Cloud-Speicher
Proseminar Speicher- und Dateisysteme
SoSe 2012

Agnes Marcol
Betreuerin: Michaela Zimmer

Abgabetermin: 30. September 2012

Contents

1 Cloud-Speicher allgemein **2**
Was ist eigentlich die Cloud? . . . 2
Möglichkeiten und Vorteile . . . 2
Nutzer und Anbieter . . . 3
Cloud-Arten . . . 3

2 Funktionalität anhand von konkreten Beispielen **5**
Grundbegriffe . . . 5
Dropbox . . . 7
Ubuntu One . . . 9
Team Drive . . . 10
Die 3 Anbieter im Überblick . . . 14

3 Cloud-Sicherheit **14**
Was gilt es zu schützen? . . . 14
Vor wem und vor was sollte geschützt werden? . . . 15
Sicherheitslücken bei den Anbietern . . . 16

1 Cloud-Speicher allgemein

Was ist eigentlich die Cloud?

Der Begriff "Cloud" ist eines der ältesten Sinnbilder der Informationstechnik und beschreibt einen virtuellen Bereich innerhalb von Rechnernetzen. Dabei spielt das Innerste und der Bestimmungsort der zur Verfügung gestellten IT-Infrastruktur für den Benutzer in erster Linie keine Rolle und ist ihm meistens unbekannt oder kann nicht ohne weiteres identifiziert werden, sie scheint ihm wie in einer "Wolke" verhüllt.

Cloud-Computing ist dabei der Oberbegriff, hierbei werden Dienstleistungen der Informationstechnik (Infrastruktur, Rechenleistung, Speicherplatz, Plattformen, Software) meist über das Internet zur Verfügung gestellt. Eine solche Dienstleistung des Cloud-Computing ist der Cloud-Speicher (Storage-as-a-service). Hierbei wird Speicherplatz an die Benutzer vermietet, die Cloud dient dabei als Ablageort für Daten und Dateien der Benutzer.

Möglichkeiten und Vorteile

Der Benutzer kann Daten, Dateien und Programme in der Cloud ablegen und bearbeiten, somit kann der Cloud-Speicher für **Datensicherung und Backup** genutzt werden. Dadurch kann sich der Benutzer vor Datenverlust schützen, da seine Daten nicht mehr nur lokal auf dem Rechner zu Hause gespeichert sind, sondern auch in der Cloud bereit stehen. Ausserdem ist der Zugriff auf die eigenen Daten von einem beliebigem Gerät mit Internetzugang möglich, z.B. über einen Browser oder einen Anbieter speziellen Cloud-Client.

Es können auch mehrere Benutzer mit entsprechender Autorisierung gemeinsam auf die Daten zugreifen und diese bearbeiten (**Filesharing**). Dadurch kann man z.B. Dokumente oder Fotoalben für andere Nutzer zugänglich machen und muss diese nicht als Anhang in Emails verschicken.

Einige Anbieter bieten auch die Möglichkeit der **Versionsverwaltung**, die besonders beim Programmieren erforderlich ist, da so mehrere Personen ohne räumliche Bindung gemeinsam und parallel an einem Projekt arbeiten können, ohne das es ungewollt zu Dateiüberschreibungen kommt.

Auch die Möglichkeit der **Synchronisation** sollte nicht unerwähnt bleiben, hierbei kann der Benutzer seine unterschiedlichen Geräte untereinander synchronisieren, indem diese Geräte auf die Informationen in der Cloud zugreifen. Somit ist jedes Gerät auf dem aktuellen Stand ohne häufige manuelle Synchronisation, vorausgesetzt es besteht eine Verbindung zum Internet.

Immer mehr Anbieter erweitern ihr Angebot und bieten **Musik-Streaming** an. Dabei wird in der Regel zunächst festgestellt, welche Musik der Nutzer besitzt und ob diese in der Datenbank des Anbieters vorhanden ist. Die Titel, die übereinstimmen kann der Nutzer dann auf seinen Geräten über die Cloud beziehen und muss sie somit nicht lokal gespeichert haben.

Möglichkeiten und Vorteile des Cloud-Speichers zusammengefasst:

- Datensicherung, Copy, Backup - Schutz vor Datenverlust, keine Beschaffung und Wartung von Hardware, Zugriff auf eig. Daten von beliebigen Geräten
- Versionsverwaltung - gemeinsames Arbeiten an Projekten
- automatische Synchronisation - keine manuelle Synchronisation
- Filesharing - Zugriff für mehrere Benutzer
- Musik-Streaming - spart Speicherplatz auf mobilen Geräten

Nutzer und Anbieter

Grundsätzlich kann zwischen dem Cloud-Nutzer, dem Cloud-Anbieter und den Ressourcen-Anbietern unterschieden werden. Der Cloud-Nutzer ist die Stelle, die Rechenleistung von Cloud-Diensten in Anspruch nimmt. Der Cloud-Anbieter stellt diese Dienste dem Cloud-Nutzer bereit und kann sich von den Ressourcen-Anbietern unterscheiden. Der Ressourcen-Anbieter stellt dem Cloud-Anbieter für die Cloud-Datenverarbeitung seine Hard- oder Software zur Verfügung, damit diese zusammengefasst dem Nutzer angeboten werden kann.

Um das Nutzer-Anbieter-Verhältnis zu veranschaulichen dient folgendes Beispiel: Eine Person (der Cloud-Nutzer) nutzt die Dienstleistung von Dropbox (Cloud-Anbieter). Hierbei ist Amazon der Ressourcen-Anbieter für Dropbox, denn die nutzen die Amazon Web Services.

Cloud-Arten

Cloud-Ressourcen können als Public oder Private Clouds zur Verfügung gestellt werden, dabei unterscheiden sich die beiden Formen nicht technisch, sondern vor allem organisatorisch.

