Dropbox, auch verschlüsselt

Tom Novacek, 17.03.2014

Die **"Firma" dropbox** bietet auf ihrem Server **Ordner zur Miete** an. So etwas ist nicht neu. Wir alle benutzen seit langemeinen solche Dienste, wir benutzen nämlich **E-Mail Postfächer (Mail Boxen)** zur Miete. Daher hier zunächst ein kleiner Exkurs zum Thema E-Mail.

Wie funktionieren Mailboxen? Wie unterscheidet sich der Zugriff POP von IMAP?

- Zu jedem **E-Mail-Konto** gehören (mindestens) zwei Ordner **auf dem Server des Maildienstes** t-online, Vodafone, 1und1, web.de, gmx.de....
    - ein Eingangspostfach ("INBOX")
    - ein Ausgangspostfach
- Im Eingangspostfach liegen eingehende E-Mails für Sie zum Abholen bereit
- im Augangspostfach liegen E-Mails von Ihnen zum Versenden bereit, normalerweise nur kurze Zeit, da die Übertragung zum Empfänger sofort beginnt.
- Zu griff auf diese beiden Postfächer haben Sie
    1. entweder **mit Ihrem Browser** (Ingernet Explorer, Firefox, Chrome, Safari, Opers....), indem Sie beim Maildienst mit Benutzername und Passort einloggen
    2. oder durch ein **Mailprogramm auf Ihrem PC** (Outlook. Thunderbird, K9Mail, Gmail, Apple Mail Programm, Windows Mail...), mit dem Sie empfangene Mails anschauen und auswerten, eigene Mails verfassen und versenden und alle verwalten ohne **direkt** mit dem Maildienst zu korespondieren.
       Das **Mailprogramm enthält** ebenefalls einen Ordner "**Posteingang**", und einen Ordner "**Postausgang**". Wenn die Mail aus dem Postausgang gesendet wurde, ist dieser Ordner leer und eine Kopie der Mailwird in einen weiteren Ordner "Gesendet" abgelegt.
- Im Fall 2 - Mailprogramm auf dem eigenen PC – müssen die Mailboxen auf dem Server des Maildiensts und die Mailboxen auf dem PC aufeinander abgestimmt sein. Dazu gibt es zwei Protokolle (Verfahren):
    - Bei **POP**, dem Post Office Protokoll, liegt die Verwaltung der Mails beim Mailprogramm auf dem PC. Dort werden Mails gespeichert, gelöscht, erzeugt, kopiert. Der Maildienst des Servers ist bloß ein Zwischenglied zwischen Mailprogramm und dem Internet.

      Inzwischen übernimmt der Maildienst aber einige Funktionen z. B. Spam- und Virenerkennun und beim Posteingang auf Wunsch zuerst die Kopfzeilen einer Mail übertragen.

    - Bei **IMAP, dem** Internet Message Access Protocol, liegen die Verwaltung beim Maildienst auf dem Server. Das lokale Mailprogramm erzeugt zwar Mails, **gespeichert** sind sie aber im Ordner Inbox **auf dem Server**. Auch der Ordner mit den Kopien gesendeter Mails und der Papierkorb liegen dort. Damit sind alle Daten und Dienste von einem **beliebigen PC** aus erreichbar, wenn dieser mit dem Internet verbunden ist. Das funktioniert mit beliebigen - auch unterschiedlichen - Mailprogrammen, ja sogar auch ohne Mailprogramm mit Methode 1 und dem passenden Passwort.

  IMAP bietet Vorteile, wenn man Mails auf zwei oder mehr Geräten empfangen und senden möchte, etwa auf einem stationären PC und einem Smarthone. Beide haben Zugriff zu denselben Daten auf dem Server. Eine eingegangene Mail wird auf beiden Geräten angezeigt, *eine von dem einen Gerät gesendete Mail wird auch auf dem anderen Gerät als gesendet angezeigt.*

  Die Synchronisierung zwischen den Daten des IMAP-Servers und den Daten auf den Geräten ist ein komplexer Vorgang mit vielen Einstellmöglichkeiten. Man möchte etwa auf dem Smartphone nur die neuesten und wichtigsten Mails lagern und löscht die übrigen. Dadurch dürfen diese Mails auf dem Server aber nicht gelöscht werden, sonst würden sie auf dem PC auch verschwinden. Oder man möchte den Papierkorb nur auf dem PC sehen, nicht auch auf dem Smartphone. All das führt zu neuen Verfahren wie "expunge", "Ordner abonnieren" und das IDLS Kommando, darüber hinaus gibt es neue Mail-Zustände

wie "Zum Löschen vorgesehen". Dieses Thema würde aber vom Ziel, die Dropbox zu erklären, zu weit ablenken und soll hier nicht weiter verfolgt werden. Es ist aber ein Hinweis auf Synchronisierprobleme, die ähnlich auch bei Dropboxen auftreten.

