# Verschlüsselte Backups mit Time Machine


Mit Time Machine hat Apple eine interessante und einfache Backup-Lösung in MacOS X Leopard integriert. Für meinen Geschmack ist Time Machine allerdings ein klein wenig zu »einfach« geraten. Es lassen sich beispielsweise leider keine Einstellungen zu den Backup-Intervalle vornehmen und Time Machine kann nur auf ein Backup-Medium sichern. Zudem kann Time Machine leider keine verschlüsselten Backups anlegen, was gerade für mobile Nutzer ein »No-Go« darstellen dürfte. Eine externe Festplatte mit den gesamten Backup-Daten unterwegs zu verlieren ist keine schöne Vorstellung.

## Vor- und Nachteile eines verschlüsselten Backups

Backups werden in den seltensten Fällen verschlüsselt. Das hat neben der oftmals fehlenden Möglichkeit einer sicheren Verschlüsselung in der eingesetzten Backup-Software auch oft praktischce Gründe: allgemein kann man sagen, dass ein verschlüsseltes Archiv anfälliger gegen Fehler ist. »Kippt« nur ein Bit, ist ein ganzer Block des Chiffrats unbrauchbar. In einem Klartext-Archiv betrifft ein solcher Fehler nur eine Datei — was auch schon schlimme Folgen haben kann, aber nicht zwangsläufig so einen großen Bereich betrifft. Desweiteren bringt eine Verschlüsselung immer Performance-Einbußen mit sich. Von dem administrativen Aufwand gar nicht erst zu sprechen.
Normalerweise werden Backups auch in »sicheren« Umgebungen gemacht. In Firmen wandern Backupmedien im Regelfall in den Tresor oder befinden sich in Räumen, die nur für wenige befugte Personen zugänglich sind — jedenfalls sollte es so sein. Denn warum sollte man sich die Mühe machen, einen Datenserver gegen unbefugte Zugriffe zu schützen wenn die Backup-Medien mit allen Daten einfach zugänglich sind. Zudem eine Backup-Bibliothek ja weit mehr als nur die reinen Daten enthält. Vielmehr ist ein Backup eine ganze Daten-Historie aus der ein böswilliger Mensch nicht nur den aktuellen Datenbestand sondern auch dessen Änderungen über Wochen, Monate oder sogar Jahre rekonstruieren kann!

Mobile Nutzer haben hier ein zusätzliche Problem. Wie das Backup der Notebook-Daten auf der externen Platte sicher vor fremdem Zugriff schützen? Da kann das Notebook noch so gut mit Fingerabdruck-Sensor, Passwort etc. abgesichert sein wenn ein Dieb einfach nur die kleine USB-Backup-Festplatte mitnehmen muss um freien Zugriff auf alle Daten zu haben.

Kann man Backup-Verschlüsselung im gut gesicherten Serverraum noch vernachlässigen so ist sie unterwegs essentiell wichtig und ein Muss!

## Time Machine

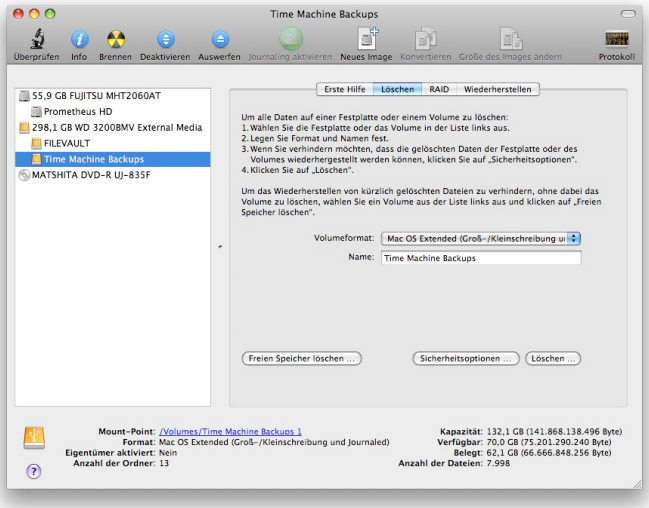
Leider bietet Time Machine keine Option an, um die Backups zu verschlüsseln. Gab es solch eine Einstellung noch in einem frühen Leopard ReleaseCandidate so ist sie mittlerweile wohl aus technischen und/oder ergonomischen Gründen verschwunden. Wahrscheinlich war das Handling von verschlüsselten Backups nicht ganz so einfach zu bewerkstelligen. Vielleicht kommt die Option nochmal zurück, aber bis dahin muss der Mac-Nutzer sich anders helfen.