Private Clouds sind vernetzte Rechner, die unter der rechtlichen Verantwortung einer einzigen Daten verarbeitenden Stelle stehen. Als Private Clouds werden auch Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen bezeichnet, z.B. Stellen der öffentlichen Verwaltung oder eines Unternehmenskonzerns.

Hierbei befindet sich der Anbieter und der Nutzer im selben Unternehmen bzw. gehört der selben öffentlichen Stelle an, was die Sicherheitsrisiken in Bezug auf die Daten verringert. Organisation und Betrieb werden innerhalb der zuständigen Stelle abgewickelt. Der Zugang ist beschränkt auf Mitarbeiter und autorisierte Personen und erfolgt in der Regel über ein Intranet bzw. eine Virtual Private Network-Verbindung. Im Unterschied zu öffentlichen Clouds sind Private Clouds bei Netzbandbreite und Verfügbarkeit nicht eingeschränkt. Sie bieten dem Anbieter und dem Nutzer mehr Kontrolle sowie einen besseren Ausfallschutz.

Eine besondere Form von In-House Clouds als Private Clouds sind virtualisierte Desktops mit einem Betriebssystem der verantwortlichen Stelle, auf das Mitarbeiter über Thin Clients, mobile Laptops oder PCs zugreifen und hierüber Daten verarbeiten können.

Bei **Public Clouds** wird die Rechenleistung von Dritten im Sinne des Datenschutzrechtes (§ 3 Abs. 8 S. 2 BDSG) angeboten.

Die Ressourcen-Anbieter dieser Public Clouds sind meistens große globale IT-Unternehmen wie Amazon (EC2), Google, Microsoft, IBM oder Hewlett-Packard (zusammen mit Intel und Yahoo). Die Daten der Cloud-Nutzer werden auf weltweit verteilten Servern bzw. Serverfarmen gespeichert und verarbeitet. Die Server und teilweise auch die Software wird von den Ressourcen-Anbieter an die Cloud-Anbieter wie z.B. Dropbox vermietet, die wiederum ihre Cloud-Dienste mit eigener Client-Software an den Cloud-Nutzer verkaufen/vermieten.

Neben den kommerziellen Public Cloud Angeboten gibt es öffentliche, zumeist akademische Einrichtungen wie z.B. Universitäten, die Cloud Computing zur Verfügung stellen.

Hybride Clouds sind eine Mischung von Private- und Public Clouds, also eine Nutzung sowohl von eigenen wie auch fremden Ressourcen. Hybride Clouds ermöglichen bei Auslastung der internen Rechnerwolke die Ausweichung auf eine öffentliche. Die Herausforderung dabei ist die Integrierung von IT-Umgebungen, Private Cloud und Public Cloud auf der Applikations-, der Middleware- und der Infrastruktur-ebene in Bezug auf Services, Sicherheit und Nutzbarkeit.

Eine Besonderheit stellen die **Community Clouds** dar, bei denen eine Cloud-Infrastruktur gemeinsam genutzt wird, wobei gemeinsame Anforderungen, z.B. zur Sicherheit, zum Datenschutz oder zu weiteren Compliance-Anforderungen kollektiv vereinbart und festgelegt werden.

Hierbei schließen sich Unternehmen oder Organisationen der gleichen Branche zusammen und bilden aus ihren Private Clouds die Community Cloud, die dann nur den Mitgliedern der Community zugänglich sind. Solche Clouds bieten sich überall dort an, wo Unternehmen oder Organisationen gleiche Anforderungen und Aufgaben haben und die gemeinsame Nutzung der vorhandenen Infrastruktur anstreben.

Ein Vorteil der Community Cloud ist die Reduzierung des Kapazitätsbedarfs durch gemeinsame Nutzung von Ressourcen und Anwendungsprogrammen.

2 Funktionalität anhand von konkreten Beispielen

Im folgenden Abschnitt wird die Funktionalität der Public Cloud Anbieter anhand von 3 konkreten Beispielen erläutert. Die Anbieter Dropbox, Ubuntu One und Team Drive werden dabei unter den Kriterien Funktionsweise, Angebot und Datenschutz verglichen.

Auf den Punkt **Datenschutz** der jeweiligen Anbieter wird im 3. Abschnitt dieser Ausarbeitung **Cloud-Sicherheit** unter dem Punkt **Sicherheitslücken** noch mal genauer eingegangen.

Um die genaue Funktionsweise beschreiben zu können, müssen vorher einige Grundbegriffe und Services erläutert werden, die für die Beschreibung später verwendet werden.

Grundbegriffe

DeduplizierunRegelm

Bei der Deduplizierung geht es darum redundante Daten zu erkennen und zu beseitigen bevor sie abgespeichert werden. In Verbindung mit dem Nutzen eines Cloud-Speichers dient dieser Prozess zur Komprimierung der Datenmenge des Cloud-Nutzers, die auf den Servern des Cloud-Anbieter gespeichert wird.

Block-Level-Deduplizierung Daten bzw. der Datenstrom wird in Datenblöcke zerlegt, die meistens 512 Byte beinhalten. Jedem Block wird durch eine Hash-Funktion ein eindeutiger Hash-Wert zugewiesen, der wie ein Fingerabdruck den Block identifizieren kann (Fingerprinting). Wenn Daten nun wiederholt vorkommen zeigt sich das indem einige der Blöcke den selben Hash-Wert haben. Das wird erkannt und durch Referenzierung auf den bereits gespeicherten Block entsteht ein kompakter "Bauplan" durch den der ursprüngliche Datenstrom wieder hergestellt werden kann. Weisen die Dateien nur geringfügige Änderungen auf, dann werden nur die Unterschiede, die zwischen den Dateien bestehen, gespeichert. Da identische Blöcke nicht nur innerhalb einer Datei auftreten können, sondern potenziell in unterschiedlichsten Informationen gefunden werden, sind hohe Kompressionsraten möglich die Speicherplatz reduzieren.[1]

