Online Storage

Daniel Senff
s0514457

HTW Berlin / University of Applied Science
Angewandte Informatik (Master)
Wintersemester 2011/2012

Inhaltsverzeichnis

1. Einleitung

Der Personal Computer bot seinem Nutzer ein zentrales System. Die Festplatte des Computers war der Hauptmassenspeicher eines Anwenders und durch Vernetzung konnten Daten einfach ausgetauscht werden. Alle privaten Dokumente und Dateien lagen auf diesem zentralen Rechner.

Mit dem Aufkommen mobiler und multipler Endgeräte kommen je Gerät neue Speicherorte hinzu, die je nach Anwendungszweck unterschiedliche Daten dezentral vorhalten.
Die Anforderung dezentral auf die selben Datenbestände zugreifen zu können und diese konsistent und synchron zu halten verlangte neue Lösungen zur Cloud-basierten Datenspeicherung. Außerhalb des eigenen Netzwerks wird eine Infrastruktur bereitgestellt die Dateien vorhält, mit dem lokalen System synchronisiert und sie damit auf verschiedenen Plattformen und Endgeräten zur Verfügung stellt.

Wichtig bei diesen Diensten ist der Aspekt der Datensicherheit und des Datenschutzes. Dienste, die eine Auslagerung von Dateien in die Cloud ermöglichen, sollten daher unter besonderer Beobachtung in Bezug auf die technische Infrastruktur sein um die Datenintegrität, Sicherheit und Stabilität zu gewährleisten.

Welche Anforderungen werden an einen solchen Service gestellt und wie diese von ausgewählten Diensten erfüllt werden, versucht diese Arbeit zu betrachten. Es wird auf den Aufbau der Infrastruktur, insbesondere der Kryptografie, eingegangen und soll einen Einstiegspunkt zur Beurteilung der Sicherheit dienen.
Diese Arbeit wird drei Dienste beleuchten und gegenüberstellen, wie diese Aspekte umgesetzt werden. Dropbox ist der Service mit der größten Verbreitung, der allerdings 2011 auch vermehrt in der Kritik war, nicht sorgsam genug mit den Daten seiner Nutzer umgegangen zu sein. Wuala, ist ebenso wie Dropbox, Closed Source, versucht allerdings durch client-seitige Verschlüsselung, Sicherheitsmängeln der Dropbox Infrastruktur zu umgehen. Syncany ist eine Open Source-Lösung, die im fortgeschrittenen Beta-Stadium ist und Nutzern ermöglichen soll ihre eigene Data-Cloud zu eröffnen.

2. Grundlagen von Online-Speicher

Mit der Auslagerung von Daten und Dateien vom lokalen Computersystem in die Cloud können viele Probleme des persönlichen Datenmanagements über verschiedene Orte und Plattformen angegangen werden. Über Services zur Dateisynchronisierung können Nutzer Dateien überall hin mitnehmen und jederzeit unterwegs verfügbar halten. Darin eingeschlossen ist nicht nur Lese-, sondern auch Schreibzugriff.

2.1 Cloud-Services

Der Service kann in 2 Elemente aufgeteilt werden: Die Cloud-Server-Infrastruktur, sowie die einzelnen Clients, die auf diese Infrastruktur zugreifen.

Die Cloud-Server bilden ein nach außen geschlossenes Netzwerk aus physikalischen Servern, die mittels Replikation und Datensynchronisation zusammengefasst werden. Die Cloud bietet definierte Interfaces über die von außen auf die Daten zugegriffen werden. Wie die Daten konkret in der Cloud abgelegt werden wird über diese Schnittstelle nicht weiter kommuniziert. Die Datenorganisation ist dabei unabhängig vom Client.

Der Client ist ein Anwendungsprogramm, das die Schnittstelle der Cloud bedient und aus der Cloud liest und zurück schreibt. Dieses Programm bietet dem Nutzer die eigentliche Funktionalität, die Cloud zur Datenverarbeitung bleibt im Hintergrund unsichtbar. Dieser Client kann auf verschiedenen Plattformen laufen und kann jeweils für den Zweck und den Anwendungsfall unabhängig von der Cloud-Infrastruktur angepasst werden.

Bei Online-Storage-System ist die Cloud die Infrastruktur in der Dateien des Nutzers persistent abgelegt werden, während die Clients des Nutzers auf verschiedenen Endgeräten verbunden sein können und auf die in der Cloud gehaltenen Dateien zugreifen können.