Das **Mailsystem ist zur Übertragung** von Dateien geeigent, hat aber einige **Beschränkungen**:

- Die Datenmenge ist begrenzt, bei kostenlosen Maildiensten auf einige Megabytes.
- Wegen der starken Gefährdung auf dem langen Weg durch das Internet werden die Mails "gefiltert": keine ausführbaren Dateien wie .exe, Beschränkungen im Dateinamen des Anhangs usw.
- Sollen mehrere Empfänger dieselbe Mail erhalten,
    - muss der Absender sie adressieren (muss also die Mailadressen kennen und verwalten)
    - oder er kann kann mehreren Personen erlauben, Mails aus dem Eingangspostfach des Mail-Servers selbst abzuholen, wie das bei unserem "Rundbrief" eingerichtet ist. IMAP erlaubt das ohne weiteres, POP bietet dafür die Einstellung "Mail auf dem Server belassen". Die Verwaltung dieses Zugriffsrechts wird aber im Mailsystem nicht unterstützt – Wer hat Zugriffsrecht wofür? Wie kann man es entziehen? Außerdem müssen nicht mehr benötigte Mails zentral und manuell gelöscht werden

Die Beschränkungen des Mailsystems legen es nahe, ein *ergänzendes System* einzurichten und das ist die

"Dropbox"

(es gibt mehre ähnlich funktionierende Systeme unter Namen SkyDrive, Google Drive, iCloud...)

- Das kostenlose Programm dropbox erzeugt beim Installieren auf dem PC
    - einen speziellen Ordner "Dropbox" mit einer Verknüpfung in der Fußleiste 
    - Zugleich erzeugt es auf einem dropbox-Server einen eigenen dropbox-Ordner und
    - synchronisert diese beiden Ordner, indem es jede Änderung im lokalen dropbox-Ordner in den zugehörigen Ordner im dropbox-Server überträgt.
    - In den lokalen dropbox-Ordenr kann man beliebige Unterordner einrichten und mit beliebigen Daten füllen, alles wird im dropbox-Order des Servers automatisch nachgebildet.
- Zu einen Unterordner oder eine Datei kann man in der lokalen Dropbox einen "**Link freigeben**". Dadurch weist das dropbox-System dem entsprechenden Ordner oder der Datei im dropbox-Server eine Internet-**Linkadresse** zu, die so komplex aufgebaut ist dass sie wie durch ein Passwort geschützt wirkt. Mit dieser Linkadresse kann man mit einem Browser auf einem beliebigen PC die freigegebenen Daten abholen.

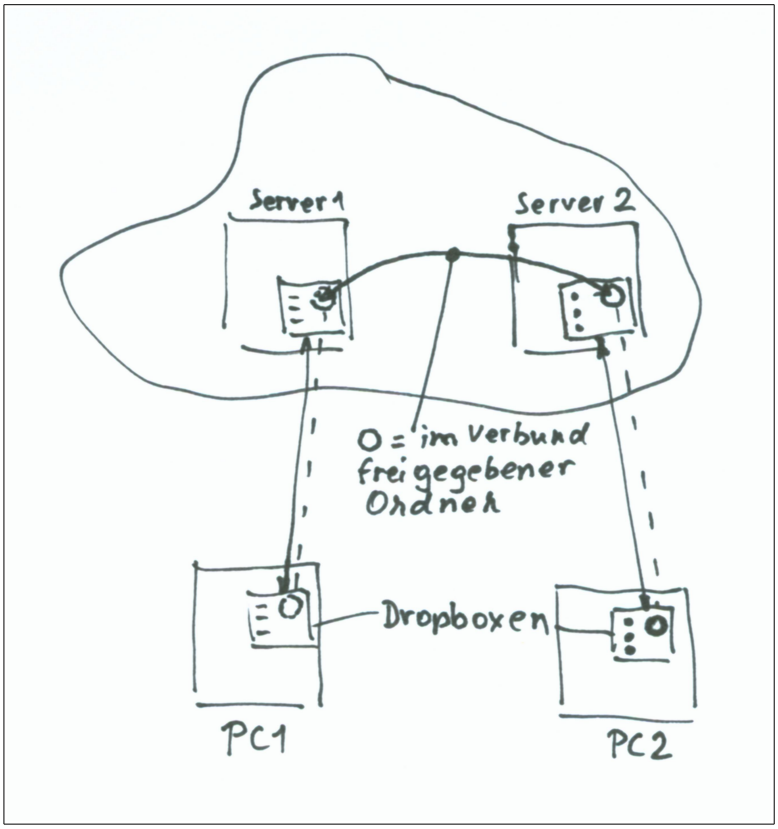
    Ich habe noch keine Möglichkeit gefunden, einen solchen Link wieder unwirksam zu machen. Nach Umbenennen funktioniert der Link zwar nicht mehr, aber das ist doch etwas umständlich. Am besten erzeugt man einen speziellen Ordner für die Freigabe und löscht ihn später.