File-Level-Deduplizierung Ähnlich wie bei der Block-Level-Deduplizierung, nur das hierbei die Dateien nicht in Blöcke zerteilt werden, sonder jede einzelne Datei einen Hash-Wert zum vergleich mit anderen Dateien erhält. Die Kompressionsraten ist wesentlich geringer als bei der Block-Level Variante, da nur die gesamte Datei verglichen wird.[1]

Amazon Web Services (AWS)

Eine Sammlung von Webservices, die von Amazon im Internet als Cloud-Lösung anbietet. Amazon Web Services wurde im Juli 2002 als Dienst für andere Webseiten oder Client-seitige Anwendungen gestartet. Die Dienstleistungen werden großteils über HTTP transportiert, wobei auch andere Protokolle genutzt werden können (SOAP, REST). Nach Angaben von Amazon haben sich bereits über 490.000 Entwickler für die Nutzung von AWS registriert (Stand 25. Februar 2009).[2]

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3) gehört zu den Webservices von Amazon. S3 ist ein File Hosting Service, der dem Kunden erlaubt Dateien über das Internet auf einem zentralen Datenspeicher (Servern von Amazon) abzulegen, zu bearbeiten und zu löschen. Die Daten werden hierbei in Buckets organisiert und können mit einem individuellen Schlüssel, einem Namen der vom Entwickler festgelegt wird und amazonweit nur ein einziges Mal vorkommen darf, abgerufen werden. Da Buckets auch als URLs adressiert werden können, gibt es für diese Buckets zusätzlich noch Beschränkungen bei der Zeichenauswahl im Namen. Beim Erzeugen des Links muss auch angegeben werden, wie lange dieser verfügbar sein soll.

> Beispiel für die URL eines hochgeladenen Objektes:
>
> Eine Datei "wolke.txt" in einem Bucket "cloud" wäre unter folgendem Link erreichbar: http://cloud.s3.amazonaws.com/wolke.txt

Jeder Benutzer darf maximal 100 Buckets benutzen, die nicht ineinander geschachtelt werden können. In diesen Buckets können jedoch beliebig viele Dateien abgelegt werden, die mindestens ein Byte und maximal 5 TB groß sein dürfen. Wichtig ist auch hier wieder die Eindeutigkeit des Dateinamens innerhalb eines Buckets. Neben der eigentlich gespeicherten Datei enthält ein S3-Objekt auch noch Metadaten wie z.B. Content Type und Datum der letzten Veränderung.

Der Nutzer kann auswählen, in welcher Region die Daten auf den Servern von Amazon gehostet werden sollen, was Auswirkung auf Preis und Zugriffsgeschwindigkeit hat. Zur Zeit stehen die Regionen USA (Northern Virginia, Pacific Northwest, Oregon, Nordkalifornien), EU (Irland), Asien (Singapur, Tokio) und Südamerika (Sao Paulo) zur Verfügung. Ausserdem bietet Amazon noch die GovCloud (US) an, die speziell auf die Bedürfnisse von Ämtern und Behörden in den USA zugeschnitten ist. Dateien, die in einer Region gespeicherte sind, können nur vom Kunden direkt in eine andere Region übertragen werden. Das stellt sicher, dass gespeicherte Daten in der EU auch in jedem Fall in der EU verbleiben, was für den Datenschutz von Bedeutung ist.

Der direkte Zugriff auf die Daten ist über folgende Protokolle möglich:

HTTP Hypertext Transfer Protocol, Standard-Download-Protokoll von S3, ein allgemeines Protokoll zur Datenübertragung im Rahmen des World Wide Web[1]

SOAP Simple Object Access Protocol, ein von Microsoft entwickeltes Kommunikationsprotokoll für den Zugang zu einzelnen Projekten im Internet[1],

REST Representational State Transfer, ein Architekturstil mit dem Webservices realisiert werden[1]

BitTorrent ein kollaboratives Filesharing-Protokoll für Sharing von großen Dateien[1]

Es gibt auch Open-Source-Implementierungen wie **JetS3t** (Java), die die Interaktion mit S3 direkt innerhalb einer Programmiersprache ermöglichen.

Dropbox

Das Unternehmen Dropbox Inc. wurde 2007 in den USA gegründet, seit September 2008 ist der Cloud-Speicher von Dropbox erhältlich und zur Zeit einer der führenden Cloud-Anbieter Weltweit. Die Software ist auch auf Deutsch verfügbar, Kundenservice und Online Hilfe jedoch nur in Englisch möglich.

Dropbox bietet die Möglichkeit der Online-Datensicherung, Synchronisation und das Teilen der Daten mit anderen Nutzern.

Funktionsweise

Durch die Installation des Dropbox-Clients, der für die Betriebssysteme Windows, Mac OS X, Linux, iOS, Android und Blackberry verfügbar ist, wird auf dem Gerät ein neuer Ordner erstellt: die Dropbox. Alle darin gespeicherten Dateien werden bei bestehender Internet-Verbindung auf einen zentralen Server kopiert, als zentrales Speichersystem nutzt Dropbox den Amazon Web Service S3, somit findet die Speicherung auf den Amazon Servern in den USA statt. Durch die Nutzung der Block-Level-Deduplizierung werden bei Änderungen innerhalb einer Datei nur die geänderten Bereiche übertragen. Früher fand die Block-Level-Deduplizierung Nutzer übergreifend statt, da dies jedoch durch das Programm Dropship zweckentfremdet wurde, ging Dropbox zur Single-User-Deduplizierung über.

Nach der Installation des Clients werden alle Daten ständig mit dem Server synchronisiert, so das der Zugriff auf aktuelle Daten von mehreren Geräten über den Client oder auch den Webbrowser möglich ist.

Dateien können auf drei Arten mit anderen geteilt werden:

Öffentlich über den *Public Folder*, ein öffentlich erreichbares Verzeichnis, jeder hat über dieses Verzeichnis Zugriff auf alle enthaltenen Daten.

