

# Cloud Speicher



Agnes Marco1

Proseminar Speicher- und Dateisysteme

SoSe 2012

# Ablauf

## Cloud-Speicher allgemein

- Was ist die Cloud?
- Möglichkeiten
- Vorteile
- Nutzer u. Anbieter
- Cloud-Arten

## 3 Beispiele

- Dropbox
- Ubuntu One
- TeamDrive

## Kritik / Problematik

- „Cloud-Sicherheit“
- Sicherheitslücken

# Was ist die Cloud?

- Virtueller Bereich
- Bestimmungsort nicht identifizierbar
- Ablegen, bearbeiten von Daten, Dateien, (Programmen)
- Mehrere Benutzer mit entsprechender Autorisierung
- Oberbegriff: Cloud-Computing mit Cloud-Diensten
- ein solcher Dienst: Cloud-Speicher (Storage-as-a-service)
- Hardware befindet sich „in der Cloud“ (externe Server)



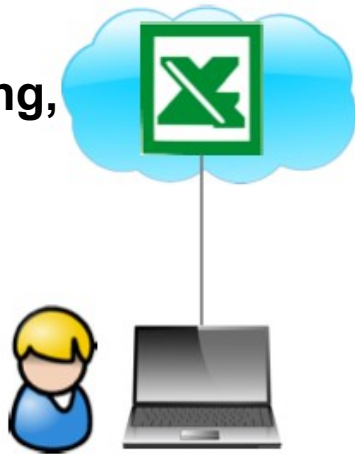
# Was ist die Cloud?

Cloud-Speicher als Möglichkeit für:

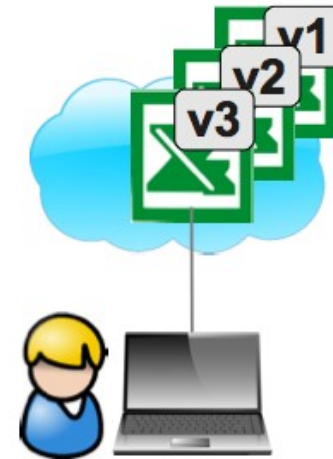
- Datensicherung, Copy, Backup
- Versionsverwaltung
- Synchronisation
- File-Sharing
- Musik-Streaming

# Möglichkeiten des Cloud-Speichers

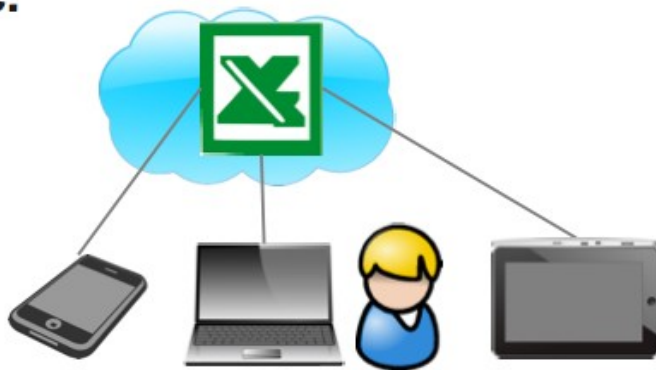
**Copy**  
(Datensicherung,  
Backup)



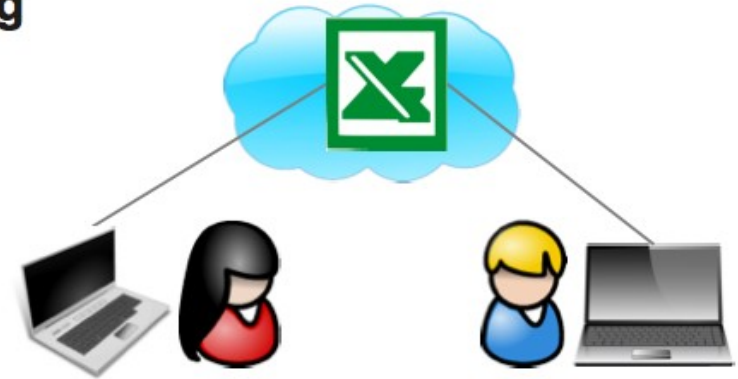
**Versions-  
verwaltung**



**Sync.**



**Sharing**



# Vorteile

- Datensicherung / Backup
- keine Beschaffung und Wartung von Hardware
- Synchronisation von Daten und Geräten
- Zugriff auf eig. Daten von beliebigen Geräten  
(Internetzugang, Browser)
- Daten teilen mit Anderen

