Sync, Trend Micro Safe-Sync, Web.de Online-Speicher

### **Sensible Daten bei Online-Speicherdiensten immer selbst sichern**

Der Datenschutz bei Online-Speicherdienste hat im "test" nicht gut abgeschnitten. Online-Speicherdienste sind praktisch, aber angesichts von PRISM und Tempora sind sich viele Nutzer nicht mehr sicher, welchen Cloud-Diensten sie noch vertrauen können.

Grundsätzlich werden europäische Cloud-Dienste zwar als sicherer eingestuft als die US-Konkurrenz. Doch wenn es nicht nur um Urlaubsfotos, sondern um sensible Informationen wie die Korrespondenz mit der Krankenkasse oder dem Arbeitgeber geht, sollten Nutzer ihre Daten dort trotzdem nicht unverschlüsselt speichern, so die Empfehlung der Tester. Es wurden 13 Anbieter getestet, darunter 7 aus Europa. Alle Cloud-Dienste speichern die Daten ihrer Nutzer demnach verschlüsselt ab. Allerdings behalten 12 von 13 Firmen anschließend eine Kopie des Schlüssels und haben so weiter Zugriff auf die Daten. Das gilt sowohl für Europa als auch für die USA. Bei US-Diensten kommt außerdem hinzu, dass Sicherheitsbehörden sich jederzeit Zugriff auf die dort gespeicherten Daten verschaffen können.

### **Verschlüsseln mobil oder auf dem PC**

Zum Schutz vor neugierigen Blicken werden im «test» (Ausgabe 8/2013) kostenlose Programme wie Boxcryptor und Cloudfogger empfohlen. Beide funktionieren den Angaben nach gut und zwar sowohl auf mobilen Plattformen als auch auf dem PC. Durch die Verschlüsselung fallen allerdings einige praktische Funktionen weg: Auf diese Weise geschützte Bilder lassen sich nicht mehr auf dem Cloud-Server in einer Galerie betrachten. Richtig überzeugen konnte die Tester keiner der Kandidaten: 7 Anbieter wurden mit "Befriedigend" bewertet, 6 erhielten nur ein "Ausreichend". Kritik gab es außer am Datenschutz vor allem an der Bedienung, etwa wegen fehlender oder schlechter Hilfsfunktionen.

**dunkle Wolke** Die Forscher des Fraunhofer Instituts haben Cloud-Speicherdienste unter die Lupe genommen. Die meisten überprüften Angebote sind in Punkto Datenschutz und Datensicherheit durchgefallen.