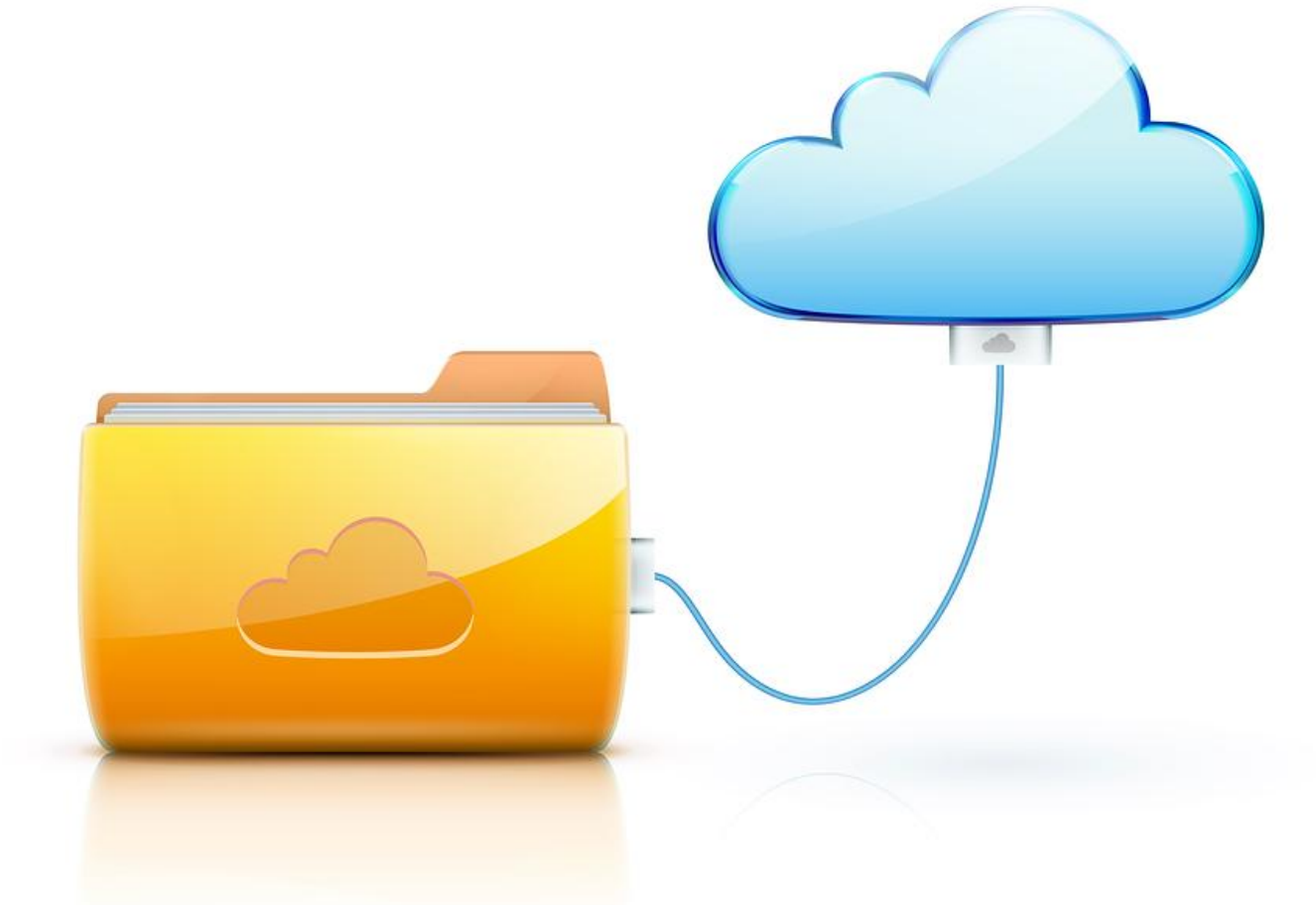
www.datensicherung.tips/thema/cloud-speicher



E-BOOK
RATGEBER

CLOUD-SPEICHER

1 Cloud-Speicher 3

2 Funktionen vergleichen 3

2.1 Desktop-Clients 3
2.2 Smartphone Apps 4
2.3 Onlinezugriff 5
2.4 Spezial-Schnittstellen 5

3 Sicherheit 7

3.1 Verschlüsselung 7
3.2 Sichere Übertragung 8
3.3 So sicher sind Online Speicher 8
3.4 NSA, GCHQ, etc. 9

4 Anbieter 10

4.1 Dropbox: Der Marktführer 10
4.2 Wuala: Der sichere Online Speicher 11
4.3 SkyDrive: Nahtlose Microsoft Eingliederung 12
4.4 Google Drive 13
4.5 Telekom Cloud: Deutscher Anbieter 14
4.6 Strato Hidrive: Professioneller Anspruch 15
4.7 1&1 (1und1) 17
4.8 MEGA 17
4.9 Livedrive 18
4.10 Fabasoft 19
4.11 SugarSync 20
4.12 SafeSync 21

5 Spezielle Backup-Lösungen 22

5.1 Mozy 22
5.2 Norton Cloud Backup 23
5.3 Carbonite 23
5.4 Dogado 24

6 Fazit 25

6.1 Sicherheit gegen Datenverlust 25
6.2 Zugriff von überall 25
6.3 Viel Bandbreite notwendig 26
6.4 Backups 26

1 Cloud-Speicher

Cloud-Speicher machen den Zugriff auf synchronisierte Dateien von überall auf der Welt aus möglich, sei es über Smartphone Apps für Android, iPhone und Co, oder über den Webbrowser per Onlinezugang. Zudem bieten Sie in puncto Datenverlust weitaus mehr Sicherheit, als wir es offline jemals könnten. Was den Datenschutz angeht, so sind insbesondere die europäischen Anbieter führend: Wuala, TrendMicro mit SafeSync und Strato Deutschland lagern die Dateien allesamt auf Rechenzentren in Deutschland oder zumindest Europa und müssen sich damit an strenge Datenschutzrichtlinien halten. Sicherheitsfunktionen wie AES-256bit Verschlüsselung sollten auch die letzten Zweifel hinsichtlich Datenschutz ausräumen und ein Maximum an Schutz bieten.

2 Funktionen vergleichen

Die Anbieter unterscheiden sich natürlich in der Größe des Speichers bzw. den Preisen dafür. Daneben spielen aber eine Reihe technischer Aspekte eine Rolle, die sich von Anbieter zu Anbieter teilweise deutlich unterscheiden.

2.1 Desktop-Clients

Fast jeder Anbieter von Online Speicher bietet seinen Kunden einen eigens entwickelten Desktop Client an. Dies ist ein Programm, dass Sie auf Ihrem Computer installieren und mithilfe dessen Sie die Daten automatisch auf die Online Festplatte synchronisieren können. Sie müssen dafür fast gar nichts unternehmen, denn der Upload Prozess geschieht erstens automatisch genau dann, sobald der Desktop Client erkennt, dass eine Datei verändert, gelöscht oder neu hinzugekommen ist. Zweitens werden veränderte Daten im Hintergrund so mit der Cloud synchronisiert, dass Sie während Ihrer normalen PC-Arbeit gar nichts davon mitbekommen, da die eingenommene Upload- bzw. Downloadgeschwindigkeit variabel angepasst werden kann - je nach Auslastung des Computers.

Desktop Clients haben also im Prinzip bei allen Anbietern den gleichen Zweck: Sie synchronisieren die Dateien hin zur Online Festplatte und wieder zurück. Die Art, wie die Daten auf dem lokalen PC gespeichert werden, kann jedoch unterschiedlich sein. Derzeit existieren zwei Möglichkeiten.

2.1.1 Spezieller Ordner

Es wird ein neuer Ordner an einem frei definierbaren Speicherort auf der Festplatte angelegt, der als Synchronisierungsordner fungiert. Die Dateien, die synchronisiert werden sollen, legen Sie einfach in diesen Ordner ab. Umgekehrt werden alle Dateien, die Sie von

andernorts auf den Cloud Speicher geladen haben, in diesen Ordner heruntergeladen. Dies hat zum einen den Vorteil, dass Sie sehr übersichtlich in einem Hauptordner sehen können, welche Dateien synchronisiert sind. Andererseits hat diese Methodik auch einen Nachteil: Wenn Ihr Desktop PC mehrere Festplatten besitzt oder Sie die bestehende Festplatte auf so genannte Partitionen unterteilt haben, haben Sie auf einer einzelnen Festplatte nicht immer genug Speicherplatz zur Verfügung, um alle Dateien des Synchronisierungsordners aufzunehmen. Dann heißt es, Platz zu schaffen oder von A nach B zu verschieben, um die Kapazitäten anders aufzuteilen.