URLs mit *Public Links*, hierbei wird eine codierte URL für einzelne Dateien erstellt, die man dann weitergeben kann, eine Löschung der URL ist jederzeit möglich.

Dropbox User über die *Shared Folder*, Verzeichnisse können ausschliesslich mit anderen Dropbox Nutzern geteilt werden, so das jeder Nutzer Änderungen an den Dateien durchführen und neue Dateien hinzufügen kann, bei Konflikten durch konkurrierende Versionen werden diese separat abgespeichert.

Ein Versionsverwaltungssystem wie bspw. Git bietet Dropbox nicht. Jedoch gibt es die Möglichkeit auf vorherige Versionen von gelöschten oder überschriebenen Dateien zuzugreifen. Bei einer der Pro Versionen, oder für 40,-$ pro Jahr, ist die Wiederherstellung zeitlich nicht beschränkt, in der kostenlosen Version ist dies bis zu 30 Tagen möglich. Zu einer Besonderheit zählt das automatische erstellen von Fotogalerien aus speziellen Bilderordnern namens *Photos*, die man dann auch verlinken und veröffentlichen kann.

Kosten und Volumenangebot

Im Juli 2012 hat Dropbox seine Preismodelle umfassend geändert, eine Liste der aktuellen Preise und Produktvarianten:

Produkt	Volumen	Kosten pro Monat	Kosten als Jahres-Abo
Kostenlos	2 - 8 GB	-	-
Pro 100	100 GB	9,90 $ (ca. 8,- €)	99,99 $ (ca. 80,- €)
Pro 200	200 GB	19,90 $ (ca. 16,- €)	199,- $ (ca. 160,- €)
Pro 500	500 GB	49,90 $ (ca. 40,- €)	499,- $ (ca. 400,- €)

Der Preis von Dropbox liegt durchschnittlich mit 0,10 $ (ca. 8 Cent) pro GB im Monat im Mittelfeld der Angebote. Durch das Weiterempfehlen von Dropbox an Freunde kann man sein Datenvolumen pro geworbene Person kostenlos um 250 MB erweitern, bis hin zu maximal 8 GB. Generell ist das kostenpflichtige maximale Volumen unbegrenzt. Für grösseren Speicherbedarf gibt es Dropbox für Teams, es beginnt ab 1000 GB Speicherplatz für 5 Benutzer für 795,- $ pro Jahr und lässt sich mit 200 GB für jeden weiteren Benutzer erweitern.

Sicherheit, Verschlüsselung und Transfer

Befinden sich die Daten in dem Dropbox Ordner auf ihrer lokalen Festplatte, so findet von Seiten des Dropbox-Clients keine lokale Verschlüsselung statt. Dafür kann der Benutzer aber selbständig durch Verschlüsselungsprogramme wie z.B. TrueCrypt sorgen, jedoch stehen durch die Verschlüsselung vor dem Hochladen einige Funktionen nicht mehr zur Verfügung, wie zum Beispiel das Herstellen öffentlicher URLs. Bei Verlust des eigenen Verschlüsselungsschlüssel ist natürlich eine Wiederherstellung durch Dropbox nicht mehr möglich.

Die Datenübertragung zwischen dem lokalen Desktop-Clients von Dropbox und den Servern findet mit einer 256-Bit-SSL (Secure Sockets Layer)-Verschlüsselung statt. Auch bei den mobilen Dropbox-Apps, die diese Funktion unterstützen, wird bei dem Datenaustausch eine 256-Bit-SSL -Verschlüsselung genutzt. Dabei ist zu beachten, dass nicht alle mobilen Mediaplayer verschlüsseltes Streaming unterstützen, daher sind von den Servern gesendete Media-Dateien nicht immer verschlüsselt.[4]

Nach dem Hochladen der Dateien findet auf den Servern eine AES-256-Verschlüsselung statt, der Verschlüsselungsschlüssel wird von Dropbox verwaltet und der Kunde hat keinen Zugriff darauf.

Dropbox verwendet zur Datenspeicherung Amazon S3, es werden redundante Back-ups aller Daten an verschiedenen Stellen, also auf Servern in mehreren großen Datencentern, gespeichert. Laut Amazon wird für die physisch Sicherheit durch Videoüberwachung und professionelles Sicherheitspersonal in Militärqualität gesorgt.[2]

Dropbox gibt auch an, erhebliche Schutzmaßnahmen gegen Netzwerksicherheitsprobleme wie DDoS-Angriffe (Distributed Denial of Service, Nichtverfügbarkeit eines Dienstes), MITM-Angriffe (Man in the Middle, unbefugte Einsicht und Manipulation von

Daten durch einen “Mittelsmann”) oder Packet Sniffing (Software zur unbefugten Netzwerkanalyse) zu ergreifen, welche das genau sind, wird nicht mit angegeben.[4]

Da sowohl die Server als auch der Hauptsitz von Dropbox sich in den USA befinden, gilt der Datenschutz der Vereinigten Staaten, dieser ist rechtlich kaum durch Gesetze oder andere Vorschriften geregelt.[3]

Ubuntu One

Ubuntu One ist seit Mai 2009 in dem Open Source Betriebssystem Ubuntu integriert. Das Unternehmen Canonical mit Sitz auf der Isle of Man ist maßgeblich an der Entwicklung des Betriebssystems Ubuntu und des Cloud-Speichers Ubuntu One beteiligt. Die Ubuntu One Webseite sowie eine Online Hilfe und ein Forum sind in englischer Sprache vorhanden. Auch der Ubuntu One Client ist Open Source Software, lediglich die Serversoftware ist proprietärer Software, die eine Änderung nicht erlaubt.

Ubuntu One bietet die Möglichkeit der Datensicherung, der Synchronisation von mehreren Geräten und das Teilen seiner Daten mit anderen Personen.

