Mehrere Truecrypt Laufwerke/Container mit nur einem selben Passwort beim Start einbinden

Inhaltsverzeichnis

Problem

Man hat zwei, drei oder noch mehr Partitionen oder Container auf seinem Rechner, die mittels Truecrypt verschlüsselt sind und alle ein einziges (das gleiche) Passwort haben. Zum Einbinden muss dieses aber jedesmal eingegeben werden.

Lösung

Man kann die "Auto-Mount"-Funktion von Truecrypt benutzen oder sein eigenes kleines Skript (Linux) bzw. eine Batch-Datei (Windows) beim Systemstart ausführen lassen. Die Handhabung unter Mac OS sollte ähnlich zu den Linuxparametern sein.

Arbeitsumgebung

Diese Anleitung geht von einem bereits gestartetem System mit angemeldetem Benutzer aus. (Andernfalls lesen Sie bitte das Kapitel "Zur Benutzung des Loginpassworts".) Alle verschlüsselten Laufwerke liegen auf einer Festplatte. Natürlich können die Partitionen oder Container auch auf mehrere Festplatten verteilt sein, die Namen der Einhängepunkte verändern sich dann aber dementpsrechend.
Grundkenntnisse im Umgang mit Windows oder Linux und wie man ein Truecrypt-Laufwerk erstellt, sollten vorhanden sein. Diese Anleitung behandelt also die "nächste Stufe".

	Windows	Linux
1	unverschlüsseltes Betriebssystem (häufig auf Laufwerk C:\)	unverschlüsseltes Betriebssystem (im Bsp. ohne Swap-Partition)
	\Device\Harddisk0\Partition0	/dev/sda1
x	erweiterte Partition	
2	verschlüsseltes Laufwerk in erweiterter Partition (z.B. D:\)	/media/windows_d
	\Device\Harddisk0\Partition2	/dev/sda5
3	verschlüsseltes Laufwerk in erweiterter Partition (z.B. E:\)	/media/windows_e
	\Device\Harddisk0\Partition3	/dev/sda6

Warnung/Haftungsausschluss

Keylogger, Trojanische Pferde und andere Spyware könnten auf dem Rechner nach Passwörtern schauen. Die Benutzung von nur einem Passwort und/oder die Eingabe auf der Konsole geschieht **auf eigene Gefahr und Verantwortung**!

Linux

Getestet unter Ubuntu mit Truecrypt 6.x und 7.x. Vorgehensweise für Debian, Mandriva, Mint, Red Hat, Fedora, CentOS, SuSE/openSuSE und andere sollte ähnlich sein.

> Vorbereitung (Root-Rechte, Einhängepunkte, usw.)

Um Truecrypt-Laufwerke unter Linux einzubinden, benötigt man eigentlich Administratorrechte (root, su). Mit ein klein wenig Vorbereitung, kann man sich zukünftig die Passwortabfrage des Root-Passworts aber ersparen und Truecrypt als normaler Nutzer ausführen. (Achtung: potentielles Sicherheitsrisikio)

Nun benötigt man noch die Einhängepunkte (Mount-points) um die Laufwerke darauf einzubinden. Diese müssen einmalig mit Root-Rechten erstellt werden. z.B.

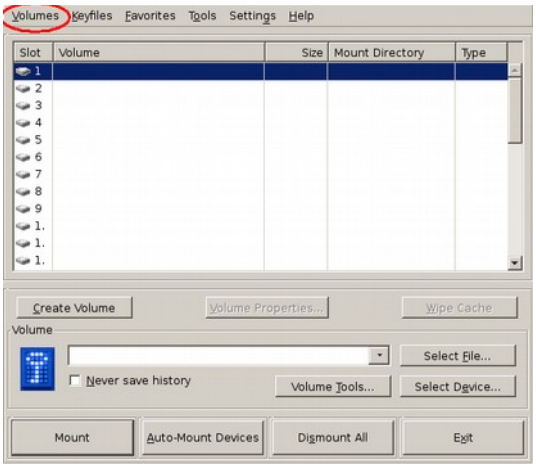
```
sudo su
mkdir /media/Data
mkdir /media/Personal
```

Wenn Sie keine Einhängepunkte erzeugen, wird Truecrypt seine eigenen Namen für die Laufwerke vergeben: "truecrypt1", "truecrypt2", ...