Diese Clients bieten viele Features, die zum komfortablen Gebrauch benötigt werden. Ziel ist dabei eine unaufdringliche Handhabe, mit der der Anwender diesen Service ohne Mehraufwand nutzen kann. Online-Speicher-Systeme sollten möglichst automatisiert ablaufen und Nutzereingaben unnötig zu machen. Die automatische Erkennung von geänderten Dateien, diese in die Cloud hoch zu laden und synchron zu halten, ist dabei eine wichtige Grundlage eines solchen Hintergrunddienstes. Auch Konfliktbehandlung bei konkurrierendem Schreiben wird vom System behandelt und gelöst. Nur in Ausnahmen muss der Nutzer eingreifen. Änderungen und Funktionsweise der Anwendungen sollten verständlich kommuniziert werden.
Clients können weiterhin zusätzliche Features wie automatische Backups anbieten. Je nach Implementierung kann ein Client ein eigenständiges Programm oder in das Betriebsystem integriert sein. Für Service-Anbieter relevant geworden ist inzwischen die Verfügbarkeit auf verschiedenen Plattformen um möglichst von allen Systemen aus - insbesondere auch mobilen Endgeräten - die Dateien des Nutzers zur Verfügung zu stellen.

Online-Storage ist daher Teil der größeren Idee des Nomadic Computing, die umfasst, dass der Anwender von kleinen Satelliten Computern umgeben ist und alle auf gemeinsame Datenbestände zugreifen. In diesem Moment ist auch der Terminus eines Thin-Client angebracht.

2.2 Online Storage Provider

Seit dem Jahr 2008 haben sich eine Vielzahl Dienste etabliert, die die beschriebene Dienstleistung - Online-Speicher in der Cloud - anbieten, und entsprechende Mittel zur Dateisynchronisation zur Verfügung stellen. Die Dienste unterscheiden sich sowohl in ihrer technischen Infrastruktur, als auch in ihrem Businessmodel und ihrer Einbettung. *Ubuntu One* und *MobileMe* dienen als Unterstützung der zugrundeliegenden Plattform und werden vom selben Hersteller – Canonical respektive Apple – angeboten; unabhängige Anbieter sind meist auf verschiedenen Plattformen vertreten. Die Systeme sind untereinander nicht kompatibel.
Aufgrund der Anzahl der Service-Dienstleister wurden für diese Arbeit drei exemplarische Dienste ausgewählt.

Dropbox[1] ist 2011 das verbreitetste Online-Storage-System. Die Installation und Konfiguration sind sehr einfach. Die Benutzeroberfläche gleichsam unaufdringlich und schlank in das Dateisystem integriert. Offizielle Clients für Dropbox gibt es für alle modernen Desktop-Betriebssysteme sowie die verbreitetsten mobilen Betriebssysteme iOS, Android und BlackBerry.

Wuala[2] basiert auf der theoretischen Schlüsselverwaltung Cryptree, die Studenten der ETH Zürich entwickelt und Wuala daraus gründeten. Wuala bietet einen Client in dem Dateien abgelegt und in einem verteilten Dateisystem in der Cloud abgelegt werden können. Dieser Client kann auch

1 Offizielle Webseite von Dropbox: http://www.dropbox.com
2 Offizielle Webseite von Wuala: http://www.wuala.com

Zugriff über das native Dateisystem als Netzlaufwerk zur Verfügung stellen. Automatische Synchronisierung und Backups können ohne Aufwand eingerichtet werden. Der Client ist verglichen zu Dropbox ein komplexer, bietet aber auch Raum für verschiedene Nutzungsszenarien.

Syncany[3] ist genau genommen kein Service-Anbieter, sondern ein Open-Source-Projekt, das eine Software anstrebt mit der Online-Storage Dienste selbst gehostet werden können. Dabei wird auf eine komplexe Cloud-Infrastruktur verzichtet. Im Client können eine Vielzahl hosting-basierter Speicherorte definiert werden[4] auf die die Daten verschlüsselt abgelegt werden.
Syncany ist Ende 2011 in aktiver Entwicklung und die Nightly Build aus dem Entwicklungsrepository kann getestet werden. Ein erster stabiler Release ist zum Zeitpunkt dieser Arbeit für Ende Januar 2012 angekündigt. Dieser Release enthält zunächst nur den Hintergrundservice und die Betriebssystemintegration. Eine grafische Benutzeroberfläche ist ebenfalls in Arbeit, ist aber niedriger priorisiert.