# Nutzer und Anbieter

## Cloud-Nutzer

Nimmt Speichervolumen von Cloud-Anbieter in Anspruch

## Cloud-Anbieter

Stellt dem Cloud-Nutzern die Cloud-Dienste bereit, kann Ressourcen-Anbieter in Anspruch nehmen

## Ressourcen Anbieter

Stellt Cloud-Anbietern für Datensicherung Hard- oder Software zur Verfügung

# Cloud-Arten

## Private Cloud

Vernetzte Rechner, eine DV-Stelle  
hat rechtliche Verantwortung

## Public Cloud

Speichervolumen wird von  
Drittanbietern angeboten, Daten  
werden auf Servern gesichert

## Hybride Cloud

Mischung aus Private und Public,  
Nutzung von eig. und fremden  
Ressourcen

## Community Cloud

Infrastruktur wird von  
vers.  
Institutionen/Personen  
gemeinsam genutzt,  
Anforderungen  
(Sicherheit, Datenschutz)  
werden kollektiv  
vereinbart



# 3 Beispiele



# Dropbox

- Kategorie: Dateisynchronisation
- Entwickler: Dropbox Inc.
- 2007 gegründet, Firmensitz in USA
- Serverstandort: USA (Amazon)
- Lokale Speicherung im Dropbox Ordner
- Datensicherung, Synchro., Sharing
- Kosten: 2-10 GB free, 50 GB ca. 8 € / Monat, 100 GB ca. 16 € / Monat, Teams: 1 TB+, ab 5 Mitgliedern, ab ca. 630 € / Monat
- Volumen: unbegrenzt



# Dropbox

- Plattformen: Win, Mac, Linux, iOS, Android, BlackBerry
- Zugriff über Webbrowser möglich
- derzeit nur Single-User-Deduplizierung (=> Dropship)
- Amazon Web Services (AWS)
- Zentrales Speichersystem: S3 von Amazon (Simple Storage Service, key-value FileHosting Service)



