DIE 5 GRÖSSTEN CLOUD-DIENSTE IM SICHERHEITSTEST

Auf die eigenen Daten immer und überall zugreifen zu können, ist auch für viele Privatleute von großer Bedeutung. Das geht bequem und einfach mit einem Cloud-Dienst. Wie es dabei um die Sicherheit der Daten steht haben wir, gemeinsam mit den Analysten von umlaut, für Sie getestet. › von Stefan Schasche

Für die überwältigende Mehrheit der größeren Unternehmen in Deutschland ist die Cloud-Nutzung heute eine unverzichtbare Selbstverständlichkeit. Aber auch im Privatbereich wird die Cloud immer wichtiger; allein schon, weil die Anzahl der mobil genutzten Geräte zunimmt. Wer nur einen stationären PC besitzt, der kann seine Datensicherung auch auf einem Cloud-Laufwerk vornehmen, aber wirkliche Vorteile entstehen daraus nicht. Zum einen ist, egal wie schnell der Internetzugang auch sein mag, eine lokale Datensicherung immer schneller. Zum anderen sind Festplatten derart preiswert geworden, dass lokale Backups selbst riesiger Datenmengen für ganz wenig Geld erfolgen können. Das Blatt wendet sich jedoch, wenn man mehrere Geräte im Einsatz hat und zudem auch noch mobil unterwegs ist. Dann werden Cloud-Dienste zu einem unschlagbaren Service.

Mit dem Smartphone geschossene Bilder sind beispielsweise umgehend auf allen Endgeräten, vom Notebook bis zum PC, daheim verfügbar. Es besteht, unabhängig vom Standort, ein stetiger Zugriff auf die Dateien, und wird irgendwo eine Änderung vorgenommen, muss man sich um eine Anpassung und unterschiedliche Versionen keinerlei Sorgen machen. Prinzipiell sorgt eine Cloud auch für Sicherheit, weil Datenverluste im Grunde nicht vorkommen.

Das sieht bei einem privaten Backup schon anders aus, weil Festplatten nicht unbedingt die zuverlässigste Hardware sind, und auch gegen Katastrophen wie ein Feuer oder Diebstahl sind sie nicht gefeit. Nutzer von Cloud-Diensten sollten sich jedoch stets bewusst sein: Sie vertrauen ihre Daten einem Dienstleister an, der diese möglicherweise auf Servern im Ausland lagert. Das mag bei Urlaubsfotos kein Problem sein,

bei privaten Dokumenten wie Passkopien, Testamenten oder Verträgen sieht das aber schon ganz anders aus. Daher sollte sich jeder genau überlegen, welche Dateien einer Cloud anvertraut werden sollen und welche eher nicht. Bei welchem Anbieter Ihre Daten am besten aufgehoben sind, zeigt Ihnen dieser Cloud-Sicherheitstest. Wir haben die fünf Dienste untersucht, die in Deutschland die größte Verbreitung haben.

Apple iCloud: Ideal für iPhone & Co.

Die iCloud von Apple ging 2011 an den Start und gehört damit zu den dienstältesten Cloud-Diensten am Markt. Wer ein Apple-Gerät im Einsatz hat, der ist mit einiger Sicherheit auch iCloud-Nutzer, denn bereits mit der Erstellung einer Apple ID ist man bei der iCloud angemeldet. Zwar lässt sich die iCloud auch mit Windows-Geräten verwenden, aber viele der Automatismen stehen dann nicht zur Verfügung. Dateien lassen sich zur Weiterbearbeitung beispielsweise nur mit Apple-Programmen wie Pages oder Numbers anlegen und fließend auf einem anderen Gerät weiterbearbeiten. In unserem Vergleichstest bildet die iCloud das Schlusslicht. Zwar gibt es bei der Sicherheit des Datenflusses, der iCloud-Webseite und der Webserver nichts zu bemängeln, jedoch verlor die iCloud bei der Authentifizierung entscheidend an Boden. In erster Linie bewertet *umlaut* das Passwort-Reset als unsicher, weil die hierfür verwendeten Fragen, beispielsweise nach dem Geburtsdatum oder Mädchennamen der Mutter, für Unbefugte recht einfach herauszufinden sind. Eine Zwei-Faktor-Authentifizierung funktioniert darüber hinaus nur bei Verwendung von Apple-Geräten.