Außerdem müssen Sie Dateien aus ihrer bisherigen Ordnerstruktur reißen und schaffen damit eine inkonsistente Struktur auf der Festplatte. Ein Beispiel: Wenn sie ihre Fotos normalerweise auf D:/Fotos speichern und ihre Videos auf D:/Videos, dann befindet sich der Synchronisierungsordner z. B. unter D:/Dropbox. Sie wollen nicht alle Bildergalerien synchronisieren und auch nur ein paar Videos sollen übertragen werden. Sie müssen nun bspw. die Teneriffa 2013-Galerie und das James Bond-Video aus ihren jeweiligen Dateistrukturen holen und in den Dropbox Ordner stecken. Fotos und Videos befinden sich also jetzt an zwei verschiedenen Speicherorten auf der Festplatte, was zu mehr Unübersichtlichkeit führt. Dieser Nachteil wird durch Variante 2 vermieden.

2.1.2 Ausgewählte Verzeichnisse

Sie können Dateien und Ordner markieren, um sie zu synchronisieren. Der Client fügt in diesem Fall dem Explorer eine zusätzliche Funktion hinzu, mit der Sie Dateien und Ordner als zu synchronisieren markieren können. So können Sie ganz gezielt nur bestimmte Dateien synchronisieren, ohne diese aus ihrer Ordnerstruktur herausreißen zu müssen, wie es bei Variante 1 der Fall ist. Die derzeitige Ordnerstruktur wird also nicht verändert und bleibt wie gewohnt erhalten. Nachteil: Es kann recht unübersichtlich werden, synchronisierte Dateien zu verwalten und wiederzufinden, da Sie sich durch eben jene ursprüngliche Ordnerstruktur klicken müssen. Oft greifen die Clients hier jedoch unterstützend unter die Arme und listen alle Dateien selbst nochmal tabellarisch auf.

2.2 Smartphone Apps

Die meisten Anbieter bieten Smartphone Apps für Android, iPhone, iPad und Windows Phone an. So haben Sie Ihre Daten auch unterwegs immer dabei. Dies macht es sehr leicht, das Smartphone z. B. als MP3 Player zu benutzen, da Sie die gespeicherte Musik einfach herunterladen oder streamen können. Dies wird jedoch keineswegs Ihr monatliches Downloadvolumen leersaugen, denn Sie können selbstverständlich konfigurieren, dass veränderte Daten nur per WLAN synchronisiert werden sollen. Zudem steht meist die Möglichkeit zur Verfügung, Dateien auf das Smartphone herunterzuladen, so dass gar keine Internetverbindung mehr nötig ist, um auf Musik und Videos zuzugreifen. Weil Smartphones jedoch deutlich weniger Speicherplatz zur Verfügung haben, als die heimische Festplatte,

wird vorher natürlich speziell auf Ordner- oder Dateiebene ausgewählt, welche Daten mit der Online Festplatte synchronisiert werden sollen.

Besonders praktisch an den Smartphone Apps der Cloud Speicher ist, dass aufgenommene Fotos und Videos direkt nach dem Erstellen in die Cloud synchronisiert werden können. Damit sind die Fotos und Videos auch sofort auf Desktop PC und allen anderen Geräten verfügbar, ohne dass das Smartphone per Datenkabel oder Bluetooth mit dem Laptop verbunden werden muss.

2.3 Onlinezugriff

Wer gerade kein Smartphone zur Verfügung hat oder andernorts per Computer auf seine Daten zugreifen möchte, kann das immer über den Internetbrowser tun. Die Anbieter stellen hierfür eine Website zur Verfügung, auf der Sie sich mit Usernamen und Passwort einloggen können und anschließend Zugriff auf ihre Daten haben. Hier können Sie z. B. schnell ein Dokument herunterladen, bearbeiten und wieder hochladen.

Per Onlinezugriff stehen oft auch zusätzliche Funktionen des Cloud Speicher zur Verfügung, wie z. B. passwortgeschützte Freigabe von Dateien, Erstellen von Bildergalerien für Freunde und Familie oder das Setzen von Berechtigungen. Auch soziale Netzwerke sind meist eingebunden, so dass Sie Fotos und Videos aus dem Onlinezugriff heraus teilen können.

2.4 Spezial-Schnittstellen

Manche Anbieter verzichten auf einen eigenen Desktop Client und setzen stattdessen auf alternative Zugriffskonzepte. Wir stellen die wichtigsten dieser Protokolle vor:

2.4.1 FTP

Das File Transfer Protocol (FTP) ist ein Netzwerkprotokoll zur Übertragung von Dateien über das Internet auf den Cloud Speicher. Mittels eines so genannten FTP Clients kann der Nutzer zum Server via Usernamen und Passwort verbinden und hat dann Zugriff auf die darauf befindlichen Daten. Diese können dann entsprechend verwaltet und heruntergeladen werden. FTP ist eine international gängige Schnittstelle für Dateiübertragungen, die von einigen Anbietern von Cloud Backup Lösungen zur Verfügung gestellt werden.

Standardmäßig stellt FTP jedoch eine unverschlüsselte Verbindung her und für eine sichere Verbindung mittels FTP muss eine verschlüsselte Verbindung manuell über SSL eingerichtet werden. Aufgrund dessen existiert mit dem SFTP Protokoll eine Alternative zu FTP, die auf SSH aufbaut und eine verschlüsselte Verbindung zum Server herstellt.

2.4.2 WebDAV

WebDAV ist wie FTP ein Protokoll zur Dateiübertragung zwischen einem Client und einem entfernten Server. Während FTP jedoch ein eigenständiges Protokoll darstellt, setzt WebDAV auf dem HTTP Protokoll auf, welches für den regulären Internetverkehr im Webbrowser zuständig ist (Port 80). Aufgrund dessen für WebDAV kein Aufwand für IT-Systemadministratoren notwendig, da keine zusätzlichen Ports geöffnet werden müssen (Port 21 hingegen zusätzlich für FTP). Da im HTTP Protokoll im Gegensatz zu FTP umfassende Authentifizierungsrichtlinien definiert sind, stellt WebDAV zudem eine sicherere Alternative zu FTP dar.

Ein weiterer Vorteil von WebDAV ist, dass WebDAV eine synchrone Verbindung zum Server aufbaut, während FTP für jeden Befehl eine einzelne Verbindung herstellt. Insbesondere bei vielen kleinen zu übertragenen Dateien kann die Übertragungszeit mit FTP daher deutlich länger dauern.

Auch WebDAV ist in Natura jedoch eine unverschlüsselte Verbindungsmöglichkeit. Je nach Anbieter kann jedoch eine SSL-verschlüsselte Verbindung hergestellt werden, mit der ein Abhören der Daten zwischen Client und Server (etwa in WLAN Hotspots) erschwert bzw. gänzlich verhindert werden kann.

2.4.3 SMB

SMB steht für Server Message Block und ist ein Kommunikationsprotokoll in Netzwerken, mit denen Dateien, Drucker und weitere Serverdienste in Netzwerken geteilt werden können. In der Praxis wird es in Verbindung mit Cloud Backup Lösungen dazu verwendet, die Online Festplatte direkt als virtuelles Laufwerk in den Explorer einzubinden. Die Online Festplatte kann dann wie gewohnt als Pseudolaufwerk verwendet werden, ohne dass ein separater Ordner über einen PC Client angelegt werden muss. Mittels SMB kann man also sogar gänzlich auf einen externen PC Client verzichten, da Veränderungen auf dem SMB Laufwerk in Echtzeit abgebildet werden.

In puncto Sicherheit soll das reine SMB Protokoll jedoch Probleme bereiten. In den letzten Jahren sind in Verbindung mit SMB mehrere Probleme und Schwachstellen bekannt geworden, denen man mit einer clientseitigen Verschlüsselung gerecht werden sollte.

2.4.4 Rsync

Auch das Netzwerkprotokoll Rsync dient der Dateiübertragung von einem Quellverzeichnis in ein Zielverzeichnis. Im Gegensatz zu SMB oder FTP kann Rsync auch nur Teile von Dateien übertragen, die geändert worden sind. Dies funktioniert jedoch nur bei unkomprimierten Formaten. So wäre bspw. denkbar, bei Backups nur die geänderten Daten und -Dateiteile zu übertragen. Zur Verwendung von Rsync wird ein Client benötigt.

3 Sicherheit

Wer seine persönlichen Dateien auf externen Rechenzentren sichern möchte, will seine Daten in erster Linie natürlich sicher aufbewahrt wissen. Ich persönlich würde einen Cloud Backup Dienst nur nutzen, wenn ich abends beruhigt einschlafen kann in der Beantwortung der Frage, ob jemand fremdes meine Urlaubsbilder, in Textdateien gespeicherte Bank- und Kreditkartendaten oder Kontaktlisten einsehen könnte. Gerade in der heutigen Zeit, als im Juni 2013 Edward Snowden die NSA Enthüllungen an den Tag gebracht hat, ist die Frage nach Sicherheit der Dateien auf Online Speicher Lösungen den meisten Leuten so bewusst und wichtig geworden wie nie zuvor.