3. Datenschutz

Mit dem Auslagern von persönlichen Daten vom eigenen Computer in das Datennetzwerk eines externen Betreibers gibt man als Nutzer weite Teile der Verantwortung und Zugriffskontrolle ab. Gerade in geschlossenen Systemen muss der Nutzer dem Anbieter Vertrauen sorgsam mit seinen Daten um zu gehen. Um Anbietern nicht gänzlich blind vertrauen zu müssen geht es im Folgenden darum heraus zu arbeiten welche Probleme des Datenschutzes zu betrachten sind und welche Lösungen die ausgewählten Systeme bieten.

3.1 Anforderungen der Datensicherheit

Betrachtet man die Datensicherheit der Dienste sind zunächst einige Begriffsklärungen nötig um die Anforderungen an einen solchen Service festlegen zu können. Beim Datenschutz muss zwischen der Privatheit der Daten und der Datensicherheit unterschieden werden.

Ersteres, dem Schutz der Vertraulichkeit von Daten, unterliegt die Zugriffskontrolle und Absicherung von Daten vor dem unbefugten Zugriff Dritter. Das schließt Cracker, Firmenmitarbeiter, aber auch Sicherheitsbehörden ein.
Datensicherheit (data security) beschreibt dagegen vielmehr den technischen Schutz vor Veränderung, Manipulation und Löschung der Daten. Daten sollen nicht unbemerkt manipuliert werden können und auf einen solchen Versuch sollte die Software aufmerksam machen und diesen technisch Unterbunden.

Beide Aspekte können durch Kryptografie angegangen werden beispielsweise durch das Verschlüsseln und Signieren von Dateien.
Computer und die sensiblen Daten, die sie beinhalten bieten tiefe Einblicke in den Menschen und stehen unter besonderem Grundrechtsschutz, nicht zuletzt auch durch das Urteil des Verfassungsgerichtes zur Gewährleistung von Datenintegrität aus dem Jahr 2008. (BVerfG 2008)

Neben dem technischen Schutz der Daten gibt es Anforderungen, die ebenso relevant für die Auswahl eines Online-Storage-Providers sind, auf die in dieser Arbeit jedoch nicht weiter eingegangen wird. So ist der Schutz der Infrastruktur von hoher Bedeutung, einerseits der Schutz vor Einbrüchen und Datenlecks, andererseits auch vor technischem Versagen wie einem Serverausfall. Welche Faktoren können zu einem Ausfall der Cloud führen, welche Schwachstellen

3 Offizielle Webseite von Syncany: http://www.syncany.org
4 Darunter fallen Lokale Speicherorte im Netzwerk, FTP, Amazon S3, Google Storage und weitere Dienste, die auf offiziellen Seite gelistet sind.

in der Infrastruktur gibt es? Wie Redundant ist das System und wie Redundant werden die Daten bereit gehalten? Diese Aspekte sind von außen schwer zu beurteilen, da Provider wenig Auskunft darüber bereitstellen. Wenn es um sensible Daten geht, ist jedoch gerade auch die Informationspolitik ein wichtiges Kriterium.

4. Grundlagen der Kryptografie

Um die definierten Anforderungen zu erfüllen bedarf es der Kryptografie zum Verschlüsseln der Daten, zum Sicherstellen der Konsistenz und der Zugriffskontrolle.
Bei der angewandten Kryptografie zu betrachten und zu unterscheiden sind die Datenverschlüsselung und die Schlüsselverwaltung.

Von Bedeutung für die Datenverschlüsselung sind der Schlüssel, der Verschlüsselungsalgorithmus und der Verschlüsselungsmodus. In der Krypto-Analyse gilt das Prinzip, das die Sicherheit eines kryptographischen Systems vom Schlüssel ausgehen soll und nicht vom Algorithmus (Schneier 1996, p5). Ein Schlüssel muss unter allen Umständen geheim bleiben, wohingegen der Algorithmus öffentlich und hinlänglich erprobt sein sollte.

4.1 Datenverschlüsselung

Bei der Datenverschlüsselung sind zum einen der Verschlüsselungsalgorithmus und der Verschlüsselungsmodus relevant. Verschlüsselungsalgorithmen gibt es eine Vielzahl die sich in der Praxis bewährt haben darunter AES, Blowfish und weitere. Der Algorithmus allein sagt jedoch wenig über die Qualität der Verschlüsselung aus, sondern ist vielmehr eine Designentscheidung zwischen Geschwindigkeit und Härte. Wie der Algorithmus angewendet wird und wie sicher diese Anwendung ist hängt vom Verschlüsselungsmodus ab.