Dropbox: Der Cloud-Veteran

Der in den USA beheimatete Dienst Dropbox ist sogar noch drei Jahre älter als die iCloud und war damit einer der ersten universellen Cloud-Dienste auf dem Markt. Eine Basis-Version für Privatanwender mit zwei GByte Speicherplatz ist gratis, die Variante Dropbox Plus mit zwei TByte kostet pro Monat 9,99 Euro. Generell ist Dropbox sehr einfach bedienbar und nicht zuletzt aus diesem Grunde sehr populär. Wer möchte, kann in der Dropbox abgelegte Dateien über einen privaten Link mit anderen Nutzern teilen. Eine automatische Synchronisation von Daten erfolgt auf Wunsch mithilfe eines Sync-Ordners. Diese

TESTVERFAHREN CLOUD-DIENSTE

umlaut Die Analysten von *umlaut* testen und bewerten die Cloud-Dienste in unserem Vergleichstest in vier verschiedenen Kategorien, in denen es jeweils 20 beziehungsweise 30 Punkte zu holen gibt. Der Testsieger kann somit maximal 100 Punkte einfahren.

AUTHENTIFIKATION (MAX. 30 PUNKTE)
Hier geht es um die Sicherheit der Authentifizierung. Wir testen, ob die Web-App hinreichend gegen Brute-Force-Angriffe schützt, ein sicheres Passwort-Reset implementiert ist und es eine 2-Faktor-Authentifizierung gibt.

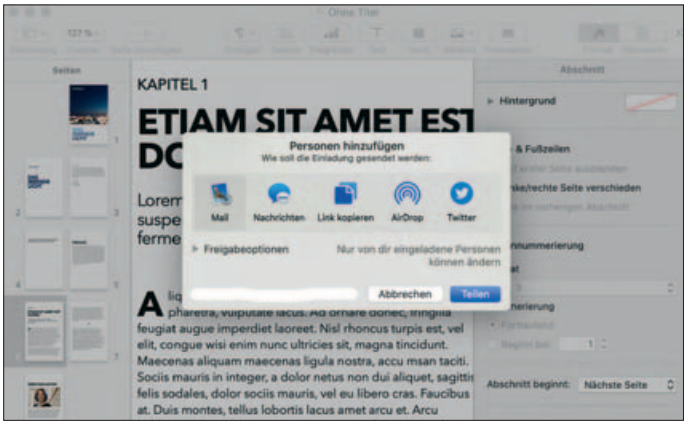
INTEGRITÄT (MAX. 30 PUNKTE)
Hier geht es um die Evaluierung von Autorisierungsmechanismen. Geprüft wird dabei beispielsweise, ob ein Angreifer unsichere Session-IDs für Attacken nutzen oder Session-Cookies abfangen oder manipulieren kann.

ABSICHERUNG DES DATENFLUSSES (MAX. 20 PUNKTE)
Wer sichere Verschlüsselungsmechanismen verwendet, sichere Server-Zertifikate nutzt und sämtliche Daten nur verschlüsselt überträgt, der punktet hier.

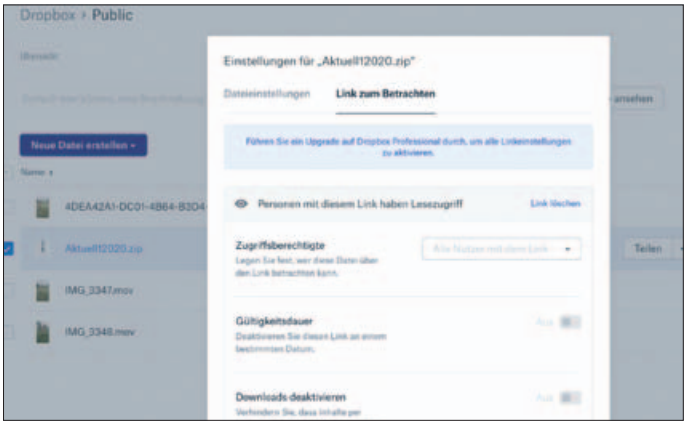
WEBSEITEN-SCHUTZ (MAX. 20 PUNKTE)
Unsere Evaluierungsmethodik prüft, ob die Web-Applikation sichere Header an die Client-Seite überträgt und Angreifern keine wertvollen Informationen offenlegt.