3.1 Verschlüsselung

Sicherheit seiner gespeicherten Daten erhält man jedoch nur durch ausgeklügelte Verschlüsselungsalgorithmen. Die verschiedenen Algorithmen, die derzeit existieren, funktionieren im Grunde genommen alle ähnlich und unterscheiden sich lediglich in der Zeit, die es benötigt die Verschlüsselung zu knacken. Als bewährter Standard hat sich der AES (Advanced Encryption Standard) etabliert, der im Jahre 2000 zertifiziert wurde und als der sicherste Verschlüsselungsalgorithmus der Welt gilt. Derzeit sind keine Schwachstellen dieser Verschlüsselung bekannt. Die Bezeichnungen der 3 AES-Varianten AES-128, AES-192 und AES-256 beziehen sich allesamt auf die gewählte Schlüssellänge, TrueCrypt als Verschlüsselungs-Tool empfiehlt bspw. eine Schlüssellänge von mindestens 20 Zeichen, bestehend aus Buchstaben mit Groß- und Kleinschreibung, Sonderzeichen und Ziffern. Der sicherste AES-256 Bit Standard ist nach dem heutigen Stand der Technik praktisch unknackbar.

Mit einem Computer, der pro Sekunde eine Milliarde Schlüssel durchprobieren könnte, was technisch noch nicht möglich ist, würde man 3*10 hoch 51 Jahre brauchen, um einen gängigen 256-bit-Schlüssel zu knacken.» Also drei Oktilliarden Jahre (eine 3 mit 51 Nullen). (Peter Kohler)

Viele Anbieter für Cloud Speicher haben eine AES Verschlüsselung auf ihren Dateisystemen integriert, jedoch nicht alle. Fehlt die Verschlüsselung, liegen die Dateien also komplett unverschlüsselt auf den Festplatten der Online Backup Dienste und Mitarbeiter und Hacker dieser Dienste haben (theoretisch) Zugriff darauf. Auch ein verlorenes Smartphone oder ein geklauter PC ermöglicht dem Finder bzw. Dieb somit Vollzugriff auf die synchronisierten Daten.

3.2 Sichere Übertragung

Es genügt jedoch nicht auf eine verschlüsselte Speicherung der Daten zu achten. Es gibt noch eine weitere Schwachstelle in der Kette vom Client zum Server und zurück: Die Übertragung der Dateien zwischen Client und Server. Also von ihnen zur Online Festplatte und zurück. Auch diese Übertragung muss verschlüsselt geschehen, damit die Daten auf dem Übertragungsweg zwischen Client und Server nicht abgefischt werden können. Stellt man sich nun vor, dass die Daten je nach Anbieter teilweise sogar bis in die USA übertragen werden müssen, so ist dies ein sehr langer Weg, der u. U. von Geheimdiensten oder Hackern infiltriert sein könnte. Nicht immer müssen jedoch NSA und Co hinter solchen Absichten stecken. Ein viel einfacheres und praxisnahes Beispiel umgibt beinahe jeden von uns: Internet Access Points. Wer unterwegs ist und sich mit Notebook oder Smartphone in ein Netzwerk verbindet - etwa ein WLAN Hotspot bei McDonald's oder Starbucks- und dann keine verschlüsselte Verbindung zu eben jenem aufbaut, der läuft Gefahr dass der Datenverkehr von Hackern abgefischt wird. Entsprechende Tools machen dies kinderleicht. Dies gilt übrigens nicht nur für Cloud Backup Dienste, sondern für den gesamten Internetverkehr, der über Access Points geführt wird. Login Daten, Kreditkartendaten und persönliche Informationen werden zum Teil immer noch unverschlüsselt übertragen und machen es Hackern leicht, diese im Netzwerk mitzulesen und abzugreifen.

3.3 So sicher sind Online Speicher

Die Sicherheit der Cloud Speicher Anbieter lässt sich am ehesten daran erkennen, ob dieser die Daten verschlüsselt speichert oder nicht. Aufgrund der jüngsten NSA Enthüllungen sind auch der Standort der Rechenzentren sowie der Firmensitz der Unternehmung von Bedeutung. Wir unterscheiden in folgende Stufen der Sicherheit.

3.3.1 Stufe 1 - Verschlüsselte Übertragung

Die zu synchronisierenden Daten werden verschlüsselt vom Client zum Server übertragen, werden dort jedoch unverschlüsselt gespeichert. Mitarbeiter des Dienstes oder Hacker, die sich illegalen Zugriff auf den Server verschaffen, haben uneingeschränkten Zugriff auf alle Daten. Auch ein verloren gegangenes Smartphone oder ein geklauter Desktop PC wird damit zum Problem. Während der Übertragung sind die Daten jedoch nicht zu entziffern und gelten nach heutigem Stand der Technik als abhörsicher.

3.3.2 Stufe 2 - Verschlüsselte Übertragung und Speicherung

Die zu synchronisierenden Daten werden verschlüsselt übertragen, anschließend auf dem Server des Anbieters mittels AES verschlüsselt und auf der Online Festplatte verschlüsselt abgelegt. Hacker des Dienstes haben keine oder nur sehr geringe Chancen, gewonnene Daten zu entziffern. Da die Dateien erst auf dem Server des Anbieters verschlüsselt werden, muss der Schlüssel hierfür beim Anbieter gespeichert werden. Wird der Schlüssel zusammen

mit den Daten abgegriffen, ist es Dritten theoretisch weiterhin möglich, die Daten abzurufen und dann zu entschlüsseln.

3.3.3 Stufe 3 - End-To-End Verschlüsselung durch Anbieter

Die zu synchronisierenden Daten werden verschlüsselt übertragen und bereits beim Anwender verschlüsselt, nicht erst auf dem Server des Anbieters wie in Stufe 2. Dies wird als End-To-End Verschlüsselung bezeichnet. Dadurch bleibt der Schlüssel lokal beim Anwender - der Anbieter und eventuelle Eindringlinge in das Rechenzentrum des Anbieters haben theoretisch keinerlei Möglichkeiten, die gespeicherten Daten zu entschlüsseln. Nachteil: Wird das Passwort der Verschlüsselung vergessen oder verschlampt, sind die gespeicherten Dateien unbrauchbar.

Da die Verschlüsselung durch den Client des Anbieters geschieht, besteht theoretisch immer noch die Möglichkeit, dass der Anbieter des Cloud Backup Dienstes den Schlüssel zusammen mit den Daten in unerlaubter Weise auf seine Rechenzentren überträgt und die Daten somit entschlüsseln werden können.

3.3.4 Stufe 4 - End-To-End Verschlüsselung durch Anwender

Die zu synchronisierenden Daten werden verschlüsselt übertragen und bereits beim Anwender mittels AES-256bit verschlüsselt. Der Anwender nutzt im Gegensatz zur Stufe 3 sein eigenes Verschlüsselungs-Programm, wie z. B. TrueCrypt, womit die Dateien durch ein externes Programm verschlüsselt werden, auf das der Anbieter der Cloud Backup Lösung keinen Einfluss hat. Dies ist die einzig wahre End-To-End Verschlüsselung und gilt derzeit als die sicherste Variante, Daten auf dem Cloud Speicher abzulegen.

3.4 NSA, GCHQ, etc.

Die NSA und GCHQ Enthüllungen haben gezeigt, dass ausländische Geheimdienste bereit sind, unsere Daten in großem Stil zum einen während der Übertragung abzugreifen und zum anderen auch direkt auf Dienste wie Facebook oder Google zuzugreifen, um Daten abzurufen. Aus diesem Grunde ist momentan von Online Speicher Lösungen, die

- ihren Sitz in den USA oder Großbritannien haben,
- Rechenzentren in USA oder Großbritannien betreiben,

dringend abzuraten. Wer dennoch ein Abonnements bei solchen Anbietern kaufen möchte, der sollte tunlichst Stufe 4 befolgen und die gespeicherten Daten mit einem eigenen Verschlüsselungs-Programm und mindestens 20 Zeichen langem Passwort verschlüsseln. Ein Restrisiko kann dann allerdings nicht ganz ausgeschlossen werden, denn: Der AES Verschlüsselungsalgorithmus ist eine US-amerikanische Verschlüsselung. Ein Schelm, wer Böses dabei denkt.

4 Anbieter

Nicht zuletzt durch Dropbox sind Onlinespeicher einem breiten Publikum bekannt geworden und haben dadurch stark an Akzeptanz gewonnen. Seitdem hat sich eine ganze Reihe von großen und kleinen Anbietern zum Ziel gesetzt, Dropbox zu kopieren oder zu verbessern.

4.1 Dropbox: Der Marktführer

Dropbox ist einer der bekanntesten Anbieter von Cloud Speicher mit Sitz in den USA und existiert bereits seit dem Jahre 2007. Dropbox ist einer der Pioniere unter den Anbietern von Cloud Backup und ist einer der führenden Services - Über 50 Millionen Nutzer laden etwa alle drei Tage über eine Milliarde Dateien auf Dropbox hoch. Dropbox ist insbesondere dafür bekannt, seinen Nutzern den Einstieg so leicht wie möglich zu machen. Mithilfe von Video-Tutorials oder einer Online Tour zum Durchklicken sollte es somit jedem möglich sein, auf den Dienst ohne Probleme zuzugreifen.

4.1.1 Zugriffsmöglichkeiten

Dropbox bietet eine Vielzahl von Leistungen und Features. Hauptsächlich dreht sich bei Dropbox alles um die Clients. Der Desktop Client, den sicherlich die meisten Benutzer zur automatischen Datensynchronisation verwenden, ist verfügbar für die Betriebssysteme Windows, Mac und Linux und deckt damit den Großteil aller erhältlichen Betriebssysteme ab. Dateien, die sich im Dropbox Folder befinden, werden automatisch auf die Online Festplatte hochgeladen und sind damit sicher gespeichert. Dank einer Versionsverwaltung werden auch ältere Versionen von Dokumenten und Bildern gespeichert.