Der Verschlüsselungsmodus beschreibt, wie ein Stream von Daten verschlüsselt werden soll. Verschlüsselungsmodi(Mode of operation) werden auch Ciphers genannt. Daten werden bei Blockcipher-Verfahren in Blocks konstanter Größe aufgeteilt und jeder Block einzeln verschlüsselt. Wird jeder Block mit dem selben Algorithmus und demselben Schlüssel verschlüsselt, so können auch in der resultierenden verschlüsselten Datei noch Muster gefunden werden, da gleiche Blöcke das gleiche Resultat liefern. Eine schlechte Cipher kann es einem Angreifer mithin ermöglichen den verwendeten Schlüssel zu errechnen. Eine gute Cipher erwirkt, dass jeder Block durch ein definiertes Protokoll individuell verschlüsselt wird. Für die Cipher selber gilt, was schon für den Algorithmus galt: Die Cipher sollte öffentlich, dokumentiert und erprobt sein. Die Sicherheit zieht eine gute Cipher einerseits aus dem zugrundeliegenden Schlüssel und der Zufälligkeit des Initialisierungsvektor. (Schneier 1996, p166)
Der Initialisierungsvektor (IV) ist ein zufälliger Ausgangswert, der bei der Cipher als Initialisierungsseed zum Verrauschen des ersten Blocks dient. Der IV hat dieselbe Länge wie ein Block. Initialisierungsvektoren können ebenso öffentlich sein.

Je nach Cipher-Implementierung können Initialisierungsvektor, Schlüssel, Blöcke und Blocksignaturen eingesetzt werden um jeden Block einzeln zu verschlüsseln und später wieder entschlüsseln zu können.
Verbreitete Cipher sind beispielsweise die Electronic Codebook (ECB) und das Cipher-Block-Chaining (CBC). ECB beschreibt dabei den einfachsten Modus, in dem jeder Block einfach mit dem Schlüssel verschlüsselt wird. ECB hat das Problem, dass identische Blöcke den selben Ciphertext erzeugen und damit wieder erkennbare Muster bei der Verschlüsselung entstehen. Andere Cipher wie beispielsweise CBC umgehen dies. Beim CBC wird der Klartext des Blocks zunächst mit dem Initialisierungsvektor XOR gerechnet und anschließend mit dem Schlüssel

verschlüsselt. Der resultierende Ciphertext wird als Initialisierungsvektor für die Berechnung des nächsten Blocks durchgeführt. (Schneier 1996, p168-171)

4.2 Schlüsselverwaltung

Neben dem Verschlüsselungsalgorithmus ist der benutzte Schlüssel und die dahinterstehende Schlüsselverwaltung sehr wichtig. Hier kann unterschieden werden zwischen dem privaten Hauptschlüssel des Nutzers, der zur Authentifizierung des Zugriffs auf die Nutzerdaten dient und der abgeleiteten Schlüssel, die im Hintergrund zur Sicherung des Dateibaumes und der Zugriffskontrolle dienen.

Die Schlüsselverwaltung bei Online-Storage hängt an der einzelnen Implementierung, grundsätzlich ist das Verschlüsselungsverfahren aber immer symmetrisch. Mit einem Schlüssel wird eine Datei verschlüsselt und mit dem selben Schlüssel wieder entschlüsselt. Dieses einfache Prinzip wird komplizierter wenn es um die Zugriffsverwaltung verschiedener Nutzer geht. In dem Fall muss für jedes Verzeichnis oder jede Datei ein eigener Schlüssel verwendet werden, der allen Teilnehmern bekannt ist. Diese Komplexität zu reduzieren versuchen Schlüsselverwaltungsverfahren wie Cryptree, das von Wuala benutzt wird und auf das später noch eingegangen wird.

Der private Schlüssel des Nutzerkontos ist das wichtigste Sicherheitselement des Systems und sollte daher gut gewählt in Länge und Komplexität sein. Wer Zugriff auf diesen Schlüssel hat, hat letztlich Zugriff auf alle Daten des Systems, daher sollten Schlüssel und verschlüsselte Daten getrennt voneinander abgelegt werden. Liegt der private Schlüssel beim Online-Storage-Provider so ist die Konsequenz, dass dieser Zugriff auf die verschlüsselten Daten hat und sich im Falle von Datenlecks auch Andere Zugriff verschaffen können. Die Schlüsselqualität hängt dabei von der Bitlänge des Schlüssels ab.