Stefan Schasche, Redakteur PCgo

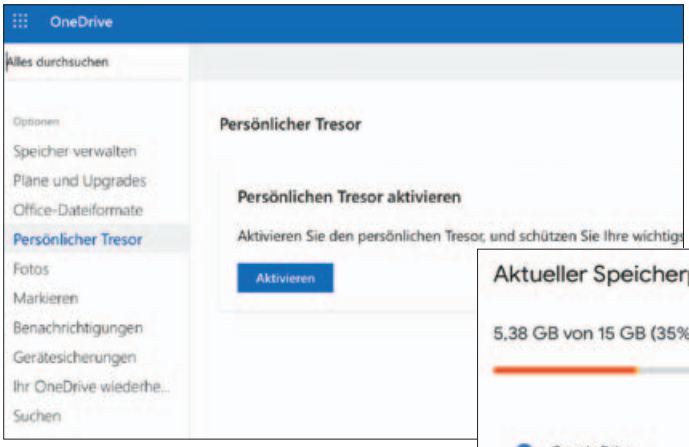
EXPERTEN-MEINUNG Wer Apple-Geräte nutzt, für den gibt es zur iCloud keine wirkliche Alternative. Wichtig für alle Anwender ist hier, die Antworten auf die Sicherheitsfragen möglichst kompliziert zu gestalten, auch wenn diese gar nicht korrekt sind. Den Mädchennamen Ihrer Mutter können Sie sich auch ausdenken.
Wer Sorgen hat, dass seine Daten in den USA lagern, für den empfiehlt sich die MagentaCloud der Telekom oder, wer Microsoft 365 nutzt, auch OneDrive. Ich selbst bin mit den Gratis-Varianten bei vier Anbietern vertreten und komme so kostenlos auf jede Menge Speicherplatz, den ich nicht mal annähernd ausreize.



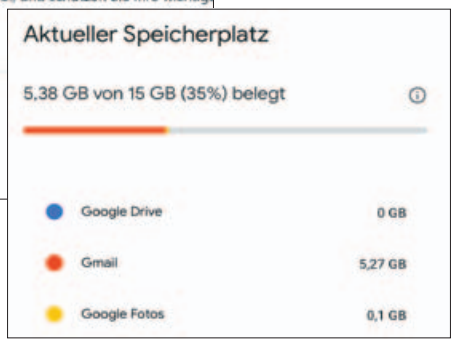
Nur wer Apple-Software nutzt, kann in der iCloud Dokumente mit anderen Personen oder an einem anderen Rechner weiterbearbeiten.



Über den Public-Ordner der Dropbox lassen sich Dateien ganz einfach mit anderen Anwendern teilen.



Sehr wichtige Daten lassen sich im OneDrive-Tresor mit einer weiteren Identitätsprüfung sichern.



GMail zwackt Speicherplatz von Google Drive ab. Insgesamt 15 GByte sind hier gratis.

Daten müssen letztlich aber stets auf einem Rechner gespeichert bleiben, um nicht zu verschwinden. So einfach die Dropbox auch zu bedienen ist, so hat sie bei der Integrität ein Manko. Bei geteilten Rechnern, zum Beispiel in einem Internetcafé, könnten sich spätere Nutzer des Rechners über ein einfaches Zurückgehen im Browser Zugang zu Dateinamen, E-Mail-Adresse und anderen Daten des Vornutzers verschaffen, wenn dieser die Dropbox genutzt hat. Dropbox-Kunden sollten sich also immer komplett aus der Dropbox ausloggen und den Browser schließen, bevor sie den Rechner verlassen.