Schon in dieser Stufe kann eine Dropbox nützlich sein:

- Man bekommt ein ausfallsicheres automatisches Backup und sogar ein einfaches Archiv s. u.)
- Man kann von fremdem PCs mit Internetanschluss auf eigene Daten passwortgeschützt zugreifen,
- Man kann die Schlüsseladresse Freunden verraten, die können damit Daten abholen – z. B. laufende Reiseberichte.
- Ordner und Dateien können schreibgeschützt sein.

Verbund von Dropboxen

Die Dropboxen mehrerer Teilnehmer können verbunden werden:



- Der Besitzer eines Dropbox-Ordners gibt ihn frei ("**Ordner freigeben**" zum Unterschied von "Link freigeben" wie oben beschrieben).
- Dabei gibt er die Mailadresse des Partners an, die dieser beim Einrichten seiner Dropbox benutzt hat.
- Der Partner erhält an diese Adresse vom Dropboxsystem eine Mail mit dem Angebot, den freigegebene Ordner in seine Dropbox aufzunehmen

  Da alle Dropboxen in einem gemeinsamen System verwaltet werden, ist in der Dropbox des Partners nur eine Verknüpfung zum freigegeben Ordner enthalten, es gibt daher hier keinen weiteren Synchronisationsvorgang.
- Die Freigabe kann das Recht für den Partner enthalten, seinerseits weitere Freigaben zu erteilen
- Der Besitzer kann in seinem Ordner Dateien ablegen, löschen oder ändern, die Änderungen erscheinen zeitverzögert im Ordner des Partners.
- Der Partner kann ebenso Dateien in seinen Ordner ablegenen, ändern oder löschen, die Änderungen erscheinen zeitverzögert im Ordner des Besitzers
- Jeder der beiden kann Dateien des anderen ändern oder löschen, wenn er dazu berechtigt ist (Schreibschutz).
  Das Spiel der Berechtigungen ist schon ungter Windows komplex und gsnz besonders, wenn Besitzer und Partner unterschiedliche Betriebssysteme verwenden (Apple-, Android-, Linux- und Windows-Versionen). Manche Dateien haben zusätzlich interne Zugriffsbeschränkungen.

Das Zeitproblem der Synchronisierung

Angenommen, der Besitzer ändert eine Datei im freigegebenen Ordner seiner lokalen Dropbox, hat aber im Moment keinen Internetzugang. Sie habe danach den Zustand B (wie Besitzer).

Gleichzeitig ändert der Partner dieselbe Datei seiner lokalen Dropbox in den Zustand P (wie Partner). Sobald er seine Arbeit beendet überträgt das Dropboxsystem die geänderte Datei in des Besitzers Dropbox im Dropbox-Server.

Sie sollte eigentlich gleich darauf auf den PC des Besitzers geladen werden, das muss aber warten, bis der Besitzer on-line ist.

Dann aber stehen zwei widersprüchliche Aufgaben an:

- Die Version P soll auf den PC des Besitzers geladen werden und dort die Datei (in Version B) überschreiben
- Die Version B soll über das Internet auf den PC des Partners geladen werden und dort die Datei im Version P ersetzen.

Welcher Vorgang ist schneller? Und geht eine der beiden Versionen verloren?

Das Dropboxsystem entschärft das Problem, indem es in den Dropboxen beide Versionen ablegt, eine davon mit dem Zusatz "[Dateiname] **in Konflikt stehende Kopie**", und es den beiden Teilnehmern überlässt, die beiden Versionen wieder zusammenzuführen.

Innerhalb eines PCs werden solche Kollisionen zwischen zwei gleichzeitigen Bearbeitungen vermieden, indem der erste Zugriff die Datei temporär gegen weitere Zugriffe sperrt. Über das Internet funktioniert so etwas nicht, wenn ein PC vorübergehend keine Verbindung mit dem Dropbox Server hat

Verschlüsseln

Die Dateien werden beim Synchronisieren verschlüsselt übertragen, im Dropbox-Server aber im Klartext gelagert. Es kann zweckmäßig, wichtige Dateien nicht im Klartext sondern verschlüsselt in den Dropboxen – lokal und auf dem Server - zu halten. Ich verwende dafür das kostenlose Programm **BoxCryptor**, da es davon Versionen für alle gebräuchlichen Betriebssysteme gibt (div. Windows Varianten, iOS, Android, UBUNTU usw.).