Funktionsweise

Seit 2011 ist eine Client-Software auch für die Betriebssysteme Windows, Android und iOS erhältlich, der Zugriff über einen Webbrowser ist ebenfalls möglich. In Ubuntu ist der Ubuntu One Ordner im Benutzerverzeichnis integriert, für den Betrieb unter Windows muss man eine Software installieren, die dann lokal einen Ubuntu One Ordner erstellt, auf den man über den Explorer zugreifen kann. Für den Zugriff unter Android und iOS gibt es Apps in den jeweiligen Stores. Nach der Installation werden bei bestehender Internet-Verbindung alle Daten, die in dem Ubuntu One Ordner abgelegt werden mit Hilfe des Ubuntu One Clients auf die Server übertragen. Ubuntu One nutzt wie Dropbox den Web Service S3 von Amazon und arbeitet mit Single-User-Deduplizierung, die Deduplizierung ist auf File-Level-Ebene implementiert, wenn kleine Änderungen an einer Datei vorgenommen werden, wird die gesamte Datei neu auf den Server kopiert. Die Datenbank mit Metadaten für die einzelnen Benutzer befindet sich auf Amazon Servern in den USA, die eigentliche Datenspeicherung erfolgt auf anderen Servern, deren Region von Ubuntu One nicht öffentlich angegeben wird.

Mehrere Geräte können mit dem Ubuntu One Ordner verbunden werden, so dass der Client alle Daten in dem Ordner auf allen Geräten synchronisiert, dabei werden Konflikte erkannt und nur die gelöscht, die nicht durch aktuelle Änderung des Benutzers entstanden sind. Bei der Nutzung des Ubuntu Betriebssystems können auch Kontakte und Notizen, die mit der Software Tomboy erstellt wurden, über Ubuntu One synchronisiert werden.

Das Teilen seiner Daten mit Anderen ist über zwei Wege möglich:

URLs es kann eine URL erstellt werden, es kann festgelegt werden, ob die Daten nur angesehen oder auch editiert werden dürfen.

Ubuntu One User es können andere Ubuntu One Benutzer zum Teilen von Daten und Ordnern ausgewählt werden, auch hier kann man Lese- und Schreibrechte vergeben.

Eine Versionsverwaltungssoftware oder die Möglichkeit geänderte oder gelöschte Objekte wieder herzustellen ist nicht vorhanden.

Eine Besonderheit ist das kostenpflichtige Musik Streaming Angebot von Ubuntu One, hierbei stehen dem Benutzer 20 GB Speicherplatz für eigene Musik zur Verfügung. Diese kann dann nach der Speicherung auf dem Ubuntu One Server bei bestehender Internet-Verbindung auf einem iOS oder Android fähigem Mobilgerät gestreamt werden.

Kosten und Volumenangebot

Eine Liste der aktuellen Preise und Produktvarianten:

Produkt	Volumen	Kosten pro Monat	Kosten pro Jahr
Ubuntu One	5 GB	-	-
extra Speicherplatz	20 GB	2,99 $ (ca. 2,40 €)	29,99 $ (ca. 23,80 €)
Musik Streaming	20 GB	3,99 $ (ca. 3,20 €)	39,99 $ (ca. 31,70 €)

Der durchschnittliche Preis von Ubuntu One liegt mit 0,14 $ (ca. 11 Cent) pro GB im Monat auch im Mittelfeld. Das maximale Volumen ist unbegrenzt und jeweils in 20 GB Paketen erweiterbar.

Sicherheit, Verschlüsselung und Transfer

In dem Ordner werden die Daten vor dem Hochladen nicht automatisch verschlüsselt, dafür muss der Benutzer bei Bedarf selber sorgen z.B. mit Encrypted Filesystem, einer Verschlüsselungserweiterung für Unix-artige Dateisysteme. Zum Transport der Daten vom lokalen Ubuntu One Ordner an die Server wird eine 256-Bit-SSL -Verschlüsselung genutzt. Nach dem Transfer befinden sich die Daten unverschlüsselt auf den Servern, Ubuntu gibt das auch in seinen FAQ auf der Webseite offen wieder.[5] Die Daten sind somit für alle verfügbar, die befugt oder unbefugt Zugriff auf die Server haben. Da auch hier die Amazon Server genutzt werden, wird von Seiten Amazons laut Aussage für die physische Sicherheit der Daten durch militärartige Überwachung gesorgt.[2]

Team Drive

Team Drive Systems GmbH wurde im Jahr 2005 von dem Software-Entwicklungshaus SNAP (SNAP Innovation GmbH) in Hamburg gegründet. Damals trug es noch den Namen „PrimeSharing Deutschland GmbH“ und die Entwicklung der Software wurde von der Innovationsstiftung Hamburg aus öffentlichen Mitteln der Hansestadt Hamburg gefördert.[6]

Team Drive war zu Beginn nur für das Betriebssystem Windows verfügbar und wurde damals in den Versionen 1.x mehrfach ausgezeichnet, zum Beispiel mit dem Innovationspreis 2007 der Initiative Mittelstand.[6]

Team Drive kann zur Datensicherung und Synchronisation zwischen mehreren Geräten eingesetzt werden, ist bei Privatanwendern jedoch relativ unbekannt. Denn entwickelt

wurde diese Kollaborationssoftware in erster Linie für die geschäftliche Nutzung, um eine sichere Zusammenarbeit von Arbeitsgruppen und Teams über das Internet zu gewährleisten. Hierbei unterstützt die sehr gute Versionsverwaltung die parallele Bearbeitung von Dateien durch mehrere Anwender.

Funktionsweise

Inzwischen ist die Software auch für die Betriebssysteme Linux, Mac OS X, iOS und Android erhältlich. Nach der Installation der Software stellt diese eine Verbindung zum Team Drive Server her und bindet den Speicherplatz als Netzlaufwerk in den PC Arbeitsplatz ein. Alle Daten, die man dem neuen Laufwerk hinzufügt oder ändert, werden mit den Daten auf dem Server abgeglichen und gespeichert. Man kann auch beliebige lokale Ordner auswählen, diesen stehen dann alle Funktionen von Team Drive zur Verfügung.