# Dropbox

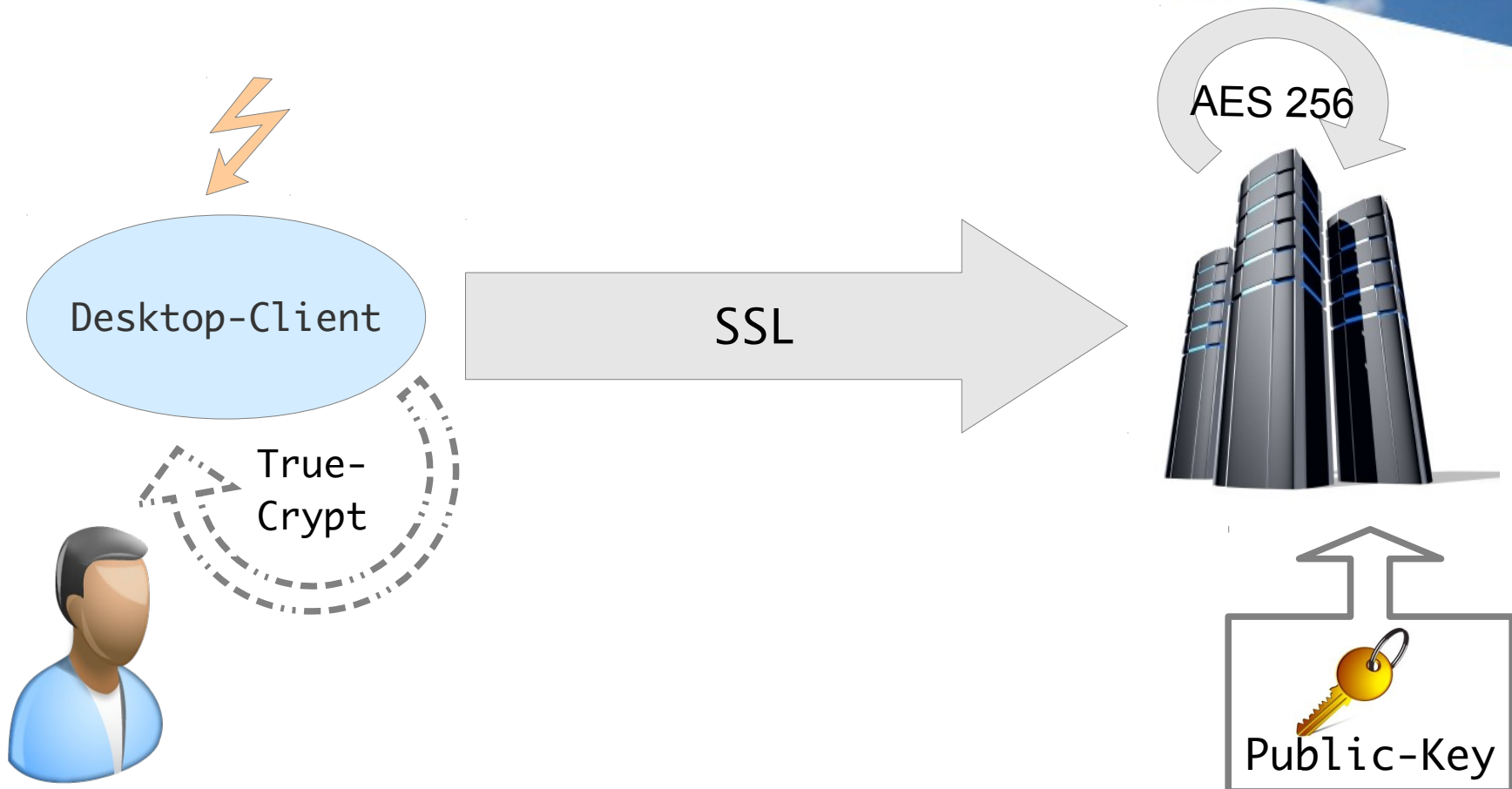
## Freigabe von Dateien und Ordnern

- Zuweisung einer URL für Dateien
- Zugriff und Bearbeitung von Dateien durch mehrere Benutzer
- bei Konflikten separate Speicherung konkurrierender Versionen
- Extra Ordner:
  - Photos: Fotogalerien, automatische Webadresse, öffentlich im Netz zu finden
  - Public: Daten werden direkt referenziert (FileHoster)



# Dropbox

## Verschlüsselung und Transfer



# Ubuntu One

- Kategorie: Online-Datensicherung
- Entwickler: Canonical Ltd.
- 2009 Einstieg mit Beta-Phase, Firmensitz in Isle of Man
- Serverstandort: unbekannt
- Lokale Speicherung: Benutzerordner / Ubuntu One Ordner
- Datensicherung, Synchro., Sharing
- Kosten: 5 GB free, 20 BG ca. 2,30 € / Monat,  
20 GB + Music Stream ca. 3,20 € / Monat
- Volumen: max 50 GB