Time Machine unterstützt Backups nur auf externe Hardware — z.B. eine USB-Festplatte oder die Apple Time Capsule. Einerseits wird so jeder Nutzer gezwungen, Backups auf ein externes Medium zu machen — was grundsätzlich keine schlechte Idee ist — andererseits beraubt Apple den Nutzer so um die für die folgende Anleitung nötige Flexibilität. Wäre nämlich Time Machine in der Lage, Backups auch in die unter MacOS X üblichen DiskImages zu sichern, könnte man einfach ein solches verschlüsseltes Image anlegen und man wäre fertig. Über ein paar Umwege geht es aber doch — und dabei kommt einem das Verhalten von Time Machine entgegen, bei Backups, die auf Netzwerklaufwerke oder die Time Capsule gemacht werdenb, eben doch ein solches DiskImage (SparseBundle) zu verwenden. Nur bei direkt am Rechner angeschlossenen Backup-Laufwerken besteht Time Machine auf eine HFS+-formatierte Partition um die zu sichernden Dateien 1:1 zu kopieren. In der folgenden Anleitung versuche ich, die Schritte, die nötig sind, um Time Machine in ein verschlüsseltes DiskImage auf einer USB-Platte sichern zu lassen — mit Hilfe es MacOS X Schlüsselbundes sogar voll automatisch wie man es von der normalen TimeMachine-Sicherung gewohnt ist. Allerdings sollte man schonmal mit dem Terminal und dem Festplattendienstprogramm gearbeitet haben.

# 0. Vorbereitung

Am Besten ist es, wenn wir mit einer frisch formatierten USB-Platte / Partition anfangen, damit keine störenden Reste von einem alten Backup mehr vorhanden sind. Zudem ist es sinnvoll, Time Machine in den Systemeinstellungen mit dem Schieberegler auf »Aus« zu stellen und erstmal zu deaktivieren.

Mit dem Festplatten-Dienstprogramm (Programme / Dienstprogramme) löscht man die gewünschte Partition und wählt als Volumeformat **MacOS Extended Groß-/Kleinschreibung (Journaled)**.




Benannt habe ich die Partition **Time Machine Backup** — hier kann sich jeder austoben wie er möchte.

Nachdem die Partiton gelöscht und mit einem neuen Dateisystem versehen wurde wenden wir uns wieder Time Machine zu. In den Systemeinstellungen weisen wir Time Machine unsere frische Partition als Backup-Laufwerk zu und starten ein Backup. Das Backup sollte aber nach ein paar Sekunden (10-20) in der Phase »Vorbereiten« abgebrochen werden. In dieser Zeit sollte Time Machine das Laufwerk schon mit einem »Cookie« versehen haben und es damit als gültiges

Backup-Medium markiert aber noch keine eigentlichen Daten gesichert haben. Nun kontrollieren wie nocheinmal, ob der Schieberegler in den Systemeinstelliungen noch auf »Aus« steht und öffnen im Finder unser Backup-Volume. Dort sollten wir einen Ordner »Backups.backupdb« vorfinden. Diesen Ordner befördern wir in den Papierkorb den wir dann im Anschluss direkt leeren.

# 1. Das DiskImage anlegen

Mit dem Festplatten-Dienstprogramm (Programme / Dienstprogramme) legt man nun ein neues, verschlüsseltes DiskImage an. Es sollte groß genug sein, um für das Backup nachher Platz zu haben. Damit Time Machine unser DiskImage auch als Backup-Image erkennt muss die Datei den richtigen Namen bekommen. Dieser setzt sich aus dem Namen des Rechners sowie der Mac-Adresse der Netzwerkkarte zusammen. Wer diese Angaben nicht kennt, findet die MAC- oder Hardwareadresse der Netzwerkkarte in den Systemeinstellungen / Netzwerk / Ethernet — oder meiner Meinung nach etwas einfacher über das Terminal (Programme / Dienstprogramme). Die folgenden Befehle zeigen die MAC-Adresse und den Rechnernamen:

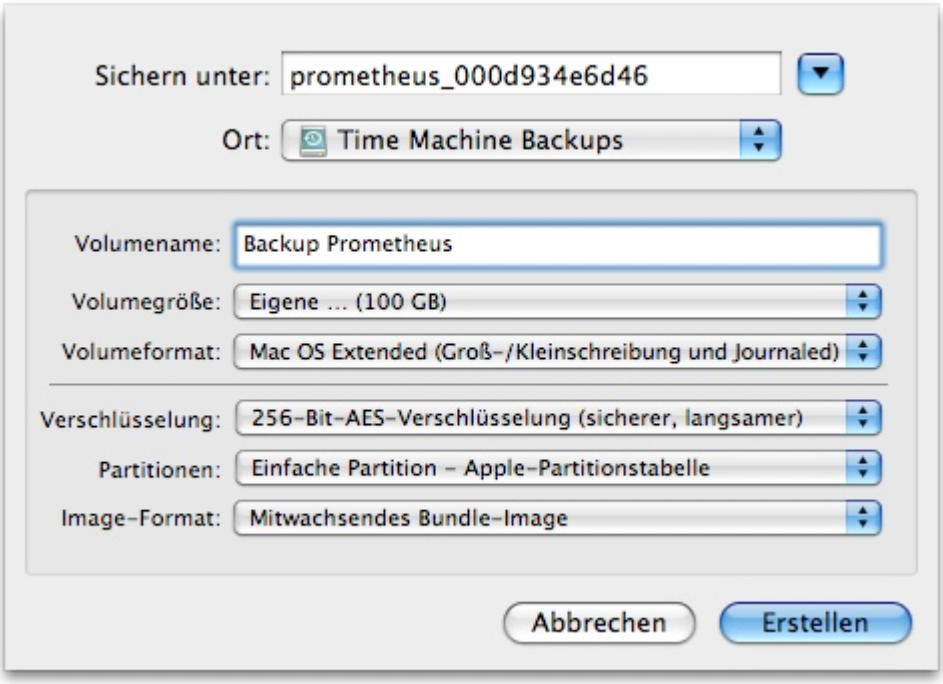
```
$ ifconfig en0 | grep ether
        ether 00:0d:93:4e:6d:46

$ hostname -s
prometheus
```

Laut diesen Angaben ist die Ethernet-Adresse meines MacMini also **00:0d:93:4e:6d:46** und der Rechnername **prometheus**. Diese Angaben werden wir im nächsten Schritt benötigen.

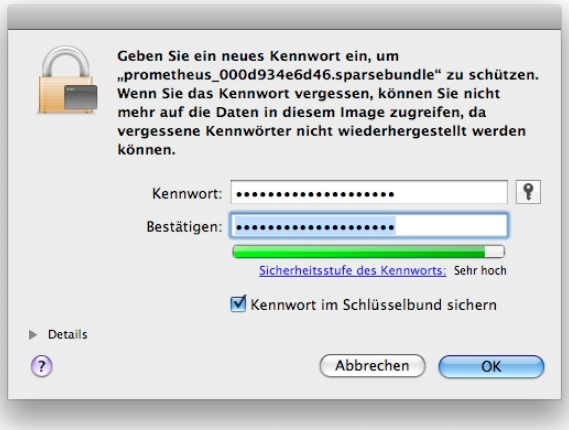
Im Festpatten-Dienstprogramm (Programme / Dienstprogramme) klicken wir auf »Neues Image«. Im darauffolgenden Dialog machen wir folgende Angaben:

| | |
|---|---|
| Sichern unter: | **prometheus_000d934e6d46** |
| | (setzt sich aus Rechnername und MAC zusammen) |
| Ort: | **Time Machine Backups** |
| | (unser Backup-Volume) |
| Volumename: | **Backup Prometheus** |
| | (kann beliebig gewählt werden) |
| Volumengröße: | groß genug ;-) |
| Volumeformat: | **Mac OS Extended** |
| Verschlüsselung: | z.B. **256-Bit-AES** |
| Partitionen: | **Einfache Partition** |
| Image-Format: | **Mitwachsendes Bundle-Image** |

(siehe Screenshot)




Nach dem Klick auf **Erstellen** wird man in einem Dialog zur Vergabe des Volume-Passworts aufgefordert. Hier sollte man sich Mühe geben und ein gutes Passwort wählen. Darauf achten, dass die Option »**Kennwort im Schlüsselbund sichern**« aktiviert ist. Danach geht's mit **OK** weiter.




## 2. System-Schlüsselbund anpassen

Damit Time Machine beim aktivieren des SparseBundle auch Zugriff auf das nötige Passwort hat muss man den im vorherigen Schritt gespeicherten Schlüsselbund-Eintrag in den System-Schlüsselbund kopieren.