Nutzern der Open Office Software wird ein spezielles Plugin angeboten. Darüber können Sie direkt aus den Open Office Anwendungen Writer, Calc und Impress auf die in Team Drive gesicherten Dateien und auf alle Vorgängerversionen der Datei zugreifen. Es gibt keine Zugriffsmöglichkeit auf die Daten über den Browser.

Es gibt drei Möglichkeiten bei der Serverwahl:

Team Drive Cloud Team Drive nutzt unter anderem Amazon Web Services. Für europäische Kunden werden ausschließlich Server in EU-Mitgliedsstaaten verwendet (überwiegend Irland). Für alle anderen Kunden werden Cloud Services in Nord-Amerika genutzt. Welche Cloud Services ausser AWS genutzt werden, wird nicht angegeben. Auf Wunsch kann der Speicherort individuell festgelegt werden. Es stehen 2 GB Speicherplatz kostenfrei zur Verfügung, mit der Option zur kostenpflichtigen Erweiterung. Regelmäßig werden automatisch mehrere verschlüsselte Sicherheitskopien erstellt.

Eigener Team Drive-Server Eigene Server, eigene NAS Laufwerke oder auch Home Mediaserver sowie beliebige andere Rechner können als eigenen Team Drive Server genutzt werden. Die Anwendung **Team Drive Personal Server** (für Windows, Mac und Linux) hilft bei der Einrichtung eines eigenen Team Drive HTTP Servers, der ausschließlich auf die Anfragen der Team Drive Clients reagiert. Der Server wird über einen frei wählbaren Port adressiert, so dass er parallel zu anderen HTTP und WebDAV Servern betrieben werden kann. Team Drive verwendet ein eigenes Authentifizierungsverfahren welches sicherstellen soll, dass nur autorisierte Team Drive Clients schreibend auf den Server zugreifen können. Laut Team Drive kann deshalb ohne Sicherheitseinbußen auf das HTTPS Protokoll verzichtet werden.[6]
Für große Unternehmen und Internet Service Provider bietet **Team Drive Enterprise Server** (nur für Linux) eine beliebig skalierbare Hosting Server Lösung an.

WebDAV Server (**Web**-based **D**istributed **A**uthoring and **V**ersioning, ein offener Standard zur Bereitstellung von Dateien im Internet[1]) Hier ist keinerlei Installation

einer Serversoftware notwendig, allerdings müssen die genutzten WebDAV Server den gesamten standardmäßigen Befehlsumfang von WebDAV unterstützen.

Das Teilen der Daten und Dateien ist nur bei vorhandener Team Drive Software möglich, jedoch gibt es bei der kostenpflichtigen Professional Version die Möglichkeit die Daten über eine URL freizugeben. Hierbei wird die Datei kopiert und erneut unverschlüsselt auf einen Team Drive-Server hochgeladen. Das Teilen und das gemeinsame Bearbeiten von Daten erfolgt über Arbeitsgruppen. Jeder erstellte Ordner in dem Team Drive Laufwerk bildet dabei eine Arbeitsgruppe. Man kann Mitglieder über ihre E-Mail Adresse zu diesen Arbeitsgruppen einladen und ihnen verschiedene Rechte zuweisen:

Download only Dateien können vom Gruppenmitglied nur heruntergeladen werden, Änderungen vom Gruppenmitglied werden nicht hochgeladen.

Read/Write Dateien können vom Gruppenmitglied bearbeitet und gelöscht werden.

Superuser Dateien können vom Gruppenmitglied bearbeitet und gelöscht werden und das Gruppenmitglied kann weitere Teilnehmer einladen.

Administrator Der Administrator kann zusätzlich Gruppenmitglieder entfernen und Dateien endgültig vom Server löschen.

Durch die Team Drive Versionsverwaltung hat man Zugriff auf ältere Versionen oder gelöschte Dateien und alle Änderungen von Gruppenmitgliedern können nachverfolgt werden.

Team Drive gibt an, die lokal abgespeicherten Daten vor dem Transfer auf den Server zu komprimieren, welches Verfahren dabei genutzt wird, ist nicht mit angegeben.

Kosten und Volumenangebot

Eine Liste der aktuellen Preise und Produktvarianten für EU-Privatkunden:

Produkt	Volumen		Kosten pro Monat	Kosten pro Jahr
	TD Cloud	eig. Server		
Team Drive Free	2 GB	2 GB*	-	-
Personal Lizenz	2 GB incl.	unbegrenzt	nur jährlich	29,99 €
Professional Lizenz	2 GB incl.	unbegrenzt	5,99 €	59,99 €
Speicherplatzerweiterung für die Personal/Professional Lizenzen:				
+10 GB	10 GB	unbegrenzt	5,99 €	59,99 €
+ 25 GB	25 GB	unbegrenzt	14,95 €	149,50 €
+ 50 GB	50 GB	unbegrenzt	29,90 €	299,00 €

* Für die Berechnung werden alle Dateien zusammengerechnet die mit dem kostenfreien Client überwacht und synchronisiert werden. Nach Erreichen des Limits ist eine manuelle Upload und Download Bestätigung erforderlich. Team Drive liegt mit einem durchschnittlichen Preis von über 60 Cent pro GB im Monat weit über den anderen

Anbietern, bietet dabei aber auch eine vielseitigere Software, sowie die Möglichkeit des unbegrenzten Datenvolumens auf eigenen Servern.

Verschlüsselung und Transfer

Bei der Installation von Team Drive werden für jede Installation jeweils ein Public-/Private-Schlüssel-Paar erzeugt. Diese Schlüssel werden für die sichere Übertragung von Team Drive-Einladungen verwendet. Der Public-Schlüssel wird auf einem von Team Drive betriebenen zentralen Server hinterlegt, der Private-Schlüssel wird beim Nutzer hinterlegt.