5. Kryptographische Implementierung

Die vorgestellten Online-Storage-Dienste benutzen alle einen kryptographischen Unterbau zur Sicherung der Daten in der Cloud. Im folgenden Abschnitt wird soweit möglich auf kryptographische Implementierungen geschaut und festgehalten, wo es Schwachstellen im System gab, die inzwischen aufgelöst wurden.

5.1 Dropbox

Dropbox ist ein geschlossenes System mit sehr wenig öffentlicher Dokumentation über die technische Implementierung, insbesondere der verwendeten Kryptografie[5]. Krypto-Analytiker sind daher auf Blackbox-Testing und Reverse-Engineering des Dienstes angewiesen um Aussagen über die Sicherheit treffen zu können. Die Beschreibung des Dienstes bezieht sich auf eine solche Analyse, die im Juni 2011 vorgestellt wurde. (Mulazzani et al 2011)

Der Dropbox Client verhält sich sehr schlank und enthält nur wenig kryptographische Logik. Der Client identifiziert sich bei Dropbox mittels Benutzername und Passwort und erhält vom Server eine Host-ID zugeteilt, über die er sich zukünftig immer authentifiziert. Einer Datei, die bei Dropbox hochgeladen werden soll wird zunächst mit einem nicht-öffentlichen Hash-Algorithmus die Signatur der Datei gebildet. Dieser Hash wird an den Server geschickt um zu überprüfen, ob die entsprechende Datei bereits hochgeladen ist oder nicht. Wenn mit diesem Hash bereits eine Datei vorhanden ist, wird dem Nutzer diese online zur Verfügung gestellt ohne dass die Ursprungsdatei

5 Bereitgestellte Dokumentation über die Kryptografie von Dropbox: http://www.dropbox.com/security

hochgeladen wird. Gibt es für diesen Hash noch keine Datei, wird über einen SSL-Kanal die unverschlüsselte Datei auf den Dropbox-Server geladen, wo die eigentliche Kryptografielogik zum Einsatz kommt. Dort wird erneut ein Hash gebildet um die Konsistent der Datei sicher zu stellen und anschließend wird sie mit dem privaten Schlüssel des Nutzers verschlüsselt und in der Wolke abgelegt.

Aus diesem Ablauf ergeben sich einige Punkte, die Sicherheitstechnisch relevant sind und genauer beleuchtet wurden.
Zum Ersten ist es wichtig nachzuvollziehen, dass der private Schlüssel des Nutzers nicht beim Benutzer, sondern auf dem Server des Betreibers abgelegt ist und zunächst auch nur dort verwendet wird. Aus Sicht von Dropbox wird dies als Feature kommuniziert, da somit eine Passwortwiederherstellung und Dateiwiederherstellung ermöglicht werden kann, indem alle Daten temporär entschlüsselt werden, ein neuer Schlüssel generiert und die Dateien neu entschlüsselt werden können. Gleichzeitig erlaubt es dem Service aber auch beim Hochladen und nach der Verschlüsselung die Rohdaten zu entschlüsseln, was bei Strafverfolgungsbehörden bereits benutzt wurde. (Dan Moren 2011) Es ist festzuhalten, dass auch wenn die Daten verschlüsselt auf dem Server liegen, die Möglichkeit des Einlesens gegeben ist und somit auch Datendiebstahl ein Thema werden kann.

Dropbox' Authentifizierung mittels Host-ID ist ein weiterer kritischer Punkt der bereits seit zwei Jahren kritisiert wird. Auf jedem System, auf dem der Dropbox-Client installiert ist wird eine config.db Konfigurationsdatei angelegt, die neben dem Benutzernamen und diversen Konfigurationseinstellungen auch die Host-ID enthält. Dies ist eine Geräte-eindeutige, anhand derer die Authentifizierung abläuft. Ist diese ID für ein Benutzerkonto aktiviert, so kann der Client ohne weitere Authentifizierung auf die Daten des Nutzerkontos zugreifen. Das gilt auch, wenn die config.db auf ein anderes System kopiert wurde und der Client hier ausgeführt wird. (Mulazzani et al 2011, p4)

Eine weitere Schwachstelle liegt in der Datei-Erkennung mittels privaten Hash-Algorithmus. Dieser Algorithmus benutzt die Hash-Funktionen der OpenSSL-Bibliothek und es ist gelungen eine modifizierte Bibliothek einzubinden, die manipulierte Hashs schickt. Somit kann am Server gefragt werden, ob bestimmte Hashs bereits hochgeladen wurden. Experimentell konnte so überprüft werden ob bekannte Dateien ins Netzwerk hochgeladen wurden oder nicht (confirmation attack). Mithilfe des modifizierten Hash-Algorithmus konnte weiterhin Zugriff auf Dateien mit dem modifizierten Hash erlangt werden. Jeweils ist dieses Verfahren nicht tauglich um explizit Dateien ab zu fischen, aber es zeigt Lücken, die fremden Zugriff nicht ausschließen lassen. (Mulazzani et al 2011, p4)
Das Verfahren Dateien, die bereits hochgeladen wurden, nicht wieder hoch zu laden, sondern den Zugriff darauf zu erlauben heißt Deduplikation. Es dient der Verringerung von Traffic und benötigtem Speicherplatz in der Cloud.