Aber auch für die mobilen Benutzer bietet Dropbox Clients an. Sowohl für Apples iOS, als auch für Googles Android ist eine Dropbox App erhältlich, mit der die Daten auch unterwegs auf Smartphone synchronisiert werden können. Aufgrund des begrenzten Speicherplatzes auf dem Smartphone ist bei den Apps natürlich auswählbar, welche Dateien synchronisiert werden sollen und welche nicht. So kann man bspw. seine Lieblingsmusik überall mit hinnehmen und muss diese nicht mehr lästig per PC Verbindung selbst managen.

Wer gerade keinen Client zur Verfügung hat, der hat natürlich auch die Möglichkeit, über das Web Interface auf seine Dateien zuzugreifen und diese von jedem Browser aus herunterzuladen und zu managen. Eine einfach zu bedienende Nutzerrechteverwaltung ermöglicht es zudem, nur bestimmten Personen bestimmte Dateien zur Verfügung zu stellen.

4.1.2 Sicherheit

Dropbox bietet umfangreiche Sicherheitsmechanismen zum Schutz der Daten seiner User. So werden die Dateien intern durch eine 256 Bit AES Verschlüsselung versehen, die nach heutigem Stand der Technik sicher ist. Zusätzlich dazu ist die Verbindung zwischen Clients und Server mit dem SSL Verfahren verschlüsselt. Dropbox steht jedoch trotzdem zum Teil in Kritik: Bemängelt wird z. B., dass die Clients ständig eingeloggt sind und keine weitere Passwortabfrage nötig ist, um Dateien hoch- oder runterzuladen.

4.1.3 Free Space und kostenpflichtige Abonnements

Bei erstmaliger Anmeldung erhält jeder User 2 GB kostenlosen Speicherplatz zur freien Nutzung ohne Traffic-Begrenzung. Für jeden geworbenen Freund gibt es 500 MB oben drauf und indem man an einigen weiteren Werbe-Aktionen mitmacht, kann man sich weitere extra MB verdienen. Wer jedoch mehr Speicherplatz benötigt, kann auf einen der kostenpflichtigen Abonnements zugreifen.

4.2 Wuala: Der sichere Online Speicher

Wuala ist eine Cloud Backup Lösung mit Sitz in der Schweiz und zeichnet sich insbesondere durch seine Datensicherheit aus. Das im Jahre 2009 vom französischen Speicherspezialisten LaCie übernommene Unternehmen spricht sich wie das französische Wort Voilá aus.

4.2.1 Zugriffsmöglichkeiten

Wie bei Dropbox existiert auch für Wuala ein Desktop Client, der sowohl auf Windows und Mac läuft, als auch auf Linux. Anders als bei Dropbox synchronisiert der Client nicht in Echtzeit - das spart Traffic und Bandbreite. In den Einstellungen lassen sich jedoch Synchronisationsabstände bis mindestens 1 Minute Abstand einstellen.

4.2.2 Sicherheit

Sicherheit und Datenschutz wird bei Wuala groß geschrieben. Ein Hauptmerkmal von Wualas Sicherheitsrichtlinie ist das ausgeklügelte Sicherheitssystem der gespeicherten Daten, das in diesem Umfang nicht viele Anbieter aufweisen. Der größte Vorteil ist, dass hochgeladene Dateien bereits beim Benutzer mit dem AES 256 Bit Verschlüsselungsalgorithmus verschlüsselt werden. Somit ist eine echte End-To-End Verschlüsselung möglich. Die verschlüsselten Dateien werden anschließend intern auf kleine Datenfragmente aufgesplittet und schließlich auf verschiedenen Servern in Europa gelagert. Nach derzeitigem Informationsstand unterhält Wuala keine Server außerhalb Europas, so dass hier ein Maximum an Datenschutz und Datensicherheit gewährleistet werden kann. Derzeitige Serverstandorte sind die Schweiz, Deutschland und Frankreich. Selbst Wuala hat keinen Zugriff auf die Daten. Daraus ergibt sich allerdings der Nachteil, dass ein vergessenes Passwort nicht wiederhergestellt werden kann, da Wuala keinen Zugriff darauf hat.

4.2.3 Free Space und kostenpflichtige Abonnements

Free User erhalten bei Wuala 5 GB Online Speicher, der bis zu 10 GB erweitert werden kann, wenn Sie Freunde zu Wuala einladen. Pro erfolgreich geworbenen User erhalten Sie anders als bei Dropbox nicht 500 MB extra, sondern 1 GB. Außerdem erhält der geworbene Benutzer nicht 5 GB Platz auf der Online Festplatte, sondern 6 GB.

Wer mehr als die 5 GB gratis Space benötigt, kann aus einem der 7 kostenpflichtigen Abonnements wählen. Anders als bei Dropbox beträgt das größte Wuala Abonnement 2 TB und nicht 500 MB.

4.3 SkyDrive: Nahtlose Microsoft Eingliederung

SkyDrive ist der Cloud Speicher aus dem Hause Microsoft. Es gehört zum Windows Live Dienst und basiert auf dem seit über 10 Jahre betriebenen Hotmail Service. Da Microsoft allerdings ein US Unternehmen ist, sind die Daten hier nicht ganz so sicher, wie bspw. bei Wuala

4.3.1 Zugriffsmöglichkeiten

SkyDrive bietet einen Desktop Client für Windows 8, Windows 7, Windows Vista und verschiedene Windows Server Versionen an, sowie einen Desktop Client für Mac. Ein Client für Linux Betriebssystem existiert leider nicht und auch Windows XP Nutzer haben das Nachsehen. Eine Besonderheit der Desktop Clients (von Microsoft liebevoll als App bezeichnet) ist, dass dieser keinen SkyDrive Ordner anlegt, sondern gleich ein neues virtuelles Laufwerk. Dieses lässt sich direkt im Arbeitsplatz verwenden. Seit Microsoft Office 2010 können Nutzer zudem Dateien direkt in SkyDrive synchronisieren, ohne diese auf das SkyDrive Laufwerk abzulegen. Zudem sind Möglichkeiten gegeben, an ein und demselben Dokument mit mehreren Nutzern gleichzeitig zu arbeiten, was so ziemlich einmalig ist. SkyDrive bietet damit Funktionen, die nur aufgrund der nahen Integrationsmöglichkeiten in Windows möglich sind und profitiert damit von dem hohen Marktanteil des eigenen Betriebssystems Windows.

Zudem stellt Microsoft Schnittstellen für Smartphones und Tablets zur Verfügung. Apps existieren für iPad, iPhone, Android und Windows Phone und unterstützt damit so viele verschiedene mobile Betriebssysteme, wie kaum ein anderer Anbieter von Cloud Backup Lösungen. Weiter ist das Web Interface über jeden beliebigen Browser zu erreichen und ist stark darauf ausgelegt, mit mobilen Geräten bedient zu werden.

4.3.2 Sicherheit

Microsoft hat in der Datenhaltung bereits jahrelang Erfahrung und speichert alle Daten verschlüsselt auf seinen Servern ab. Trotzdem wird empfohlen, die Daten bereits bei sich auf dem PC mit Verschlüsselungssoftware selbst zu verschlüsseln, hierzu eignet sich bspw.

TrueCrypt. Weil Microsoft ein US Unternehmen ist, untersteht es dem Patrion Act, der es US Geheimdiensten erlaubt, auf Daten der User, die bei SkyDrive liegen zuzugreifen. Hierfür muss allerdings ein Antrag an Microsoft gestellt werden und dieser Antrag wird von Microsoft überprüft. Nach den NSA Enthüllungen allerdings ist sicher, dass hierauf in der Vergangenheit nicht allzu viel Wert gelegt worden ist, weshalb eine nutzerseitige Verschlüsselung ratsam ist.

4.3.3 Free Space und kostenpflichtige Abonnements

Nutzer von Microsofts SkyDrive erhalten 7 GB Speicherplatz umsonst und bekommen damit vergleichsweise mehr Gratis-Speicherplatz, als bei vielen anderen Cloud Backup Lösungen. Zusätzlichen kostenlosen Speicherplatz erhalten Sie zudem, wenn Sie sich für Microsofts Office 365 Paket entscheiden: Microsoft legt dann 25 GB Speicherplatz oben drauf.

Die bezahlten Abonnements sind bei Microsoft im Vergleich ca. drei Mal günstiger als bei Dropbox und Wuala und laufen jeweils 1 Jahr lang, jedoch gibt es hier einen entscheidenden Nachteil: Das größte buchbare Paket beträgt lediglich 100 GB, womit man inkl. dem Gratis Space auf maximal 107 GB kommt. Diese Eigenschaft dürfte für viele ein K.O. Kriterium darstellen, da eine Bildergalerie des letzten Urlaubs allein schon schnell Größen von mehreren GB einnehmen kann. SkyDrive eignet sich damit am ehesten für die Dokumentverwaltung, womit Microsoft schließlich auch hauptsächlich wirbt.