Lokal werden die Daten mit dem Algorithmus AES-256 verschlüsselt. Für jeden Ordner wird ein eigener AES-256 symmetrischer Schlüssel erzeugt. Sobald ein neues Gruppenmitglied eingeladen wird, wird der symmetrische Schlüssel des Ordners mit dem Public-Schlüssel des einzuladenden Gruppenmitglieds verschlüsselt und an das Gruppenmitglied übertragen. Auch die Zugangsdaten zum Speicherplatz auf den Team Drive-Server werden in verschlüsselter Form übertragen. Das Gruppenmitglied hat nun die Möglichkeit den symmetrischen Schlüssel mit seinem Private-Schlüssel zu entschlüsseln und dem Ordner beizutreten. Mit diesem Verfahren ist sichergestellt, dass nur autorisierte Gruppenmitglieder Zugang zu den Daten haben.

Zum Transfer der Daten auf die Server wird HTTP benutzt, jedoch werden die Protokolle noch zusätzlich durch Team Drive eigene Protokolle ergänzt. Diese Protokolle sind nicht veröffentlicht, somit gibt es keine unabhängige Einschätzung über ihre Sicherheit und Qualität.

Da alle 256 Bit AES Private-Schlüssel, die für den Zugriff auf die Daten benötigt werden, ausschließlich lokal bei den Nutzern gespeichert sind, kann keine unbefugte Entschlüsselung der Daten auf den Servern statt finden.

Team Drive wurde vom unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) geprüft und mit dem Datenschutzgütesiegel ausgezeichnet.[6] Das ULD ist eine Dienststelle des Landes Schleswig-Holstein mit Sitz in Kiel. Es nimmt staatliche Kontroll- und Beratungsfunktionen im Bereich des Datenschutzes sowie der Informationsfreiheit wahr.[3]

Die 3 Anbieter im Überblick

Anbieter	Dropbox	Ubuntu One	Team Drive
Gründung Firmensitz	2005 USA	2009 Isle of Man	2005 Hamburg
SpeicherAngebot Free	2 - 10 GB	5 GB	2 GB
Preis GB/ Monat	ca. 8 Cent	11 Cent	60 Cent
Plattformen	Win, Mac, Linux, iOS, Android BlackBerry	Win, Linux (Ubuntu), iOS, Android	Win, Mac, Linux, iOS, Android
Verschlüsselung Lokal: Übertragung: Server:	 keine SSL AES 256	 keine SSL keine	 AES 256 eig. Protokolle AES 256
Serverstandort	USA	unbekannt	EU oder eig. Server

3 Cloud-Sicherheit

Rechtlich erfolgt die Bereitstellung und Nutzung von Clouds im Rahmen eines Schuldvertrags, bei dem sich eine Vielzahl von juristischen Fragestellungen ergeben können. Diese Cloud-Verträge sind nicht eindeutig zuordenbar, sondern eine Typenmischung mit Anteilen eines Mietvertrags, einer Leihe und eines Dienst- und/oder eines Werkvertrages (Schulung, Pflege, Schnittstellenanpassung).

Über die Cloud-Verträge hinaus können Sicherheitszusagen über Security-Service-Level-Agreements (SSLA) verabredet werden. Tatsächlich bleiben die Cloud-Anbieter bei ihren Garantien für Sicherheitsmaßnahmen „wolkig“. SSLA haben regelmäßig den Charakter von allgemeinen Geschäftsbedingungen.

Es gibt keine internationalen Regelungen für Datenschutz und -sicherheit. Je nach Situation gelten die Datenschutzbestimmungen (falls vorhanden) des Landes bzw. der Region in dem sich der Sitz des Unternehmens und/oder die Server befinden. Deshalb ist bei der Wahl eines Cloud-Anbieters der Standort des Unternehmens und der Server zu berücksichtigen, die meist in verschiedenen Regionen liegen.

Was gilt es zu schützen?

Das zentrale Problem des Cloud Computing besteht darin, die Integrität und Vertraulichkeit der Datenverarbeitung des Cloud-Nutzers zu gewährleisten. Dies gilt nicht nur für die Verarbeitung personenbezogener, sondern sämtlicher Daten, bei denen es auf Vertraulichkeit und Integrität ankommt, z.B. für Betriebs- und Geschäftsgeheimnisse, für Forschungsdaten oder für anderweitig immateriell-rechtlich geschützte Daten. Es geht um das Unterbinden unberechtigter und schädigender Zugriffe Dritter.

Vor wem und vor was sollte geschützt werden?

Zugriff Dritter

Legaler Zugriff Durch die Verlagerung des Ortes der Datenverarbeitung in einen anderen Staat ergibt sich, dass Dritte, die keine Cloud- oder Ressourcen-Anbieter sind, in diesem Staat möglicherweise tatsächlich und evtl. auch auf rechtlicher Grundlage Zugriff auf diese Daten nehmen dürfen. Dies gilt vorrangig für die Behörden der „inneren Sicherheit“, also Polizei, sonstige Strafverfolgungsbehörden, nationale Geheimdienste, oder Finanzbehörden. Es ist nicht auszuschließen, dass das nationale Recht, etwa wegen eines völligen Fehlens von Datenschutzrestriktionen, sogar den Zugriff durch private Dritte erlaubt. Je niedriger das Datenschutzniveau in dem Staat ist, in dem die Datenverarbeitung tatsächlich stattfindet, desto größer ist die Gefährdung der Betroffeneninteressen durch die Cloud-Datenverarbeitung. Die Motivation für derartige legale Zugriffe muss nicht in der Gefahrenabwehr oder der Ermittlung von kriminellen Handlungen liegen. So gehört es zu den rechtlichen Aufgaben und Befugnissen vieler nationaler Geheimdienste, für die heimischen Interessen Wirtschaftsspionage zu betreiben. Dies kann in keinem Fall im Interesse des Cloud-Nutzers und sollte auch nicht in dem der Cloud- und Ressourcen-Anbieter liegen, lässt sich aber rechtlich nicht und faktisch nur schwer verhindern.