Ebenfalls an der Implementierung der Hash-Funktion – allerdings serverseitig – hängt die Möglichkeit Slack-Space, anonymen Speicherraum in der Wolke zu nutzen. Wird eine Datei im Dropbox-Dateisystem gelöscht, so wird nur die Verlinkung auf die Datei gelöscht, jedoch nicht die physische Datei in der Cloud. Kennt man den Hash der Datei, so kann auch nach der Löschung weiterhin die Datei geladen werden. Dies erlaubt es beliebig viel Speicher zu benutzen und anonym Dateien zu tauschen.(Mulazzani et al 2011, p7)

Laut der Analysten, die diese Schwachstellen zusammengetragen haben wurde Dropbox informiert und Wege zur einfachen Lösung bereitgestellt. Dropbox soll darauf hin einen Quickfix eingespielt

haben, über weiter gehende Änderungen der Infrastruktur ist im Anschluss nichts bekannt geworden.

Laut offizieller Dokumentation werden Dateien mittels AES-256 verschlüsselt. Dabei ist jedoch nicht bekannt über welchen Mode of Operation.

5.2 Wuala

Im Gegensatz zu Dropbox geht Wuala offen mit der verwendeten Kryptografie um. Zwar ist der Source-Code nicht-öffentlich, so wurden dennoch Krypto-Analytiker zu Code-Reviews eingeladen. Desweiteren haben Mitarbeiter von Wuala Arbeiten herausgegeben und Vorträge über Cryptree, die Theorie hinter Wualas Schlüsselverwaltung gehalten. (Meisser et al, 20)

Cryptree ist ein Verfahren zur Verwaltung von Schlüsseln eines Dateisystems. Dieses Verfahren soll Schreib- und Lesezugriffe auf veränderliche Verzeichnisse definieren. Die Veränderlichkeit ist dabei ein wichtiges Element, da Dateien wie auch Verzeichnisse in Dateibäumen verschoben werden können und sich dadurch Zugriffsrechte – insbesondere Zugriffsrechte zusätzlicher Personen – ändern. Cryptree definiert dabei eine doppelte Baumstruktur, die die Verzeichnisse abbildet. Jeder Knoten dieser Baumstruktur entspricht einem Verzeichnis und besitzt einen Schlüssel. Dieser Schlüssel ist regressible (regressible keys), was eine Methode ist Schlüssel zurück zu ziehen und neu vergeben zu können, ohne Daten neu verschlüsseln zu müssen, da der alte Schlüssel aus dem neuen Schlüssel zurückgerechnet werden kann. Die Knoten zwischen den Verbindungen sind Kryptografische Verlinkungen (cryptographic links), die eine Rechtevererbung ermöglichen. Ein Nutzer der Zugriff auf einen Schlüssel K1 hat, bekommt mittels einer kryptografischen Verlinkung auch Zugriff auf den verlinkten Schlüssel K2.

Die Cryptree Schlüsselverwaltung wird serverseitig zur Verwaltung der Zugriffsschlüssel benutzt. Unabhängig davon wird die hochgeladene Datei bereits client-seitig mit dem privaten Schlüssel des Nutzers verschlüsselt. Dieser private Schlüssel setzt sich zusammen aus Benutzername und Passwort, was einerseits einen guten Schlüsselgenerierungsalgorithmus und vom Nutzer eine gute Passwortwahl erfordert um die Sicherheit zu erhöhen. Durch die client-seitige Verschlüsselung hat der Dienst Wuala keine Möglichkeit ohne den privaten Schlüssel an die hochgeladenen Daten zu kommen. Was sich Wuala jedoch vorbehält ist die Hashs einer Datei zu speichern und damit Dateien, die illegale Inhalte haben zu sperren und unzugänglich zu machen. (Meissner 2011)

Deduplikation wird auch bei Wuala angewandt, indem Dateien zunächst mit einen eindeutigen Schlüssel basierend auf dem eindeutigen Hash der Datei lokal verschlüsselt werden. Dieser eindeutige Schlüssel wiederum wird mit dem privaten Schlüssel des Nutzers verschlüsselt[6]. Wenn die verschlüsselte Datei in die Wuala-Cloud geladen wird kann dort der Hash der verschlüsselten Datei herangezogen werden um zu überprüfen, ob bereits eine verschlüsselte Datei, die genau diesen Hash erzeugt vorhanden ist.