> Variante 1: Die "Auto-Mount"-Funktion

Für die Auto-Mount-Funktion gibt es zwei Möglichkeiten. Entweder Truecrypt sucht automatisch nach vorhandenen Geräten (devices, Festplatten) und versucht, diese mit einem Passwort zu öffnen ...

```
# -> automount_truecrypt_devices.sh
truecrypt --auto-mount=devices
```



... oder man lädt eine Liste mit Favoriten. Die Favoritenliste muss einmalig erstellt werden. Dies geschieht im Truecrypt-Hauptfenster nach dem Einbinden des Laufwerks oder des Containers. Anschließend kann man das Gerät über `Menü > Favorites > Add Selected Volume` zu den Favoriten hinzufügen. Die Liste wird dann als "Favorite Volumes.xml" im Verzeichnis ~/.Truecrypt/ (/home/Nutzername/.TrueCrypt/) abgespeichert.

Danach kann man diese Favoritenliste mittels eines einfachen Skriptes laden.

```
# -> automount_trucrypt_favorites.sh
truecrypt --auto-mount=favorites
```

> Variante 2: Shell-Skript zum Einbinden

Wenn die Einhängepunkte erstellt sind, speichert man das folgende Shell-Skript (mount_truecrypt_volumes.sh) einfach ab und lässt es beim nächsten Systemstart ausführen.

```
        #!/bin/bash

        echo "1. Please enter password"

        oldConfig=`stty -g`
        stty -echo
        read password
        stty $oldConfig

        echo "2. Mounting volumes ..."

        truecrypt -t /media/windows_c/myData.tc /media/Data
--password="$password"  -k "" --protect-hidden=no
        truecrypt -t /dev/sda5 /media/Personal --password="$password"  -k ""
--protect-hidden=no
```

Erläuterungen

-t	benutze die Textversion von Truecrypt, ohne Grafische Oberfläche (GUI)
/media/windows_c/myData.tc	Ein Truecrypt-Container auf dem Windows-Laufwerk C:
/dev/sda5	eine logische Festplatte in einer erweiterten Partition (FAT/NTFS)
/media/Data	Einhängepunkt
/media/Personal	Einhängepunkt
--password=	benutzte das folgende Passwort
-k ""	benutzte keine Keyfiles (sonst Abfrage nach Keyfiles in der Textversion)
--protect-hidden=no	benutzte keine protect-hidden Volumes (sonst Abfrage in der Textversion)

Weitere Parameter bekommt man auf der Konsole mit dem Befehl `truecrypt --help`.

Windows

Getestet unter Windows XP mit Truecrypt 6.x und Truecrypt 7.x. Vorgehensweise für Windows 2000, Windows Vista, Windows 7, Windows Server 2003, Server 2008 und andere sollte ähnlich sein.

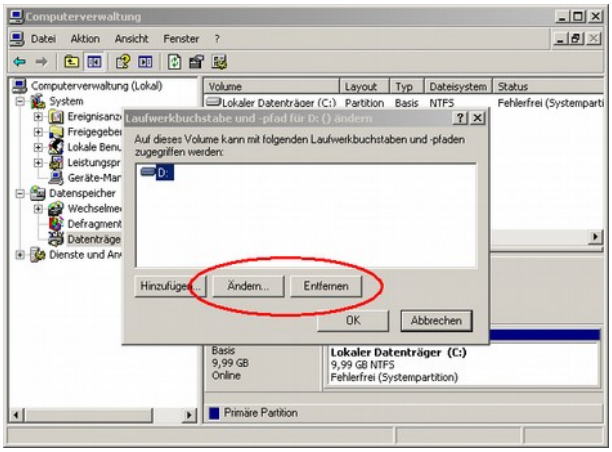
Ein Laufwerk einhängen

> Vorbereitung (Laufwerksbuchstaben im Explorer, usw.)