Google Drive: Beste Sicherheit

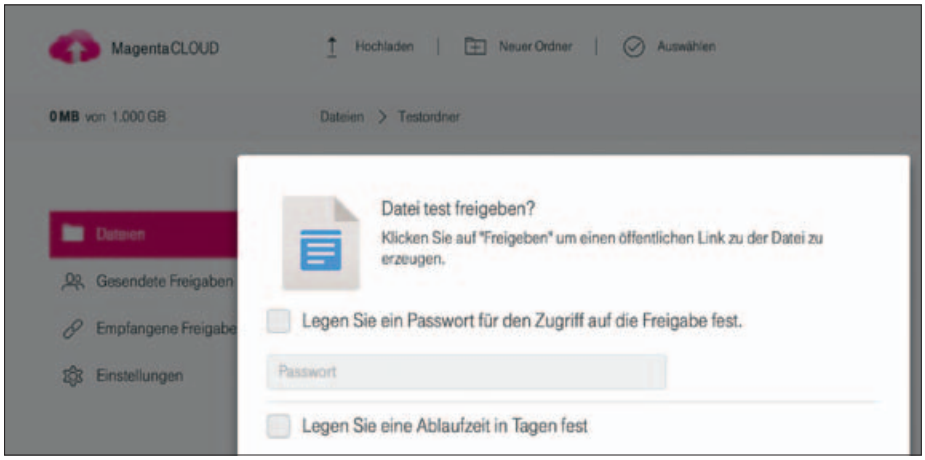
Seit 2012 gibt es den Dienst Google Drive, der zuvor als Google Docs unterwegs war und bis dahin lediglich die Erstellung und Bearbeitung von Dokumenten in der Cloud ermöglichte. Wer sich bei unserem Testsieger anmeldet, erhält üppige 15 GByte Datenspeicher gratis. Wer mehr Platz benötigt, zahlt jährlich 19,99 Euro für 100 GByte, 29,99 Euro für 200 GByte oder 99,99 Euro für zwei TByte. Die Bedienung von Google Drive ist denkbar einfach, was auch für die gemeinsame Bearbeitung von Dokumenten mithilfe von Google Docs gilt. Wo die Daten von Privatkunden letztlich gespeichert werden, dürfte höchstens Google selber wissen, denn der Konzern betreibt Rechenzentren an vielen Standorten nahezu überall auf dem Globus. Wer die Google-Cloud-Angebote für Geschäftskunden nutzt, der kann sich den Wirtschaftsraum, in dem seine Daten gespeichert werden sollen, selber aussuchen. Während Google Drive in den anderen Kategorien überzeugt, erhält der Dienst bei der Authentifizierung nur 22 von 30 möglichen Punkten. Hauptfaktor ist die vergleichsweise niedrige Anforderung an die verwendeten Passwörter, die lediglich aus acht Zeichen bestehen müssen. Zudem müssen Kunden kein eigenes Passwort für Google Drive anlegen. Stattdessen funktioniert das Google-Mail-Passwort auch für den Cloud-Service.

Microsoft OneDrive: Rundherum empfehlenswert

Auf Platz zwei unseres Sicherheitstests landet mit Microsoft OneDrive ein weiterer US-Dienst. In der Basis-Version des Dienstes erhält der Kunde fünf GByte Speicherplatz gratis, 100 GByte kosten zwei Euro monatlich. Dazu gibt es noch die Möglichkeit, Speicherplatz in Verbindung mit Microsoft 365 (früher Office 365) zu erwerben. Ein TByte kostet dann jährlich 69 Euro, für sechs TByte sind 99 Euro im Jahr fällig. Die Bedienung von Onedrive ist ähnlich einfach wie bei Dropbox oder Google Drive, zudem ist Microsoft 365 perfekt integriert. Zahlreiche Apps, etwa für Android, iOS oder Windows Phone, ermöglichen einen unkomplizierten Zugang auch aus anderen Betriebssystemwelten. Ein nützliches Feature ist, soweit man denn Microsoft generell als zuverlässigem Datendienst vertraut, der OneDrive-Tresor zum Speichern besonders wichtiger Daten. Der Zugang zu den hier abgelegten Files ist nur möglich durch eine weitere Identitätsprüfung wie einen Fingerabdruck, eine Gesichtserkennung oder per PIN oder Code, der per E-Mail oder SMS gesendet und eingegeben wird.
Unterm Strich ist Microsofts Cloud in allen Bereichen sehr gut dabei und erlaubt sich keine gravierenden Schwächen. So ist OneDrive letztlich für Privatanwender eine rundherum empfehlenswerte Option, sofern Sie sich nicht daran stören, dass die Daten in den USA lagern. Ausnahmen sind lediglich die Microsoft-365-Varianten: Hier liegen die Daten auf Servern in Deutschland.

Telekom MagentaCloud: Sichere Server in Deutschland

Im Gegensatz zu den Konkurrenten speichert die Telekom die Daten seiner Cloud-Kundschaft in Deutschland. Auf diese Tatsache weist die Telekom zu Recht auf ihrer Webseite prominent hin. Im Tarif Magenta Cloud Free



Die Oberfläche und die Schaltflächen der MagentaCloud sind sehr übersichtlich gestaltet.