4.4 Google Drive

Google Drive ist die Cloud Backup Lösung von Google - dies wird bereits aus dem Namen des Dienstes deutlich. Ursprünglich war der Dienst für reine Dokumentenverwaltung ausgelegt und wurde mittlerweile zum vollwertigen Cloud Speicher weiterentwickelt.

4.4.1 Zugriffsmöglichkeiten

Die Funktionen, die zu Zeiten des ehemaligen Dienstes Google Docs möglich waren, waren bereits maßgebend: So konnte man mit Google Drive erstmals Dokumente in einem browsergestützten Tools bearbeiten und erstellen. Das Top Feature dieser Applikation ist die gleichzeitige Bearbeitung von Dokumenten, Tabellen und Präsentation durch mehrere Benutzer gleichzeitig - Und zwar in Echtzeit. Was der Kollege auf seiner Tastatur tippt, sehen die anderen Teilnehmer mit wenigen Augenblicken Zeitverzögerung direkt auf ihrem Bildschirm. Diese Funktionen sind auch heute noch verfügbar und erfreuen sich zunehmender Beliebtheit.

Auch Google Drive wartet mit Desktop Clients und mobilen Apps auf, welcher einen eigenen Google Drive Ordner im Benutzerverzeichnis anlegt, auf dem Ordner und Dateien gedroppt werden können. Diese werden dann sofort mit der Google Drive Online Festplatte synchronisiert. Lediglich für Linux existiert derzeit noch kein Client, ist laut Google jedoch in Planung. Zudem bieten die Desktop Clients einen Offline -Modus. Damit können

Dokumente, Tabellen und Präsentation auch ohne Internetverbindung bearbeitet und angesehen werden. Wird die Verbindung wiederhergestellt, wird erneut synchronisiert. Natürlich gibt es auch ein Web Interface, das direkt mit einem möglicherweise bestehenden Google Konto verknüpft ist und z. B. im Google Chrome Browser schnell und intuitiv erreicht werden kann.

Die Apps für Smartphones und Tablets sind verfügbar für die Betriebssysteme Android und iOS und integrieren sich damit hervorragend in das System Google mit seinen vielen Apps, wie Google Docs, Google Sheets oder Google Keep.

4.4.2 Sicherheit

Wie Dropbox und Microsoft ist auch Google ein US-amerikanisches Unternehmen mit Sitz in Kalifornien. Die jüngsten Aufdeckungen zum NSA Skandal haben aufgezeigt, dass sicher geglaubte Daten schnell an Integrität und Schutz verlieren können, sobald diese die europäischen Grenzen verlassen. Microsoft, Dropbox und Google selbst beteuern hingegen den Schutz der Userdaten. Hier sollte jeder für sich einen Kompromiss finden zwischen dem besten Angebot und größtmöglicher Sicherheit.

4.4.3 Free Space und kostenpflichtige Abonnements

Kostenlos erhalten User bei Google Drive 5 GB Speicherplatz auf der Online Festplatte. Wer mehr Speicherplatz benötigt, hat die Wahl aus einem der vielen Monats-Abonnements. Diese haben jeweils eine Laufzeit von 1 Monat und werden im Voraus bezahlt. Gekündigt werden können diese jederzeit im Web-Interface von Google Drive. Im Gegensatz zu den meisten anderen Cloud Backup Lösungen bietet Google jedoch keine Jahres-Abonnements mit Rabatten an.

4.5 Telekom Cloud: Deutscher Anbieter

Der Cloud Backup Speicher der Deutschen Telekom ist eine spannende Alternative zu vielen internationalen Online Speicher Lösungen. Gerade in der Zeit, in der die jüngsten NSA Aufdeckungen viele Menschen bzgl. Datensicherheit verängstigt, ist der Online Speicher der Telekom besonders interessant geworden. Wer sich für die Telekom Cloud entscheidet, erhält zudem eine T-Online Email Adresse mit E-Mail Postfach automatisch dazu. Ob man diese nutzen möchte oder nicht, bleibt natürlich jedem selbst überlassen.

4.5.1 Zugriffsmöglichkeiten

Die Telekom bietet besonders viele Synchronisationsmöglichkeiten für seine Kunden an. Neben dem üblichen Desktop Client für Windows PC und Mac ist ein Zugriff auch über Smartphone und Tablet möglich (iOS, Android und Windows Phone). So hat man seine Lieblingsbilder, Videos und Musik auch immer unterwegs mit dabei. Zusätzlich dazu existiert

natürlich auch ein Web-Interface, über das man per Browser von überall aus auf seine Daten zugreifen kann.

Spannend sind die zusätzlichen Zugriffsmöglichkeiten per Entertain. Telekom Kunden, die auch das Fernseh-Erlebnis Entertain benutzen, können auch mittels des TV Receivers auf ihre Daten am Fernseher zugreifen. Diese Möglichkeit, seine Daten abzurufen ist bei der Telekom besonders interessant, da man so über den Entertain Receiver ganz einfach auf seine Musik und Videos zugreifen kann, um diese auf dem Fernseher bzw. der daran angeschlossenen HiFi-Anlage zu genießen, ohne lästig externe Geräte an den Fernseher anschließen zu müssen. Der Telekom Cloud Dienst integriert sich damit wunderbar in eine bestehende Entertain Konfiguration und trägt zur zentralen Vernetzung innerhalb Familie und Haushalt bei.

4.5.2 Sicherheit

Die Telekom ist ein Unternehmen mit Sitz in Deutschland und betreibt seine Datencenter auch ausschließlich in Deutschland. Daten, die mittels der Telekom Cloud übertragen werden, werden beim Transfer mit einer 128bit SSL Verschlüsselung übertragen. Auf den Servern der Telekom liegen die Dateien jedoch unverschlüsselt vor.

Hochgeladene Daten werden bei der Telekom doppelt gespiegelt, d. h. auf einem anderen Server noch einmal doppelt abgelegt, so dass bei einem Ausfall des Datencenters die gespeicherten Bilder, Videos und Dokumente nicht ins Datennirvana verschwinden.

4.5.3 Free Space und kostenpflichtige Abonnements

Die Telekom Cloud ist an den Besitz eines T-Online E-Mail Accounts gebunden. Die E-Mail Adresse stellt zugleich den Usernamen dar. Wer noch nicht in Besitz eines Accounts ist, der muss zuvor eine E-Mail Adresse registrieren. Die Telekom bietet für seinen Cloud Backup Dienst derzeit 3 Pakete zur Auswahl, wovon eines der Pakete kostenlos ist.

4.6 Strato Hidrive: Professioneller Anspruch

Strato ist ein Deutscher Spezialist für Online-Speicher, E-Mail, Webhosting und Dedicated Server Lösungen und ist den meisten Benutzern vor allem für seine Webhosting Angebote bekannt. Strato ist insbesondere interessant für Kunden, die einerseits sowieso schon Strato Kunde sind, oder andererseits Wert legen auf zusätzliche Zugriffsmöglichkeiten, wie FTP oder Rsync.

4.6.1 Zugriffsmöglichkeiten

Strato bietet für Windows und Mac einen Desktop Client an, der einen Ordner auf dem System erstellt, der als Synchronisationsordner dient. Daten, die hier hinein gezogen werden, werden automatisch synchronisiert. Außerdem gibt es natürlich auch eine Weboberfläche, über die Sie jederzeit und an jedem Ort Zugriff auf Ihre hochgeladenen

Daten haben und Daten SSL verschlüsselt hochladen können. Sie müssen sich lediglich mit ihrem Benutzernamen und Passwort auf der Strato Website einloggen.

Zugriff haben Benutzer des Strato Hidrive auch über Apps fürs Smartphone und Tablet: Diese stehen für Apple iOS, Android und Windows Phone zur Verfügung.

Besonders interessant sind bei Strato die zusätzlichen Verbindungsprotokolle:

- FTP
- SFTP
- FTPS
- Rsync (auch SSH verschlüsselt)

Damit haben Sie die Möglichkeit, über einen Filemanager wie Filezilla, per bspw. FTP Protokoll auf Ihre Daten zuzugreifen. Dies könnte insbesondere interessant sein für Linux Anwender, da für Linux kein eigener Desktop Client existiert.

Eine besondere Funktion hat sich Strato zum Thema Bilder teilen einfallen lassen. Über die eigens entwickelte Share Gallery ist es dem Benutzer möglich, hochgeladene Bilder mit wenigen Klicks zu einer Galerie zusammenzufassen und diese mit Freunden, Bekannten und Familie in einer hübschen Bildergalerie zu teilen. Auch kann eingestellt werden, ob Fotos heruntergeladen werden dürfen, oder nicht.

4.6.2 Sicherheit

Strato ist ein Deutscher Speicherspezialist, der seine Server auch nur ausschließlich in Deutschland betreibt. Somit entspricht der Datenschutz den strengen Regeln Deutscher Gesetze. Zudem werden die Daten bei Hidrive regelmäßig automatisch gesichert und auf mehreren Rechenzentren verteilt gelagert. Zudem entspricht die Datensicherheit dem TÜV Siegel.

