

Verschlüsselung von Cloudspeichern

Zusammenfassung

Cloud-Speicher sind oft unverschlüsselt. Sicherheitsbewusste Cloud-Nutzer/Innen setzen daher auf Verschlüsselungs-Tools - beispielsweise Cryptomator bietet sich als neue deutsche Open-Source-Alternative an.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörernde**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**

DFN-Cloud

Cloud-Dienste für die Wissenschaft

Gemeinsam Potentiale erschließen

Cloud-Dienste für die Wissenschaft unterliegen besonderen Anforderungen, seien es Fragen der Informationssicherheit, der Performance, der Skalierbarkeit oder der Anpassungsfähigkeit an die Prozesse in Forschung und Lehre. Auf alle diese Aspekte sind je nach Anwendungszweck passende Antworten zu finden. Vor diesem Hintergrund organisiert der DFN-Verein eine Cloud für die Wissenschaft (DFN-Cloud).

Viele wissenschaftliche Einrichtungen haben große Erfahrung mit der Bereitstellung von Cloud-Diensten. Der DFN-Verein schafft für diese Einrichtungen einen Rahmen, in dem diese Cloud-Dienste von allen Teilnehmern/Innen am DFN-Verbund genutzt werden können. In entsprechenden Forschungsvorhaben bringt der DFN-Verein dabei die beteiligten Partner/Innen zusammen, um die DFN-Cloud zu nutzen, zu erproben und ständig weiterzuentwickeln.

In diesem Sinne sind alle Einrichtungen im DFN-Verbund eingeladen, die hier vorgestellten Cloud-Dienste zu nutzen und mit ihren Erfahrungen beim Einsatz der Cloud-Dienste an der Weiterentwicklung der DFN-Cloud mitzuwirken.

Fünf Schritte in die Cloud

Für den Weg in die DFN-Cloud sind fünf Schritte erforderlich. Diese sind in der folgenden Präsentation kurz erläutert: [In fünf Schritten in die DFN-Cloud](#).

Bei weiterem Interesse an den Diensten der DFN-Cloud wenden Sie sich bitte an die Geschäftsstelle: [Michael Röder](#).

Andere kommerzielle Anbieter und Lösungen

Der Markt für Verschlüsselungslösungen ist unübersichtlich geworden - es gibt Software für **Festplattenverschlüsselung**, **E-Mail-Verschlüsselung** und mehr.

Für populäre Cloud-Speicher wie Google Drive oder Dropbox sind Zusatztools vonnöten - wie das kommerzielle **Boxcryptor**.

Aber auch aus dem Open-Source-Lager gibt es eine neue Alternative - **Cryptomator von SetLabs aus Bonn**. Die Software ermöglicht die Erstellung von beliebig vielen, als Tresoren bezeichneten Containern, die derzeit an beliebiger Stelle auf Desktopsystemen erstellt werden können und via OneDrive, Google Drive, Dropbox und iCloud synchronisiert werden können.

Auf praktisch jedem Gerät, das Anwender/Innen heute für ihre täglichen Arbeit, aber auch in ihrer Freizeit benutzen, entstehen Daten und Dateien, die sensitive Informationen enthalten. War das klassische Arbeitsgerät noch vor wenig mehr als zehn Jahren der heimische PC oder das Gerät am Arbeitsplatz, so entstehen heute schützenswerte Informationen auch auf mobilen Geräten, wie Mobiltelefonen, Tablets oder Notebooks. Der Schutz dieser Informationen vor der unerwünschten Einsichtnahme nicht berechtigter Dritter ist eine stetige und konkrete Herausforderung für jede/n Anwender/In moderner IT-Systeme im privaten wie im beruflichen Kontext.

Das Verlangen nach einer vertrauenswürdigen und sicheren Speicherung vertraulicher, geheimer oder aus sonstigen Gründen schützenswerter Daten und Dateien hat zu einer Vielzahl von Lösungen geführt, mit denen Anwender und Anwenderinnen unterschiedliche Aspekte ihrer persönlichen Sicherheit und Privatsphäre schützen können. Die Verschlüsselung ganzer Festplatten ist heute, etwa mit Microsofts Bitlocker oder Apples FileVault, in modernen Betriebssystemen vorgesehen. Für interessierte Anwender/Innen existieren Ende-zu-Ende-verschlüsselte Nachrichtensysteme wie "Signal" und auch die Inhalte der klassischen E-Mail sind heute mit vertretbarem Aufwand via S/MIME oder GPG (Gnu Privacy Guard) zu verschlüsseln, auch wenn hier noch viel Nachbesserungsbedarf mit Blick auf die Anwenderfreundlichkeit und den Schutz von Metadaten besteht, insbesondere der Mailheader.