erhalten Privatpersonen drei GByte Speicherplatz, Telekomkunden werden mit 15 GByte weit besser gestellt. 100 GByte lässt sich die Telekom derzeit mit 1,95 Euro monatlich bezahlen, für 500 GByte sind pro Monat 4,95 Euro fällig. Die Bedienung der MagentaCloud ist alles in allem einfach. Apps sind für alle Betriebssysteme und Endgeräte erhältlich, vom iPhone bis zum Android-Tablet. Die Telekom bietet eine ganze Reihe nützlicher Funktionen. Dazu gehört etwa eine Offline-Funktion für ausgesuchte Daten oder eine Freigabe von Daten an andere mithilfe individueller Links. Grundsätzlich ist die MagentaCloud daher ein empfehlenswerter Dienst, der allerdings im Bereich Authentifizierung Federn lassen muss; denn als einziger Anbieter verzichtet die Telekom komplett auf den Einsatz einer 2-Faktor-Authentifizierung. Diese ist zwar schon länger von der Telekom angekündigt worden, auf die Umsetzung warten Kunden allerdings bis heute. Das ist alles in allem natürlich sehr schade, weil der Datenstandort Deutschland für viele Anwender, die in der Cloud sensible Daten speichern möchten, naturgemäß attraktiver ist als zum Beispiel die USA. Es wäre daher wünschenswert, den Zugang auf Wunsch auch über ein sichereres Verfahren als die simple Eingabe eines Passworts zu ermöglichen. ‹

PCgo 6/20 TESTSIEGER

ANBIETER	1 GOOGLE	2 MICROSOFT	3 TELEKOM	4 DROPBOX	5 APPLE
Produkt	Google Drive	Microsoft OneDrive	Telekom MagentaCloud	Dropbox	Apple iCloud
					
GESAMTWERTUNG	**91 Punkte (sehr gut)**	**90 Punkte (sehr gut)**	**87 Punkte (sehr gut)**	**83 Punkte (gut)**	**82 Punkte (gut)**
Speicherplatz	15 GByte	5 GByte	3 GByte	2 GByte	5 GByte
Preis	gratis	gratis	gratis	gratis	gratis
Internet www.	drive.google.com	onedrive.live.com	magentacloud.de	dropbox.com	icloud.com
TECHNISCHE MERKMALE					
Speicherplatz-Erweiterungen	100 GByte / 200 GByte / 2 TByte	100 GByte / 1 TByte / 2 TByte	100 GByte / 500 GByte / 1 TByte	2 TByte / 3 TByte	50 GByte / 200 GByte / 2 TByte
Preis pro Jahr	19,99 / 29,99 / 99,99 Euro	24 / 69 / 99 Euro	23,40 / 59,40 / 119,40 Euro	119,88 / 198,96 Euro	11,88 / 35,88 / 119,88 Euro
Apps	Mac / PC / iOS / Android	Mac / PC / iOS / Android	Mac / PC / iOS / Android	Mac / PC / iOS / Android	Mac / PC / iOS
Datenverschlüsselung	nur Synchronisierung	nur Synchronisierung	ab Paket XL (1 TByte)	AES 256-bit (ab 2 TByte)	AES 128-bit
Server-Standort	USA	USA (außer Office-Tarif)	Deutschland	USA	USA
2-Faktor-Authent.	●	●	●	●	●, für Apple-Geräte
AUTHENTIFIKATION (MAX. 30 PUNKTE)	**22 Punkte**	**26 Punkte**	**21 Punkte**	**24 Punkte**	**14 Punkte**
Qualität in Prozent	73 Prozent	87 Prozent	70 Prozent	80 Prozent	47 Prozent
INTEGRITÄT (MAX. 30 PUNKTE)	**30 Punkte**	**28 Punkte**	**30 Punkte**	**22 Punkte**	**30 Punkte**
Qualität in Prozent	100 Prozent	93 Prozent	100 Prozent	73 Prozent	100 Prozent
DATENFLUSS-SCHUTZ (MAX. 20 PUNKTE)	**19 Punkte**	**18 Punkte**	**18 Punkte**	**18 Punkte**	**18 Punkte**
Qualität in Prozent	95 Prozent	90 Prozent	90 Prozent	90 Prozent	90 Prozent
WEBSEITEN-SCHUTZ (MAX. 20 PUNKTE)	**20 Punkte**	**18 Punkte**	**18 Punkte**	**19 Punkte**	**20 Punkte**
Qualität in Prozent	100 Prozent	90 Prozent	90 Prozent	95 Prozent	100 Prozent
SONSTIGES					
Vorteile	großer Gratisspeicher	Datentresor	Server in Deutschland	einfache Bedienung	ideal für Apple-Geräte
Nachteile	einfache Passwörter	Server-Standort USA	keine 2-Faktor-Authent.	Integritätsprobleme	Passwortreset unsicher

● = ja ● = nein