Ein Verschlüsselungsprogramm hat zwei Eingänge und einen Ausgang

- Einen Input für Klartext
- Ein Eingabefeld für den Schlüssel
- Einen Output für die verschlüsselte Form

Beim Entschlüsseln sind Input und Output vertauscht.

BoxCryptor benutzt dafür unterschiedliche Bedienoberflächen. Unter Windows funktioniert das Verfahren so:

- Der Besitzer startet das Programm BoxCryptor und fordert es auf, einen neuen Ordner anzulegen – im hier behandelten Fall innerhalb der lokalen Dropbox.
- BoxCryptor legt einen **speziellen Ordner für verschlüsselte Dateien an** ("Verschlüsselungsordner") verlangt die Eingabe eines Schlüssels und speichert ihn versteckt in diesem Ordner.
- Damit ist dieser Vorgang beendet.
- Später startet man BoxCryptor mit dem Auftrag, den Verschlüsselungsordner zu öffnen.
- BoxCryptor prüft, ob das wirklich ein Verschlüsselungsordner ist, verlangt die Eingabe des

Schlüssels und **erzeugt eine (virtuelle) Partition** auf der Festplatte, der man z. B. den Buchstaben P zuweist.

- Neben den Partitionen C:, D. … erscheint im Windows-Explorer nun ein P: auf dem eigenen PC
- **Verschiebt** man nun beliebige Dateien (oder Ordner) in unverschlüsselter Form in P:,
- verschlüsselt BoxCryptor sie und legt sie in den lokalen Verschlüsselungsordner.
- Sobald das Programm BoxCryptor beendet wir, **verschwindet P**: und es bleibt nur die verschlüsselten Formen auf dem PC übrig, die ehemaligen Orginale waren je verschoben und nicht kopiert worden.
- Zum Entschlüsseln startet man BoxCryptor, nennt ihm den Verschlüsselungsordner und das Passwort und hat in P: Zugriff auf die Dateien im Klartext.

Weitere Funktionen, wenn die Dropbox mit einer anderen verbunden ist:

- Der Synchronisationsmechanismus des Dropboxsystems hatte den Verschlüsselungsorder inzwischen in die Dropbox des Partners – es können auch mehrere sein – übertragen
- Der Partner startet nun seinerseits das Programm BoxCryptor verbindet es mit dem lokalen Verschlüsselungsordner.
- Darauf erzeugt BoxCryptor eine virtuelle Partition. z.B. V:, entschlüsselt den Inhalt des Verschlüsselungsordners und legt ihn in V: zur normalen Verwendung ab.

In andere Betriebssystemen hat Boxcryptor eine andere Bedienoberfläche, die Funktionen sind aber gleich.

Einige weitere Bemerkungen

- Wird eine Datei in der lokalen Dropbox gelöscht, verschwindet sie auch auf dem Dropbox-Server und in den verbundenen Dropboxen!
- Dropbox entschärft die Gefahr unbeabsichtigten Löschens dadurch, dass es einige ältere Versionen aufbewahrt, sie sind durch Einloggen in das Dropboxsystem erreichbar (einfache Archivfunktion).
- Derzeit bekommt man kostenlos 2 GigaBytes Platz, mit jedem m Partner nimmt der Platz zu.
- Die Synchronisierung ist mit heutiger Technik noch recht langsam. Daten müssen erst hoch- und dann heruntergeladen werden, die Übertragungszeiten addieren sich. 100 Megabytes können mehrere Minuten benötigen.
- Synchronisiert wird abhängig vom Betriebssystem und Version mehr oder weniger automatisch. Hat man die lokale Dropbox geöffnet, wird dort eine neue Datei eines Partners entweder sofort angezeigt oder erst nach einem Klick auf "aktualisieren" oder erst beim nächsten Starten der Dropbox – das muss man selbst herausfinden

Demos

- Dropbox lokal und im Internet zeigen
- Synchronisierung zeigen: Neuer Ordner "DemoOrdner", Bild einfügen
- Bild freigeben → Linkadresse im Wordpad zeigen
- Nur erklären: Mailübertragung der Linkadresse
- Browser, Linkadresse eingeben
- Spezialordner "Photos" erwähnen
- Verbund:
    - DemoOrdner freigeben
    - Mailadresse wir, absenden
    - Wir öffnen, Ordner ansehen, in eigene Dropbox aufnehmen
    - Über Dropbox im internet einladung löschen
    - DemoOrdner löschen
- BoxCryptor
    - Ordner neu in E:, ines..., K:
    - Textdatei erzeugen, in K: speichern
    - Zur Kontrolle öffnen
    - Boxcryptor beenden
    - Datei in E: anschauen: verschlüsselt
    - Boxcryptor öffnen ines... K: -> Klartext in K:
- Verschlüsselt in der Dropbox: genau so
    - Beispiele zeigen