Auch bei Wuala gab es anfangs während der Beta-Phase 2008 Kritik bezüglich einiger kryptographischen Implementierungen. Diese bezogen sich allerdings weniger auf das Gesamtkonzept als vielmehr einzelner Implementierungsentscheidungen, die seitdem korrigiert wurden. Beispielsweise wurden Dateiblöcke ursprünglich mittels ECB-Cipher verschlüsselt, was später jedoch auf CBC geändert wurde. Anfänglich galt auch der Schlüsselgenerierungsalgorithmus auf Basis von Nutzername und Password als schwach, weil er zu schnell war, was Brute-Force-Attacken einfacher machte. (Percival 2008)

6 Diskussion zum Thema Deplublikation bei Wuala: https://bugs.wuala.com/view.php?id=3339

Potentielle Angriffsstellen gibt es weiterhin und die Programmierer von Wuala diskutieren sehr offen zu Sicherheitsfragen und erläutern auch wo gegebenenfalls Trade-Offs zwischen Benutzbarkeit und ultimativer Sicherheit gegenüber unwahrscheinlichen Angriffsszenarien gemacht wurden[7].

5.3 Syncany

Syncany ist eine Open Source Lösung zum Synchronisieren von Dateien über verschiedene Plattformen unter Benutzung eigener Speicherorte. Syncany ist im Gegensatz zu Dropbox und Wuala kein Dienstleister der eine Cloud zur Datenspeicherung anbietet und die Datensicherheit gewährleistet, sondern eine Software, die es erlaubt selber die Einrichtung, Konfiguration, und Gewährleistung der Sicherheit zu übernehmen. Dies ist über Sicherheitsbewusste fortgeschrittene Nutzer und Firmen interessant, die privaten Daten nicht an einen fremdbetreuten Service geben wollen, können oder dürfen und daher selber eine solche Online-Storage-Lösung betreiben wollen.

Synany ist in Java implementiert und greift auf bestehende Kryptografie-Bibliotheken wie Bouncy-Castle und des Java6-Framework zurück, die ihrerseits Open-Source und etabliert sind.
Da es keinen Online-Service gibt, der Konto-Informationen bereitstellt, läuft die gesamte Konfiguration über lokale Konfigurationsdateien auf dem lokalen System des Nutzers.
Es können darin beliebig viele Profile definiert werden, die beschreiben wohin und wie ein synchronisierter Ordner verschlüsselt abgelegt werden soll. Mittels Plugins werden Verbindungen zu verschiedenen Speicherprovidern bereitgestellt, so dass die verschlüsselten Blöcke im lokalen Dateisystem, wie auch FTP, Amazon S3 und andere Dienste, abgelegt werden können.
Syncany erlaubt eine genaue Konfiguration der Verschlüsselung, darunter die Auswahl des Verschlüsselungsalgorithmus und des Mode of Operation. Die Verschlüsselung erfolgt client-seitig und jeweils mit einem im Profil definierten Schlüssel. Diese Konfigurationsdatei ist von hoher Sicherheitsrelevanz, da Passwörter im Klartext enthalten sind und diese Datei vollen Zugriff auf alle Profile und Speicherorte gibt.

Syncany ist letztlich auf eigene Gefahr zu benutzen. Es erlaubt das Betreiben eines eigenen Online-Storage-Services was gleichermaßen bedeutet, dass der Nutzer nicht einem externen Dienstleister bei für die Gewährleistung der Datensicherheit vertrauen muss, es bedeutet aber auch, dass der Nutzer die Expertise haben muss um selber die Systemsicherheit gewährleisten zu können.