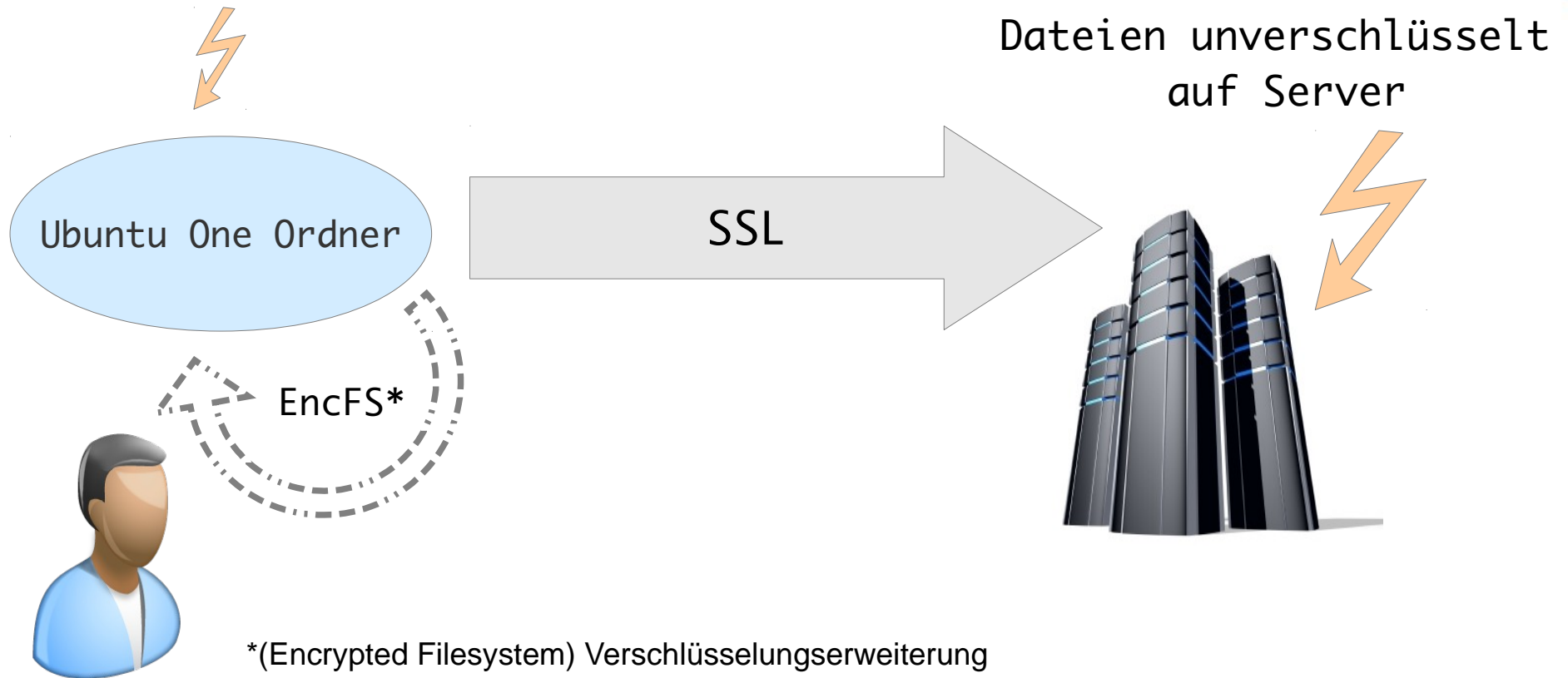
# Ubuntu One

- Plattformen: Win, Linux(Ununtu), iOS, Android
- Zugriff über Webbrowser möglich
- Single-User-Deduplizierung (file-level)
- Freigabe: für andere Ubuntu One User bzw. über Webadresse öffentlich zugänglich
- Musik Stream: 20 GB für eig. Musik, streaming auf (mobile) Geräte
- Kritik: Serversoftware von Ubuntu One ist kein OpenSource
- Speicherung und Transport: Amazon (AWS)



# Ubuntu One

## Verschlüsselung und Transfer



\*(Encrypted Filesystem) Verschlüsselungserweiterung  
für Unix-artige Dateisysteme



# TeamDrive

- Kategorie: Kollaborationssoftware
- Entwickler: TeamDrive Systems GmbH
- Gründung 2005, Firmensitz in Hamburg
- Serverstandort: EU für europäische Nutzer, Rest: USA
- TeamDrive wird als Laufwerk auf dem PC eingebunden, kein Zugriff über Browser
- Datensicherung, Synchro., Versionsverwaltung, Sharing
- Kosten: 5 GB free, 10 GB 5,99 € / Monat, 25 GB 14,95 € / Monat, 50 GB 29,90 € / Monat
- Volumen: unbegrenzt