Über die zusätzliche Funktion BackupControl lassen sich zudem Zeitpläne zur automatischen Sicherung der Daten auf seinem PC konfigurieren. Strato ist außerdem einer der wenigen Anbieter, bei dem ein eigener NAS Server Backup erstellt werden kann.

4.6.3 Free Space und kostenpflichtige Abonnements

Strato bietet seinen Mitgliedern einen Gratis Online Speicher von 5 GB mit folgenden Basisfeatures:

- Unlimited Traffic
- Dateien teilen

- Dateimanager
- WebDAV
- BackupControl

Wer mehr Speicher benötigt oder auf das FTP Protokoll nicht verzichten möchte, der wählt aus einem der beiden 3-Monats Abonnements aus. Die bezahlten Abonnements bieten dann zusätzliche Features, wie der Einbindung des Online Speichers als Windowslaufwerk (SMB), dem FTP Protokoll, Rsync u. v. m.

4.7 1&1 (1und1)

1und1 ist ein Anbieter für DSL, Telefon und Mobilfunkverträge und führte jüngst zudem seinen eigenen Online Speicher Dienst ein, der das Produktportfolio sinnvoll ergänzt und abrundet. Anders als bei anderen Anbietern ist 1&1 Online Backup Lösung jedoch ein proprietäres System: Um es nutzen zu können, müssen Sie Inhaber eines 1und1 DSL Tarifes sein.

4.7.1 Zugriffsmöglichkeiten

Der 1und1 Online Speicher bietet keinen separaten Client für den Desktop an. Vielmehr wird der Online Speicher hier als Netzlaufwerk in das bestehende System eingegliedert (Siehe: http://hilfe-center.1und1.de/webdesk-c84786/online-speicher-c84889/1und1-online-speicher-als-netzlaufwerk-in-windows-einbinden-a790223.html), sodass man die Online Festplatte als virtuelle Festplatte im Explorer verwenden kann.

Zudem existieren Apps für Android und iOS (iPhone), mit denen Sie von überall aus Zugriff auf ihre Daten haben. Mittels passwortgeschützter Freigabefunktion können Sie kinderleicht Bilder, Videos, Dokumente und anderen Dateien mit Bekannten teilen.

4.7.2 Free Space und kostenpflichtige Abonnements

Der 1und1 Online Speicher bietet seinen Kunden 25 GB Speicherplatz. Dieser kann zurzeit nicht erweitert werden und ist nur bestehenden 1und1 DSL Kunden zugänglich.

4.8 MEGA

MEGA ist der Nachfolger des One-Click Hosters MegaUpload von Kim Schmitz alias Kim Dot Com, der insbesondere im Jahre 2012 wegen MegaUpload für Aufsehen sorgte. MegaUpload ist inzwischen aufgrund einer Urheberrechtsanklage der USA geschlossen. Seit 2013 existiert nun der neue Dienst MEGA, der mit dem schlechten Ruf von MegaUpload nichts mehr gemeinsam hat. MEGA ist ein reiner Online Speicher Dienst.

4.8.1 Zugriffsmöglichkeiten

Der Zugriff auf den Online Speicher von MEGA erfolgt bisher ausschließlich über die Web-Oberfläche. Ein eigener Client für Desktop Systeme existiert weder für Windows, noch für Mac oder Linux. Jedoch existiert ein Tool namens MegaSync, mit dem es möglich ist, die Daten auf Windows Rechnern zu synchronisieren. Dieses stammt jedoch nicht von MEGA selbst. Auch eine Smartphone App sucht man bei MEGA vergeblich.

4.8.2 Sicherheit

MEGA wirbt insbesondere mit einer hohen Datensicherheit. MEGA selbst hat seinen Sitz in Neuseeland. Laut MEGA werden hochgeladene Daten mindestens auf zwei verschiedenen Rechenzentren gespeichert. Ein besonderer Vorteil bei MEGA ist, dass die Daten bereits auf dem Client mit AES-128 verschlüsselt werden, sodass selbst MEGA keinen Zugriff und keine Einsicht auf die hochgeladenen Daten hat. Damit gehört MEGA zu einem der wenigen Anbieter von Cloud Backup Lösungen, die eine echte End-To-End Verschlüsselung anbieten.

4.8.3 Free Space und kostenpflichtige Abonnements

Als Free User erhält man bei MEGA großzügige 50 GB Speicherplatz. Darüber hinaus existieren 3 Abonnements, die es in sich haben. Damit gehört MEGA zu einem der mit Abstand günstigsten Anbieter von Cloud Backup Speicher. Jedoch muss man auch deutliche Abzüge in Puncto Datenzugriff machen. Da sich MEGA zudem noch in der Beta Phase befindet und derzeit noch nicht geklärt ist, wie mit dem Betreiber Kim Schmitz bzgl. seines anhängenden Gerichtsverfahrens weiter geht, bleibt die Frage offen, ob der Dienst MEGA fortbestehen wird und falls nicht, was dann mit den Daten geschieht.

4.9 Livedrive

Livedrive ist ein Cloud Backup Dienst mit Sitz in England und gibt es in derzeit 3 Varianten: Backup, Brief Case und Pro Suite.

4.9.1 Zugriffsmöglichkeiten

Livedrive bietet mit die umfassendsten Zugriffsmöglichkeiten von allen Anbietern. Desktop Clients existieren sowohl für PC, Mac und Linux. Die Online Festplatte wird direkt als neues Laufwerk im Arbeitsplatz angezeigt (SMB Funktion). Als einer der wenigen Anbieter kann Livedrive auch unter Linux verwendet werden.

Zugriff besteht auch über eine der vielen Apps. Es wird so ziemlich jedes Betriebssystem unterstützt, das derzeit einen halbwegs nennbaren Marktanteil aufweisen kann: iOS, Android, Windows Phone und sogar Blackberry werden unterstützt. Des Weiteren gibt es eine App für Amazons Kindle Fire Tablet. Wird ein Gerät nicht unterstützt, steht unter der Webadresse m.livedrive.com eine für Smartphones und Tablets optimierte Version von Livedrive zur Verfügung.

Außerdem bietet Livedrive natürlich eine Weboberfläche an, mit der u. A. Musik direkt im Browser gestreamt und angehört werden kann. Ein einzigartiges Feature ist zudem der E-Mail Upload. Wer Daten per E-Mail an eine selbstkonfigurierte E-Mail Adresse der Form IhreEigeneAdresse@uploads.livedrive.com schickt, lädt damit automatisch den Anhang in sein Livedrive hoch.

4.9.2 Sicherheit

Livedrive hat seinen Sitz in Großbritannien (England) und betreibt derzeit 3 Rechenzentren ausschließlich in England. Auch Großbritannien ist in die jüngsten NSA Abhörskandale verwickelt, so dass hier jeder für sich selbst entscheiden muss, ob man Livedrive vertrauen mag, oder nicht.

Ansonsten werden hochzuladende Daten mit SSL verschlüsselt übertragen und auf Livedrives Rechenzentren zudem mit AES-256 Bit verschlüsselt gespeichert. Alle Dateien werden auf verschiedenen Rechenzentren verteilt gespeichert, so dass im Falle eines Ausfalls die Daten gesichert bleiben und nicht gelöscht werden. Zudem werden bis zu 30 Versionen der hochgeladenen Daten gespeichert, so dass im Falle eines versehentlichen Überschreibens von Dateien die richtige Version wiederhergestellt werden kann.

Mit Livedrive können Sie zudem Ihren NAS Server absichern und synchronisieren.

4.9.3 Free Space und kostenpflichtige Abonnements

Bei Livedrive gibt es keinen Free Space. Jedoch lassen sich alle kostenpflichtigen Abonnements 14 Tage kostenlos testen (Trial).

4.10 Fabasoft

Fabasoft ist ein Cloud Speicher mit Sitz in Linz, Österreich und legt insbesondere Wert auf Sicherheit der Daten und gehört zu den führenden Anbietern in puncto Datenschutz und Sicherheit. So speichert Fabasoft die Daten ausschließlich auf Rechenzentren in Europa und überträgt die Daten ausschließlich verschlüsselt auf die Online Festplatte.

4.10.1 Zugriffsmöglichkeiten

Der Fabaosft PC Client für Windows, Mac und Linux sorgt für einen reibungslosen Ablauf der Cloud Synchronisation und überträgt die Daten verschlüsselt und automatisch im Hintergrund, ohne dass der Nutzer etwas davon mitbekommt.

Mobile Apps stehen zur Verfügung für Android und iOS, mit denen es leicht möglich ist, Dateien wie z. B. aufgenommene Fotos direkt in die Cloud zu speichern oder in der Cloud gespeicherte Musik direkt auf das Handy zu streamen.

Neben dem Zugriff auf die Online Festplatte über das Webinterface, bietet Fabasoft zudem die Möglichkeit, die Daten über das Netzwerkprotokoll WebDAV zu erreichen.