Bei der Auswahl des jeweiligen Werkzeuges ist mit Sicherheit auch als entscheidender Aspekt zu berücksichtigen, ob die verwendete Software als kommerzielle Lösung und insbesondere als closed source entstanden ist oder ob sie auf der Implementation offener Standards beruht, in ihren Schlüsselkomponenten offengelegt und damit unabhängig validierbar ist, etwa als Open Source. Berichte haben in der Vergangenheit schon die Annahme nahegelegt, dass auch kommerzielle Produkte durch Einflussnahme Dritter in ihre Sicherheit durchaus absichtlich geschwächt worden sein könnten. Bei der Auswahl und Beurteilung von möglichen Lösungsalternativen kann beispielsweise die kontinuierlich gepflegte Website privacytools.io gute Dienste leisten.

Abgesicherter Cloudspeicher als Herausforderung

Gerade für die Anwender und Anwenderinnen mehrerer Endgeräte (Desktop und Tablet, Desktop-PC und Notebook usw.), aber auch als einfacher Mechanismus für ein kontinuierliches Backup entstehender Anwenderdateien, haben sich die oft kostenlosen oder im Einsatz sehr günstigen Cloud-Speicher-Dienste erwiesen. Die Nutzung von Dropbox, Box, Google Drive oder Microsofts OneDrive ist für viele heute schon eine Selbstverständlichkeit. Der grundlegende Zugang zu diesen Systemen kann heute schon vorbildlich über Zweifaktor-Authentifizierung geschützt werden, wobei die Aktivierung dieses zusätzlichen Schutzmechanismus jedem Anwender und jeder Anwenderin solcher Dienste nur angeraten werden kann. Ohne weitere Schutzmaßnahmen sind aber die Daten auf den jeweiligen Systemen nicht vor der Einsichtnahme Dritter geschützt. Hier werden den jeweiligen Anbietern des Dienstes ein großer Vertrauensvorschluss gewährt. Und auch das eigentlich komfortable Feature zum Teilen von Verzeichnissen zur gemeinschaftlichen Nutzung mit vertrauenswürdigen Personenkreisen kann im Zweifelsfall auch schon einmal zu einer ungewollten Veröffentlichung eigentlich privater Dokumente führen.

Um Dateien wirklich sicher in der Cloud zu lagern, müssen die Daten schon auf dem eigenen Rechner verschlüsselt werden und der Schlüssel darf dem Anbieter nicht bekannt sein. Ein Unternehmen, das mit einer solchen Speicherlösung wirbt, ist zum Beispiel die Firma Lacie mit ihrem Angebot Wuala. Die zugehörige Software für Windows, Mac, Android und iOS-Geräte schickt nur fertig verschlüsselte Dateien in die Cloud. Fünf Gigabyte sind kostenlos, mehr Speicherplatz kostet Geld.

Aber auch bei anderen Anbietern lässt sich mit Hilfe eines kostenlosen Programms eine sichere Verschlüsselung nachrüsten - zum Beispiel mit Truecrypt. Mit diesem Programm lassen sich ganze Festplatten verschlüsseln oder aber sogenannte Datei-Container anlegen. Diese lassen sich wie ein ganz normales Laufwerk in das System einbinden.

Zero-Knowledge: Ich weiß von nichts

Um dem entgegenzuwirken, haben sich alternative Dienste und ergänzende Zusatzwerkzeuge etabliert, die einen sicheren Speicherort in der Cloud ermöglichen. Gemeinsam ist diesen Werkzeugen, dass sie dafür sorgen, dass die Daten auf dem Gerät des Anwenders erst verschlüsselt werden, bevor sie auf dem Speicherdienst hochgeladen werden. Ver- und Entschlüsselung sind damit client-seitig. Die Verwaltung der notwendigen Geheiminformationen in Form von Passwörtern (als Basis der Erstellung der notwendigen Schlüssel) obliegt dem Anwender/ der Anwenderin selbst. Der Cloud-Speicherdienst kennt damit weder die unverschlüsselten Daten noch den Schlüssel oder das Passwort.

Zieht man die Analogie zu der derzeit laufenden Diskussion bezüglich der Entschlüsselung eines iPhones durch Apple auf Anforderung durch das FBI, erübrigt sich durch die eingesetzte Technik der Weg zum Cloud-Provider zur Herausgabe entschlüsselter Daten - diesem liegen die Schlüssel zu keinem Zeitpunkt vor, er kann also nur verschlüsselte Daten herausgeben. Dieses Prinzip wird auch als Zero-Knowledge bezeichnet, ein Begriff der anteilig auch von Edward Snowden geprägt wurde. Die Umsetzung dieses Prinzip sorgt dafür, dass selbst ein böswilliger Systemadministrator auf der Seite der Cloud-Plattform keinen Zugriff auf unverschlüsselte Daten und damit eine Chance zur Verletzung der Privatsphäre der Anwender hat. Als vollständige Alternative und eigenständiger Cloud-Dienst hat sich beispielsweise **Spideroak** etabliert, das eine kommerzielle, verschlüsselte Cloud-Speicherplattform anbietet (kostenpflichtig nach 60 Tagen Test).