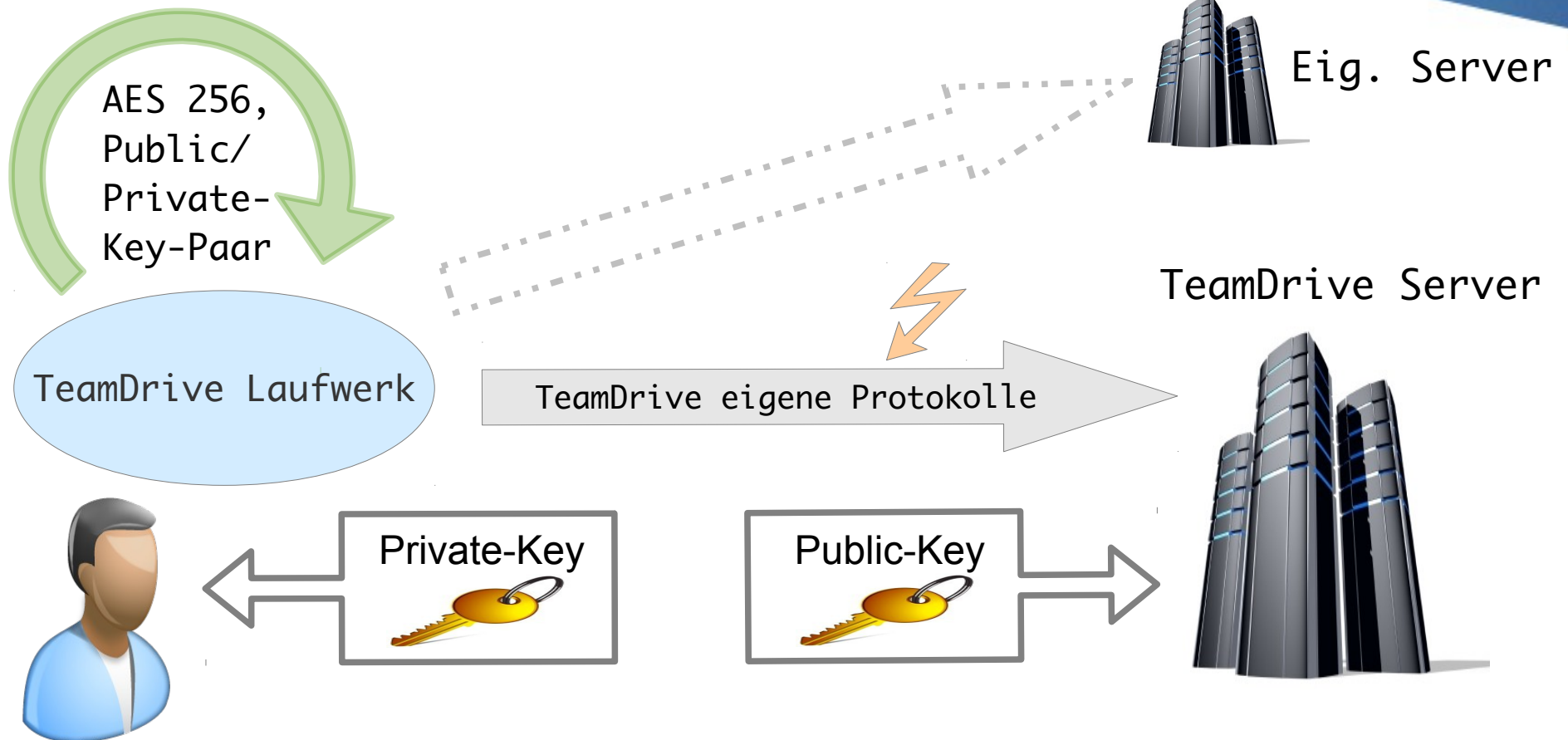
# TeamDrive

- Freigabe: Benutzer brauchen TeamDrive Software
- Link zu Dateien nur bei der Professional Version (5,99 €)
- besondere Funktionen für die parallele Bearbeitung von Dateien (Rechte-/Versionsverwaltung)
- Eig. Server und Administration möglich
- optional Server in Hamburg (ISO 27001 certified)
- Sehr gut bewertete Sicherheit (Datenschutzgütesiegel des Unabhängigen Landeszentrums für Datenschutz SH)
- Speicherung: Amazon Web Services






# TeamDrive

## Verschlüsselung und Transfer



# Vergleich der 3 Anbieter

| Anbieter  | Gründung<br>Firmensitz               | Speicher<br>Angebot<br>Free /<br>GB p. Monat | Plattformen  | Ver-<br>schlüsselung   | Server-<br>standort             |
|---|--------------------------------------|--|--|--|---------------------------------|
|    | 2005<br>USA                          | 2 – 10 GB /<br>ca. 16 Cent                   | Win, Mac, Linux,<br>iOS, Android,<br>BlackBerry<br>★ | Übertragung: SSL<br>Server: AES 256                          | USA                             |
|   | 2009 (Beta-<br>Phase)<br>Isle of Man | 5 GB /<br>9 – 12 Cent<br>★                   | Win, Linux<br>(Ubuntu),<br>Android, iOS              | Übertragung: SSL<br>Server:<br>unverschlüss.                 | unbekannt                       |
|  | 2005<br>Hamburg                      | 2 GB /<br>60 Cent                            | Win, Mac,<br>Linux                                   | AES 256 vor<br>Transfer,<br>Public/Private-<br>Key-Paar<br>★ | EU<br>eig.<br>Server<br>möglich |

# „Cloud-Sicherheit“

Was gilt es zu schützen?