Illegaler Zugriff Je nach den vorgesehenen und umgesetzten Sicherheitsvorkehrungen besteht ein Angriffsrisiko durch unberechtigte Dritte auf die von Cloud-Nutzern verarbeiteten Daten. Ein besonderes Risiko besteht darin, dass über die Cloud völlig neue Angriffsmöglichkeiten von Cyberkriminellen eröffnet werden. Diese können die schwächste Sicherheitsstelle der Cloud nutzen, um in diese einzudringen. Da die Cloud- und Ressourcenanbieter kein eigenes Interesse an der Datenverarbeitung, sondern nur an deren Vergütung haben, ist es Kriminellen eventuell leicht möglich, unerkannt in die Rolle des Nutzenden zu schlüpfen, um die Datenverarbeitung auszuspionieren und/oder zu sabotieren. Der Cloud-Nutzer trägt die Verantwortung für die Daten, die unter seinen Nutzer-Konto gespeichert werden. Wenn sich jemand unbefugt Zugang zu einem Nutzer-Konto verschafft, besteht die Gefahr nicht nur darin, dass der Unbefugte an vorhandene Daten heran kommt, sondern auch, dass er die Möglichkeit hat, unbemerkt illegale Daten auf die Server hochzuladen.

Datenverlust oder Beschädigung

Da die Daten der Nutzer lokal auf eigenen Rechnern gesichert sind und die Cloud somit primär für Backup und Synchronisation genutzt wird, ist ein Serverausfall nicht zwangsläufig ein Grund für Datenverlust. Letztendlich muss jeder für sich selbst entscheiden, was für ihn, den Datenschutz außen vor gelassen, physisch sicherer erscheint: das Backup in der Cloud, also auf externen Servern in riesigen Serverfarmen, die meist gut gesichert sind vor Ausfällen und Datenverlust, oder die Sicherung auf eigener Hardware zu Hause, wo jeder selbst bestimmen kann, wie viele Sicherungskopien er tatsächlich braucht.

Sicherheitslücken bei den Anbietern

Das Fraunhofer-Institut für Sichere Informationstechnologie kommt in seiner Studie vom März 2012 zu dem Ergebnis, dass die Sicherheit einer ganzen Reihe von Cloud-Diensten verbesserungswürdig ist.[7]

Auch die drei hier vorgestellten Anbieter wurden untersucht. Einen Überblick der Bewertung zeig diese Tabelle:

Anbieter	Dropbox	Ubuntu One	Team Drive
Registrierung	-	++	+ -
Transport	+	+	+ -
Verschlüsselung	-	- -	+
Sharing	+ -	++	+ -
Deduplikation	+	+	x

Legende:

++	sehr gut	-	schlecht
+	gut	- -	sehr schlecht
+ -	einige Schwächen	x	nicht vorhanden

Die Sicherheitslücken der Anbieter im Detail:

Dropbox

Registrierung Es gibt keine Verifizierung der E-Mail Adresse bei der Erstellung eines neuen Nutzerkontos. Dadurch ist es möglich, illegales Material hochzuladen, das einem anderen Nutzer angelastet wird.

Verschlüsselung: Es gibt keine lokale Verschlüsselung durch den Client. Der Benutzer muss/kann selbständig durch Programme wie z.B. TrueCrypt verschlüsseln. Das schränkt einige Funktionen von Dropbox ein.

Filesharing evtl. Verwendung mangelhaft verschleierter Internet-Adressen, Dropbox macht keine klaren Aussagen darüber, wer genau Zugriff auf die fraglichen Dateien hat.

Ubuntu One

Verschlüsselung Die Dateien werden weder lokal vom Client verschlüsselt, noch nach dem Transfer auf die Server und liegen somit unverschlüsselt auf den Servern. Der Nutzer muss/kann sich selber um die lokale Verschlüsselung kümmern.

Team Drive

Transfer Bei der Datenübertragung vom Client an den Server werden keine der Standardprotokolle (SSL/TSL) genutzt. Stattdessen werden unveröffentlichte propri-

etäre Protokolle verwendet, ein erfahrungsgemäß sehr fehleranfälliger Ansatz.

Filesharing Gruppenmitglieder, die bereits ausgeladen wurden, haben teilweise weiterhin Zugriff auf die Daten.

Ein wesentliches Ergebnis der Studie ist, dass alle Provider sich der großen Bedeutung von Datensicherheit und Datenschutz bewusst sind und Schutzmaßnahmen ergriffen haben. Dennoch konnte unter den betrachteten Anbietern keine Lösung gefunden werden, die alle zugrundeliegenden Sicherheitsanforderungen erfüllt.[7]

Quellen und Einzelnachweise

Einzelnachweise:

1. http://www.itwissen.info
2. http://aws.amazon.com
3. https://www.datenschutzzentrum.de
4. https://www.dropbox.com
5. https://one.ubuntu.com
6. http://www.teamdrive.com
7. http://www.sit.fraunhofer.de/de/cloudstudy.html

Quellen

http://www.cloudsider.com

http://www.itwissen.info

https://www.datenschutzzentrum.de

http://en.wikipedia.org/wiki/Remote_backup_service

http://de.wikipedia.org/wiki/Ubuntu_One

http://de.wikipedia.org/wiki/Amazon_Web_Services

http://de.wikipedia.org/wiki/Online-Datensicherung

http://de.wikipedia.org/wiki/Cloud-Computing

https://one.ubuntu.com

http://www.teamdrive.com

https://www.dropbox.com

http://www.sit.fraunhofer.de/de/cloudstudy.html

http://aws.amazon.com