4.10.2 Sicherheit

In puncto Sicherheit gehört Fabasoft zu den Branchenführern. So kann der Kunde selbst auswählen, in welchem Rechenzentrum innerhalb der EU er seine Daten aufbewahrt haben möchte. Innerhalb des Cloud Speicher können auf Datei und Ordnerebene Berechtigungen für Benutzer- und Benutzergruppen vergeben werden. Der Datentransfer auf die Fabasoft Rechenzentren erfolgt stets verschlüsselt. Zudem ist Fabasoft ISO zertifiziert.

4.10.3 Free Space und kostenpflichtige Abonnements

Fabasoft kann unverbindlich für eine 14 tägige Probephase kostenlos getestet werden. Diese Testphase muss erfreulicherweise nicht extra gekündigt werden. Das Standardpaket enthält Lizenzen für 3 Benutzer und läuft mit 1 Jahr Vertragslaufzeit.

4.11 SugarSync

Ein großer Vorteil des PC Clients von SugarSync ist, dass man selbst festlegen kann, welche Ordner synchronisiert werden soll. Bei den meisten anderen Cloud Backup Lösungen muss ein separater Ordner angelegt werden, in den die zu synchronisierenden Daten gedroppt werden müssen. Dies kann insbesondere bei verschiedenen Dateiformaten unübersichtlich werden. Bei SugarSync hingegen können beliebig viele Ordner auf verschiedenen Dateisystemen markiert werden.

4.11.1 Zugriffsmöglichkeiten

SugarSync bietet seinen Kunden PC Clients für Windows, Mac und Linux an. Mobile Apps existieren für Android, iPhone, iPad, Blackberry, Symbian und Windows Phone. SugarSnyc bildet damit so ziemlich jedes mobile Betriebssystem ab. Zusätzlich dazu kann über eine mobile Version des WebDAV zugegriffen werden.

Als besonderes Feature hat sich SugarSync eine Outlook Integration einfallen lassen. Nutzer von Microsoft Office können SugarSync in Office Outlook mittels Plugin einbinden. Hiermit lassen sich u. a. Dateianhänge mittels Mausklick in den Cloud Speicher aufnehmen und synchronisieren. Außerdem können so auch große Dateianhänge versendet werden, in dem das Plugin einen Link zur Datei auf der Online Festplatte einfügt.

4.11.2 Sicherheit

Für die Sicherheit der gespeicherten Daten sorgt zum einen eine permanente SSL Verschlüsselung der Daten während der Dateiübertragung. Zum anderen werden die gespeicherten Dateien mittels des AES-256 Bit Algorithmus verschlüsselt auf SugarSyncs Servern gespeichert. Zudem existiert eine Versionierung der Dateien bis zu einer Historientiefe von 5 Ebenen. Wenn Sie versehentlich eine Datei überschreiben, lassen sich also bis zu 5 Versionsstände wiederherstellen. SugarSync hat seinen Sitz allerdings in den

USA, Kalifornien. Aufgrund der jüngsten NSA Enthüllungen sollten die Daten bereits auf dem Client durch den Nutzer selbst verschlüsselt werden.

4.11.3 Free Space und kostenpflichtige Abonnements

SugarSync bietet seinen Mitgliedern eine 30 tägige Probephase für alle Abonnements an. Diese muss jedoch nach Ablauf der 30 Tage selbst gekündigt werden, da sonst ein kostenpflichtiges Abo eingegangen wird. SugarSync bietet recht günstige Pakete an und gehört damit zu einem der interessantesten Anbieter.

Abonnements ab 1 TB sind Business Pakete und enthalten u. a. 3 oder mehr User Accounts. Privatanwender können pro eingeladenen Freund zusätzliche 10 GB Free Space erhalten.

4.12 SafeSync

SafeSync ist der Cloud Speicher von TrendMicro, einem japanischen Spezialisten für Software im Bereich Virenschutz, Anti Spam und Internet Content Security.

4.12.1 Zugriffsmöglichkeiten

SafeSync bietet neben dem Zugriff über den Webbrowser (auch in mobiler Version verfügbar) einen PC Client an für die Plattformen Windows, Mac und Linux. Als einen besonders nennenswerten Vorteil des SafeSync Clients gilt, dass der Benutzer 2 Möglichkeiten hat, die Dateien zu synchronisieren. Erstens auf konventionelle Weise, nämlich dass ein separater Ordner angelegt wird, in denen Dateien hineingezogen werden und diese anschließend synchronisiert werden. Der Nachteil dieser Variante ist, dass nicht verschiedene Partitionen eingesetzt werden können, da alle Daten in genau einem Ordner liegen. Bei 500 GB Abonnements kann es da schon mal schwierig werden, genug Plattenplatz zur Verfügung zu haben.

Die zweite und bequemere Variante lässt mehrere zu synchronisierende Ordner zu. Diese werden lediglich im Dateisystem markiert - schon werden die darin befindlichen Dateien synchronisiert, unabhängig vom Speicherort auf der Festplatte.

Apps existieren für Android und iPhone und iPad. Damit ist der Zugriff über das Smartphone gewährleistet und Sie haben Ihre synchronisierten Daten aus dem Cloud Speicher immer mit dabei. Dateien können wie gewohnt verwaltet und geteilt werden. Aufgenommene Fotos können wahlweise auch automatisch synchronisiert werden. Zusätzlich dazu steht ein Offline Modus zur Verfügung, mit dem Dateien auf das Telefon heruntergeladen und ohne Internetverbindung geöffnet werden können.

Außerdem unterstützt SafeSync WebDAV, das nahezu identisch mit FTP ist, jedoch sicherer als das FT-Protocol.

4.12.2 Sicherheit

TrendMicro ist ein führender Anbieter im Bereich Virenschutz und Internet Security und hat eine mehr als 20 jährige Erfahrung in dieser Branche vorzuweisen. Alle Daten werden mittels des AES-256 Bit Verfahren verschlüsselt auf den Rechenzentren von SafeSync gelagert. SafeSync betreibt sein Rechenzentrum in Deutschland und unterliegt damit den Deutschen Datenschutzbestimmungen. Alle Daten werden zum Schutz vor Datenverlust mindestens doppelt auf verschiedenen Systemen gespeichert. Zusätzlich dazu werden bei SafeSync die Login-Versuche und Informationen über Änderungen der Dateien protokolliert und in einer Historie aufgelistet. Sollte sich ein Unberechtigter Zugriff zum Account verschafft haben, fällt dies somit sofort auf.

4.12.3 Free Space und kostenpflichtige Abonnements

SafeSync lässt sich wie SugarSync 30 Tage kostenlos testen. Echten FreeSpace gibt es hingegen -wie auch bei SugarSync- nicht. Alle kostenpflichtigen Abonnements laufen immer mindestens 1 Jahr. Wer sich für einen 2 Jahres Vertrag entscheidet, kann im Vergleich zur 1 jährigen Laufzeit im Schnitt ca. 16% sparen:

5 Spezielle Backup-Lösungen

Neben den allgemeinen Online-Festplatten gibt es noch einige Anbieter, die sich auf die Datensicherung bzw. regelmäßige, automatische Online-Backups spezialisiert haben.

5.1 Mozy

Mozy ist ein reiner Online Backup Service mit umfangreichen Funktionen und einer vorbildlichen Sicherheit und richtet sich sowohl an Privatkunden, als auch Geschäftskunden in den Varianten MozyHome, MozyPro und MozyEnterprise. Die PC Software von Mozy lässt sich sehr leicht zu installieren und gehört mit zu den Stärksten Client Lösungen. Die Daten werden bereits beim Anwender verschlüsselt und auf ISO-zertifizierte Rechenzentren geladen. Auf den Servern bleiben alle Versionsstände der letzten 30 Tage zudem erhalten, sodass versehentlich überschriebene oder gelöschte Dateien innerhalb eines Monats wiederhergestellt werden können.

Weil Mozy ein reiner Cloud Backup Dienst ist, können synchronisierte Dateien nicht geteilt werden, auch Funktionen wie Online Bearbeitung fehlen, die man von Online Speicher gewohnt ist. Zudem ist die maximale Kapazität auf 125 GB begrenzt, kann jedoch in 20GB Schritten kostenpflichtig zugebucht werden.

5.2 Norton Cloud Backup

Der Cloud Backup Dienst vom Sicherheitsexperten Symantec gliedert sich ausgesprochen gut in das bestehende Portfolio aus Virenschutz, Internet Security und Co, ein. Symantec blickt auf über 30 Jahre Erfahrung zurück und gehört zu einem der vertrauenswürdigsten Anbieter von Cloud Backup Diensten.

Bei der Installation der PC Software wird festgelegt, welche Ordner und Dateien gesichert werden sollen, anschließend synchronisiert der Desktop Client alle Dateien automatisch. Mit der PC Suite lassen sich zudem verloren geglaubte oder überschriebene Dateien leicht wiederherstellen. Außerdem können die Daten natürlich über die Weboberfläche abgerufen werden. Ein mobiler Zugriff, etwa über Apps o. Ä. existiert indes jedoch nicht. Ein besonderes Feature des PC Clients ist, dass der PC Client für Windows in Microsoft Office geöffnete Dokumente auch dann synchronisieren kann, wenn sich diese gerade in Bearbeitung finden. Sobald ein Word Dokument oder Excel Sheet während der Bearbeitung gespeichert wird, kann es also synchronisiert werden, obwohl es gerade geöffnet ist.