- Personenbezogene Daten
- Daten in der Cloud

(kritische Betriebs- und Geschäftsgeheimnisse)

- Cloud-Nutzer trägt Verantwortung für Daten und Verarbeitung



# „Cloud-Sicherheit“

Vor wem/was soll geschützt werden?

- Zugriff Dritter

legal z.B. durch den Patriot Act in den USA

illegal durch unbefugte Personen

- Datenverlust oder Beschädigung

Hardware-/Serverausfall



# „Cloud-Sicherheit“

- Cloud-Verträge:

Mischung aus Mietvertrag, Leihvertrag, Dienst- und/oder Werkvertrag

- keine internationalen Regelungen für Datenschutz und -sicherheit
- Security-Service-Level-Agreements
- Wichtig bei der Wahl eines Cloud-Anbieters:  
Sitz des Unternehmens und der Server



# „Cloud-Sicherheit“

- Vertraulichkeit und Integrität steigt im technischen Bereich
- Nationen erweitern Zugriffsbefugnisse in der Cloud
- Nutzer sollte das bei der Wahl seines Cloud-Anbieter berücksichtigen
- Eigene Sicherheitsmaßnahmen







# Sicherheitslücken bei den 3 Beispielen



## Dropbox

- Registrierung: fehlende Verifizierung neuer E-Mail Adressen
- Verschlüsselung: keine Client-seitige Verschlüsselung
- Filesharing: evtl. Verwendung mangelhaft verschleierter Internet-Adressen, keine klaren Angaben welche Personen Zugriff erhalten





# Sicherheitslücken bei den 3 Beispielen



## Ubuntu One

- Verschlüsselung: Dateien werden auf Client-Seite nicht verschlüsselt und liegen nach dem Transfer unverschlüsselt auf den Servern





# Sicherheitslücken bei den 3 Beispielen



## TeamDrive

- Transfer: bei Datenübertragung keines der Standardprotokolle (SSL/TSL), sondern Firmeneigene, nicht veröffentlichte Protokolle
- Filesharing: Gruppenmitglieder, die ausgeladen wurden, haben teilweise weiterhin Zugriff



# Zusammenfassung

| Cloud-Speicher   | 3 Beispiele  | Kritik / Problematik   |
|--|--|--|
| <ul style="list-style-type: none"><li>• Was ist die Cloud?</li><li>• Möglichkeiten</li><li>• Vorteile</li><li>• Nutzer u. Anbieter</li><li>• Cloud-Arten</li></ul> | <ul style="list-style-type: none"><li>• Dropbox</li><li>• Ubuntu One</li><li>• TeamDrive</li></ul> | <ul style="list-style-type: none"><li>• „Cloud-Sicherheit“</li><li>• Sicherheitslücken</li></ul> |
| <p>=&gt; viele praktische Vorteile &amp; Möglichkeiten</p>   | <p>=&gt; diverse Anbieter, Spezialisierungen, Sicherheitslücken</p>                                | <p>=&gt; Verträge lesen, Schwachstellen erkennen, Risiken bewusst machen</p>                     |

# Quellen

<http://g33ky.de/2011/5/2/Dropbox-und-Dropship/>  
<http://www.cloudsider.com>  
<http://www.itwissen.info>  
<https://www.datenschutzzentrum.de>  
[http://en.wikipedia.org/wiki/Remote\\_backup\\_service](http://en.wikipedia.org/wiki/Remote_backup_service)  
[http://de.wikipedia.org/wiki/Ubuntu\\_One](http://de.wikipedia.org/wiki/Ubuntu_One)  
[http://de.wikipedia.org/wiki/Amazon\\_Web\\_Services](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>

# Bildquellen

<https://one.ubuntu.com>

<http://www.teamdrive.com>

<https://www.dropbox.com>

[http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security\\_a4.pdf](http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security_a4.pdf)

<http://www.computerwoche.de/security/2510149/>

<http://www.smbnow.com/articles/netgear-cloud-computing>

<http://supportformicrosoft.iyogi.com/news/microsoft-talks-about-azure-cloud-security.html>

<http://www.b1-blog.de/2012/03/09/business-one-ondemand/>