7 Wuala Sicherheitsdiskussionen zu Detailfragen findet man gleichermaßen im Bugtracker: http://bugs.wuala.com als auch im offiziellen Forum: https://forum.wuala.com/viewforum.php?f=34

6. Zusammenfassung

Bei Infrastrukturen die Daten von hohem persönlichem Wert halten und Schützen sollen gibt es keinen Weg vorbei an kryptografischen Lösungen. Wie bei allen Anwendungsgebieten der Kryptografie zeigt sich auch beim Online-Speicher, dass eine gute Implementierung immer eine Frage der akzeptierten Nachteile ist. Kryptografie erfordert immer mehr Speicher, Rechenzeit und Nutzersorgsamkeit je sicherer sie sein soll. Besonderes Letzteres ist ein wichtiger Erfolgsfaktor von Systeme, die einerseits einen sicheren Service bieten soll, andererseits für den Nutzer am besten unsichtbar erscheinen. Das System soll ihn an die Hand nehmen und leicht vermitteln, wie es selbst sicher zu halten ist und frappante Fehler des Nutzers vermeiden. Für jedes System gilt es die richtige Balance aus bevormundeter und selbstbestimmter Nutzung des Anwenders. Bei Online-Storage liegt diese Balance darin ein System anzubieten, dass dem Nutzer sicheren Dateispeicher bietet, ohne durch Komplexität oder leicht zu begehenden Nutzungsfehlern Anwender zu verschrecken. Das System sollte sicherstellen, dass nicht durch Fehlbenutzung die gebotene Sicherheit kompromittiert wird.

Dropbox hat sich als Service dazu entschlossen die Kryptografie komplett vom Endnutzer zu entkoppeln unter der Maßgabe dafür ein System zu bieten, dass für jeden sehr schnell benutzbar ist. Der Trade-Off ist dabei, dass die Daten potentiell offen in der Cloud liegen. Die Gefahr liegt darin, dass durch die angewandte und beworbene Kryptografie ein falsches Gefühl für Sicherheit erzeugt wird, dem Dropbox nicht in dem Maße zu gestanden werden kann.

Wuala bedient eine sehr ähnliche Zielgruppe wie Dropbox, positioniert sich aber explizit als eine Alternative die Sicherheit und den Einsatz von Kryptografie zu einem Verkaufsthema macht. Wuala ist nicht frei von Trade-Offs, was Diskussionen zum Einsatz von Deduplikation zeigen. Wuala erfordert vom Nutzer einen bewussteren Umgang, da er selbst verantwortlich für seinen Zugangsschlüssel ist. Wuala kann kein Passwort zurücksetzen, da das Passwort Teil des Hauptschlüssels ist, der sich nicht verändern kann.

Einen anderen Anwendungsbereich verfolgt dagegen Syncany, das keine Fertiglösung bietet, sondern viel mehr das Werkzeug bildet sich selber eine Lösung zu konfigurieren. Damit ist es einerseits für viele private Endkunden uninteressant, gleichzeitig aber ein willkommenes Hilfsmittel für sicherheitsbewusste Nutzer oder Firmen, in denen externe Dienstleister nicht in Frage kommen. Syncany alleine kann nicht den Funktionsumfang der anderen vorgestellten Systeme bieten, aber als frei verfügbares Open-Source-Tool, kann es als ein interessanter weiterer Baustein für die eigene Infrastruktur werden. Der Trade-Off ist, dass es nicht massentauglich sein wird, da die Konfiguration von Speicherorten und der verwendeten Kryptografie nur Powerusern empfohlen werden kann und einfache Endnutzer im Zweifelsfall überfordert sind und mit schlechten Einstellungen der Datensicherheit eher schaden als nutzen.

Syncany wird keine Konkurrenz zu Dropbox und Wuala, da die Software unter einer anderen Prämisse arbeitet und nicht an den vollumfänglichen Service, den beide anderen Systeme anbieten, heran kommen kann.

7. Literatur

- Bruce Schneier [1994] 1996: *Applied Cryptography*, Second Edition, John Wiley & Sons
- BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
- Christopher Soghoian 2011: „How Dropbox sacrifices user privacy for cost savings“, http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html
- Colin Percival 2011: „Wuala's improved security“, http://www.daemonology.net/blog/2008-11-07-wuala-security.html
- Dan Moren 2011: „Dropbox addresses privacy concerns“, http://www.macworld.com/article/159370/2011/04/dropbox_security.html
- Dominik Grolimund, Luzius Meisser, Stefan Schmid, Roger Wattenhofer 2006: “Cryptree: A Folder Tree Structure for Cryptographic File Systems”, Computer Engineering and Networks Laboratory (TIK), ETH Zurich, CH-8092 Zurich
- Luzius Meisser 2011: „Wuala's Encryption For Dummies“, http://wualablog.blogspot.com/2011/04/wualas-encryption-for-dummies.html
- Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, Edgar Weippl 2011: “Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space”, SBA Research