Ein Fraunhofer-Institut und die IT-Firma Sirrix haben die Software PanBox entwickelt, die eine durchgehende Verschlüsselung für Cloud-Speicher bietet und "laientauglich" sein soll. Ohne Handbuch kommt der Laie aber wohl nicht aus.

Das Open-Source-Tool [PanBox](#) verschlüsselt Dateien lokal, ehe sie bei einem Cloud-Speicher wie Dropbox hochgeladen werden. Nach dem Herunterladen werden sie transparent wieder entschlüsselt. Das soll auch mit mehreren Nutzern und Geräten funktionieren. Entwickelt wurde PanBox von Fraunhofer-Institut für sichere Informationstechnologie (SIT) und der Saarbrücker [Sirrix AG](#), unterstützt mit 640.000 Euro Fördermitteln von Bundesministerium der Justiz und für Verbraucherschutz (BMJV).

Panbox bindet sich mit Hilfe der Dokan-Bibliothek als Laufwerk ins System ein. PanBox soll "laientauglich" sein, wie Michael Herfert vom Fraunhofer-SIT gegenüber heise Security bei der Vorstellung des Programms in Berlin erklärte. Zum Einsatz kommt ein Public-Key-Verfahren. Der öffentliche Schlüssel eines Nutzers/ einer Nutzerin A soll dabei über eine Art Adressbuch an einen Partner/ einer Partnerin B verteilt werden, damit diese/r für den Empfänger/ die Empfängerin von Informationen die Daten zunächst verschlüsseln und eine Art Vorhängeschloss wie vor einer Schatztruhe anbringen kann. Mit dem zugehörigen privaten Schlüssel, der auf dem Gerät von A abgelegt wird, kann A dann dieses Schloss öffnen und auf die Daten zugreifen. Die gesamte Kontrolle über das Verfahren bleibe beim Nutzer/ der Nutzerin, versicherte Herfert: "Man braucht niemand, um Schlüssel zu verwahren oder Identitäten zu bestätigen".

Die in Java programmierte Anwendung unterstützt neben Dropbox auch andere Cloud-Anbieter, die einen Sync-Ordner auf der Festplatte einrichten. Sie steht derzeit für Windows 7 und 8, Linux und Smartphones mit Android bereit. Eine Version für Mac OS X und iOS "wollen wir herausgeben", erklärte Sirrix-Chef Ammar Alkassar. Dies hänge aber auch davon ab, wie die Lösung von den Nutzern und der Open-Source-Entwicklergemeinschaft angenommen werde.

Cryptomator als Open-Source-Alternative

Als spannende Alternative in diesem Bereich ist etwa seit der CeBIT 2016 das Bonner Unternehmen setoLabs mit seiner Lösung Cryptomator angetreten. Auch hier greift das Zero-Knowledge-Prinzip. Ein klares Alleinstellungsmerkmal ist die Tatsache, dass die Software als Open Source entwickelt wird und der Quelltext auf GitHub bereitgestellt ist. Damit ist insbesondere die Möglichkeit zum Code Review gegeben, so dass interessierte Anwender die Korrektheit der Software und das Nichtvorhandensein von Backdoors überprüfen können können.

Die Software ermöglicht die Erstellung von beliebig vielen als Tresoren bezeichneten Containern, die derzeit an beliebiger Stelle auf Desktopsystemen erstellt werden können und via OneDrive, Google Drive, Dropbox und iCloud synchronisiert werden können. Jeder Tresor findet sich als Unterverzeichnis auf dem jeweiligen Cloud-Dienst wieder, durch die Clientkomponente wird er bei Freischaltung als Laufwerk bereitgestellt (loop-back WebDAV, nur lokal). Das dokumentierte Sicherheitskonzept bietet neben der Kernfunktionalität "Verschlüsselung" weitere Schutzmechanismen für die Inhalte der Daten während der Speicherung in der Cloud: Um eine mögliche Einsichtnahme in Metadaten zu verhindern wird auch der Dateiname verschlüsselt und die Dateigröße der entstehenden Dateien wird verändert. Somit werden auch Rückschlüsse über die Art und den Inhalt der Dateien auf dem Speichersystem erschwert.