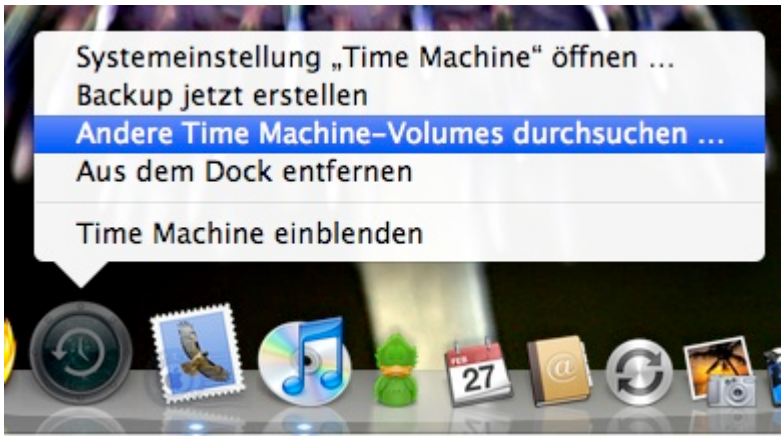
Dazu öffnet man die Schlüsselbund-Verwaltung (Programme / Dienstprogramme) und sucht im Anmelde-Schlüsselbund den Eintrag für das frisch erstelle Image. Dabei kann man die Suche benutzen indem man dort z.B. im hier vorgestellten Beispiel 'prometheus_00' eintippt. Man kopiert den kompletten Schlüsselbund-Eintrag und fügt ihn in den Sytemschlüsselbund wieder ein. Jetzt kann Time Machine unser Image öffnen.

## 3. Time Machine aktivieren / Backup durchführen

Bevor wir nun daran gehen ein erstes Backup zu versuchen sollten wir das verschlüsselte Volume erst deaktivieren, sofern es noch aktiv ist. Dann öffnen wir wieder die Systemeinstellungen für Time Machine und schieben den Regler auf »**Ein**« und starten ein Backup. Wenn alles geklappt hat sollte Time Machine nun das SparseBundle vorfinden und es aktivieren um dann dorthinein ein Backup zu erstellen. Nach der Sicherung wird das SparseBundle wieder deaktiviert — unser Backup auf der externen Festplatte steckt nun in einem AES-verschlüsselten Container! Lässt man die Platte nun am Rechner hängen sichert Time Machine ganz normal jede Stunde die geänderten Dateien — ganz automatisch wie wir das gewohnt sind.

# 4. Restore / Zeitreise mit Time Machine

Eine Wiederherstellung von Dateien mit Hilfe von Time Machine ist von Apple sehr nett gelöst, indem man die Applikation »Time Machine« startet und damit auf eine Zeitreise in die Vergangenheit geht. Leider findet das grafische Frontend das verschlüsselte Image nicht bzw. erkennt es nicht als Time Machine-Volume, selbst wenn man es vorher manuell aktiviert. Entweder man verzichtet auf die GUI und sucht sich die wiederherzustellenden Daten aus der im Backup-Volume angelegten Verzeichnisstruktur oder man behilft sich mit folgendem Trick. Apple hat Time Machine nämlich doch mit einer Option ausgestattet, andere Volumes als das autoatisch erkannte für die Zeitreise zu nutzen. Diese Option wurde allerdings (Apple-untypisch) gut versteckt.




Man muss erst das Time Machine-Symbol aus dem Programme-Order in das Dock ziehen. Im Kontextmenü des Symbols (Rechtsklick oder Ctrl-Maustaste) gibt es nun den Punkt »Andere Time Machine-Volumes durchsuchen …« — genau das, was wir wollen. Wählt man diesen Punkt kann man das (vorher manuell aktivierte) verschlüsselte Volume angeben und die Reise in die (Datei)Vergangenheit kann beginnen. Vielen Dank an Wladimir Schwenk, der mich auf diesen Trick aufmerksam gemacht hat.

# 5. Zum Abschluss

Durch die Nutzung von verschlüsselten Backup-Images erhöht man die Sicherheit ungemein. Man sollte allerdings das eigene Schlüsselbund-Passwort entsprechend sicher wählen (und auch das Passwort des Systemschlüsselbundes) damit jemand, der das Backup-Medium an den sichernden Rechner hängt nicht so schnell/keinen Zugriff erhält.

Ich hoffe, diese kleine Anleitung konnte denjenigen eine Hilfe sein, die mit Hilfe von MacOS

X-Bordmitteln auch unterwegs Backups erstellen wollen ohne dass man sich Sorgen um die Sicherheit der Daten machen muss. Diese Anleitung habe ich PPC G4 MacMini sowie einem Macbook jeweils mit MacOS X 10.5.5 getestet.