Was die Sicherheit von Norton Cloud Backup angeht, so lässt sich sagen, dass Norton bereits jahrelang Erfahrungen in dieser Branche innehat und zu den führenden Anbietern zählt. Der Datentransfer zu uns von Nortons Servern erfolgt stets verschlüsselt und auch auf den Rechenzentren von Nortons Cloud Speicher werden die Daten ständig verschlüsselt gespeichert, so dass nicht einmal Symantec Zugriff auf die Daten hat. Zudem steht eine Versionshistorie für die Daten in einem Verlauf von 90 Tagen zur Verfügung.

Das Bezahlsystem von Nortons Cloud Backup Lösung ist transparent und simpel. Standardmäßig erhält man für 3,33 € 25GB Speicherplatz und kann damit bis zu 5 Computer sichern. Eine Speichererweiterung ist für weitere 3,33 € möglich. Diese erweitert den Speicherplatz um weitere 25 GB. Die Vertragslaufzeit beträgt bei Norton immer 1 Jahr.

5.3 Carbonite

Carbonite ist ein Cloud Backup Service mit Sitz in den USA, der seinen Kunden einen besonderen Service bietet: Der Speicherplatz ist unbegrenzt. Jedoch gibt es einen kleinen Haken. Die automatische Synchronisierung des Backups erfolgt nur für bestimmte Dateitypen. Dies sind Dokumente, E-Mails, Musik, Bilder und Systemeinstellungen. Andere Dateiformate müssen manuell zum Carbonite Online Speicher übertragen werden. Ab einem verbrauchten Speicherplatz von 200 GB wird die Übertragungsgeschwindigkeit zudem gedrosselt.

Zugriff auf die Dateien erhält man bei Carbonite neben dem Zugang zum Web Interface hauptsächlich über die PC Software, die für Windows und Mac erhältlich ist. Diese synchronisiert die oben genannten Dateiformate automatisch mit der Online Festplatte und

hält diese immer up to date. Außerdem existieren für Android, iPhone, IPad, IPod Touch sowie Blackberry Apps, mit denen ein mobiler Zugriff auf die Dateien sichergestellt ist.

Carbonite ist unter den Cloud Backup Lösungen einer der wenigen Anbieter, die ihren Nutzern eine End-To-End Verschlüsselung anbieten kann. Das bedeutet, dass die zu synchronisierenden Daten bereits beim Benutzer mit der 128 Bit Blowfish Verschlüsselung verschlüsselt werden, anschließend mit Secure Socket Layer (SSL) verschlüsselt übertragen werden und auch auf Carbonites Servern verschlüsselt gelagert sind.

Carbonite gibt es für Privat- als auch Geschäftskunden in verschiedenen Varianten. Für Privatkunden stehen 3 Pakete zur Auswahl, die sich hinsichtlich der gebotenen Funktionen leicht unterscheiden und 30 Tage lang kostenlos testen lassen.

5.4 Dogado

Dogado ist ein Deutscher Cloud Speicher und bietet seinen Kunden umfassende Möglichkeiten, ein automatisches Online Backup einzurichten, um seine Daten vor Datenverlust zu schützen. Dogado gibt es zurzeit in vier Varianten, nämlich Home, Professional, Office und Enterprise, wobei Office und Enterprise zusätzlich die Möglichkeit bieten, mehr als nur einen PC abzusichern. So können mit dem Office Paket zwei Computer gesichert werden, 5 Computer können mit dem Enterprise Abonnement gesichert werden.

In puncto Sicherheit lässt Dogado keine Wünsche offen. Zunächst werden die Daten bereits lokal beim Anwender mit dem AES-256 Bit Algorithmus verschlüsselt und anschließend per SSL sicher zum Server übertragen. Dogado speichert die Daten auf zwei Rechenzentren verschlüsselt ab und hat auch keinerlei Zugriff auf das Passwort, mit dem verschlüsselt worden ist. So ist sichergestellt, dass nicht einmal Dogado Zugriff auf die Daten hat. Da Dogado zudem ein deutsches Unternehmen ist, unterliegt es den strengen Regeln Deutscher Datenschutzgesetze und gehört damit zu den sichersten Anbietern von Cloud Backup Lösungen.

Dogado ist insbesondere für Geschäftskunden interessant, weil Dogado durch seinen Sitz in Deutschland und den umfassenden Sicherheitskonzepten ein ausgesprochen seriöser Anbieter von Cloud Backup Lösungen ist. Zum anderen sind mit Dogado auch sehr umfassende Absicherungsmöglichkeiten gegeben, wie z. B. dem Backup von Server Systemen, MS SQL und Oracle Backup und der Absicherung von ganzen Computersystemen, uvm.

Da Dogado ein ausschließlicher Cloud Backup Service ist, gibt es keine Zugriffsmöglichkeit über eine App fürs Smartphone. Der Zugriff auf die Daten ist über den PC Client für Windows XP, Vista, 7, Linux, Unix, Novell und Mac OS X möglich sowie über die Weboberfläche. Mittels des PC Clients kann die Sicherung einfach und intuitiv konfiguriert werden. Einmal aufgesetzt, synchronisiert Dogado die Daten automatisch im Hintergrund.

Ein besonderer Vorteil von Dogado ist, dass die Vertragslaufzeit bei allen Paketen nur einen Monat beträgt und jeweils mit einer Kündigungsfrist von 30 Tagen kündbar ist. Auch die Bezahlung erfolgt monatlich.

6 Fazit

Viele Menschen fragen sich, wofür Sie eine Online Festplatte überhaupt einsetzen sollten - Ist die heimische Festplatte auf PC oder Laptop doch meist groß genug, alle Daten aufzunehmen. Und wenn der Plattenplatz einmal nicht mehr reicht, kauft man sich eben eine neue Festplatte. Genau an diesem Punkt setzen Cloud Backup Lösungen aber an: Sie bieten Terabyte-große Kapazitäten an Festplattenplatz zu bezahlbaren Preisen (Ab 20 € für 2 TB) an, so dass es mittlerweile zur ernsthaften Alternative geworden ist, Festplattenplatz zu mieten, anstatt zu kaufen. Dies bringt viele Vorteile mit sich.

6.1 Sicherheit gegen Datenverlust

Erstens ist es im Hinblick auf Datenverlust um einiges sicherer, die Daten auf externen Servern zu speichern. Die Dateien werden bei Cloud Backup Lösungen mindestens zwei Mal auf verschiedenen Rechenzentren an unterschiedlichen Standorten gesichert, um bei Ausfall oder Zerstörung eines Rechenzentrums trotzdem alle Dateien wiederherstellen zu können. Fällt hingegen Ihre heimische Festplatte aus, wird gestohlen oder z. B. aufgrund von Brand-, Wasser- oder Sturmschäden zerstört, sind die Daten weg.

6.2 Zugriff von überall

Zweitens werden per Online Speicher synchronisierte Dateien zentral gelagert, d. h. Sie können von überall darauf zugreifen, ohne den PC, das Notebook oder die externe Festplatte mitschleppen zu müssen (was wiederum ein Transportrisiko darstellt). Außerdem sind sie bei der Lagerung auf einer Festplatte zuhause darauf angewiesen, dass der PC ständig läuft. Er fungiert dann also als Server, der rund um die Uhr laufen muss und nicht unerhebliche Stromkosten (von den Anschaffungskosten abgesehen) verursacht. Für Cloud Speicher genügt hingegen ein Internetanschluss, um Ihre Daten von überall aus abzurufen. Sogar per Smartphone oder Tablet können heutzutage auf die Daten zugegriffen werden, denn so gut wie jeder Anbieter bietet Apps für den Zugriff auf den Cloud Speicher an. So wäre es z. B. kein Problem, synchronisierte Musik und Videos auch unterwegs, z. B. auf Reisen, zu streamen.

6.3 Viel Bandbreite notwendig

Einen Nachteil hingegen haben Cloud Speicher: Wer häufig große Dateien, die viel Speicherplatz benötigen, synchronisiert, der braucht dafür auch den passenden Internetanschluss. Ein MP3 Musikalbum (ca. 100 MB) oder die Bildergalerie vom letzten Urlaub vom Cloud Speicher wieder herunterzuladen dauert bei einem DSL 6000 Anschluss meist keine 2 Minuten. Soll es hingegen ein ganzer Film in Full HD sein (ca. 10 GB), bewegt man sich bereits im Rahmen von etwa 3,5 Stunden. Um einen Full HD Film unterwegs streamen zu können, muss mindestens mit DSL 25 Mbit oder mobil mit LTE heruntergeladen werden, damit es zu keinen Aussetzern kommt.

6.4 Backups

Da die allermeisten Nutzer Cloud Backup Lösungen sowieso nur meist deshalb benutzen, um Ihre Daten abzusichern, wobei die Geschwindigkeit des Backups dann kaum eine Rolle spielt. Da die Desktop Clients die Daten sowieso im Hintergrund synchronisieren und dies auch häppchenweise geschehen kann, fällt der Upload Prozess nicht einmal auf.

Bildquelle: PixelEmbargo / bigstockphoto.com