Die naheliegendste Möglichkeit ist es, Daten mit dem bekannten und sehr sicheren Verschlüsselungs-Tool **Truecrypt** zu kodieren. Um Truecrypt mit einem Cloud-Dienst richtig nutzen zu können, setzt das voraus, dass der Dienst nur geänderte Teile einer Datei aktualisiert, sonst muss jedes Mal die kompletten 100 MByte wieder hochgeladen werden. Das ist bei Dropbox, nicht aber bei Skydrive oder Google Drive der Fall. Beide "merken" nicht einmal, dass sich die Datei überhaupt geändert hat.

Sichere Cloud-Dienste

Wer sich ganz von Dropbox lösen will, wählt am besten einen Dienst, der von vornherein die Daten verschlüsselt. Dabei ist es wichtig, dass die Kodierung auf dem Rechner des Anwenders stattfindet und nicht erst im Web, denn sonst hat der Server-Betreiber den Schlüssel in der Hand. Die Kodierung auf dem eigenen Rechner hat natürlich einen Nachteil: Wenn man den Schlüssel (USB-Stick oder das Passwort) verliert, dann sind die Daten verloren.

Beispiele wären die Online-Speicher **Safesync, Hornetdrive, Mozy oder Wuala**. **Hornetdrive und Mozy** sind reine Cloud-Speicher, die meist als Backup Verwendung finden. Safesync und Wuala bieten auch Sync-Tools für Desktop und mobile Geräte. Kostenfreie Accounts gibt es bei Mozy (2 GByte) und Wuala (5 GByte). Der Anwender/ die Anwenderin braucht sich um die Verschlüsselung nicht zu kümmern, sie erfolgt automatisch.

Einsatz in der Praxis

Neben der Notwendigkeit eines Cloud-Accounts für die Synchronisation zwischen Geräten ist eine Registrierung oder ein Account bei Cryptomator natürlich weder notwendig noch sinnvoll. Mit dem Download und der Installation der Software liegt die Verantwortung für die Nutzung und Einrichtung beim Anwender/ der Anwenderin selbst.

Die Software ist derzeit für Microsoft Windows, Apple OS X, iOS, Linux und als Java JAR-File verfügbar, eine Version für Android ist in Aussicht gestellt. Die Desktop-Versionen sind als Download auf der Projekt-Website verfügbar, das Projekt kann durch eine Pay-What-You-Want-Option unterstützt werden, die iOS-Variante ist für wenige Euro im iOS-AppStore verfügbar.

Der Markt bietet sicherheitsbewussten Anwendern und Anwenderinnen heute viele Möglichkeiten, Dateien, die in öffentlichen Cloud-Speichern abgelegt werden sollen, vor der Einsichtnahme durch unberechtigte Dritte, auch beim Provider, zu schützen. Die in diesem Artikel genannten Systeme sollen nur als Beispiel dienen, die verfügbare Palette an Lösungen ist deutlich größer. Implementations-Alternativen für die jeweiligen Verschlüsselungsszenarien gibt es viele, nur "Nicht-Verschlüsseln" darf für informierte Anwender und Anwenderinnen keine Alternative mehr sein.

Ein mächtiges Werkzeug ist auch **VeraCrypt**. Mithilfe des Programms legen Sie sogenannte Container-Dateien an: Solche Dateien sind passwortgeschützt. Alle Dateien, die darin gespeichert werden, öffnen sich künftig nur noch nach Eingabe des definierten Geheimworts. Man legt einen VeraCrypt-Container im Cloud-Speicher ab, dann kann niemand außer den Nutzer/ der Nutzerin die enthaltenen Dateien verwenden.

AxCrypt: Dateien schnell verschlüsseln

AxCrypt ist darauf spezialisiert, einzelne Dateien zu verschlüsseln. Die Software bringt keine eigene Oberfläche mit. Das Verschlüsseln ist trotzdem ganz einfach: Es genügt, mit der rechten Maustaste auf eine Datei zu klicken und *AxCrypt, Verschlüsseln* zu wählen. AxCrypt bietet weniger Funktionen als **VeraCrypt** und ist deshalb sehr viel leichter bedienbar. Leider verschlüsselt das Tool aber keine Ordner: Das klappt nur über den Umweg, diese in ein ZIP-Archiv zu verfrachten.

Verwandte Artikel

- [Gruppenzertifikate beantragen und herunterladen](#)
- [Serverzertifikat für *.uni-jena.de-Domain beziehen](#)
- [Verschlüsselung von Cloudspeichern](#)

Titel: "Verschlüsselung von Cloudspeichern"

Stand: 01.01.2021