Nach dem Erstellen eines verschlüsselten Laufwerkes (nicht eines Containers) bleibt der Laufwerksbuchstabe oft im System erhalten und belegt diesen Platz unnötig. Beim Klick auf das verschlüsselte Laufwerk kommt dann auch noch die gefährliche Frage ob man das Laufwerk formatieren möchte.

Um den Laufwerksbuchstaben frei zu machen, benutzten Sie bitte die `Systemsteuerung > Verwaltung > Computerverwaltung > Datenträgerverwaltung >` Rechtsklick auf das Laufwerk > `Laufwerksbuchstaben und Pfade ändern > Entfernen`.

Aber **Achtung!** Überlegen Sie genau, welche Buchstaben Sie frei räumen. Entfernen Sie keine Laufwerksbuchstaben von wichtigen Laufwerken (z.B: C:\) oder Laufwerken, die noch in Benutzung sind.



Wenn Sie keinen Laufwerksbuchstaben frei machen, benutzt Truecrypt im Automount-Modus einfach den nächstfreien Buchstaben. Wenn z.B. Windows auf Laufwerk C:\ liegt und das DVD-Laufwerk D:\ ist, bekommt der Truecrypt-Container/Laufwerk einfach E:\. Falls beim Systemstart aber schon ein USB-Laufwerk angesteckt war, so kann es passieren, dass dies schon den ersten freien Buchstaben bekommen hat und Truecrypt nach F:\ weiter rutscht.

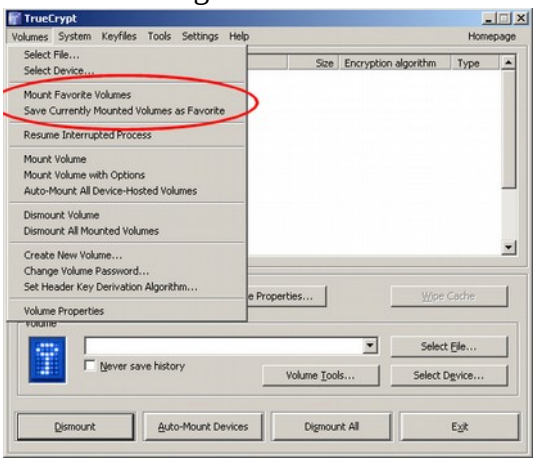
Wenn Sie jedoch mittels einer Batch-Datei den gewünschten Laufwerksnamen an Truecrypt übergeben, achten Sie darauf, dass dieser auch wirklich frei ist. Andernfalls erhalten Sie eine "Drive letter not available"-Fehlermeldung ("Laufwerksbuchstabe nicht verfügbar").

> Variante 1: Die "Auto-Mount"-Funktion

Für die Auto-Mount-Funktion gibt es zwei Möglichkeiten. Entweder Truecrypt sucht automatisch nach vorhandenen Geräten (devices, Festplatten) und versucht, diese mit einem Passwort zu öffnen ...

```
::: automount_truecrypt_devices.bat
truecrypt /auto devices
```

... oder man lädt eine Liste mit Favoriten. Die Favoritenliste muss einmalig erstellt werden. Dies geschieht im Truecrypt-Hauptfenster nach dem Einbinden des Laufwerks oder des Containers. Anschließend kann man das Gerät über `Menü > Volumes > Save Currently Mounted Volume as Favorite` zu den Favoriten hinzufügen. Die Liste wird dann in einer "Favorite Volumes.xml" im Nutzerverzeichnis abgespeichert.



Danach kann man diese Favoritenliste mittels einer einfachen Batchdatei laden.

```
::: automount_truecrypt_favorites.bat
@echo off
echo Lade Favoriten
truecrypt /q /cache y /auto favorites
truecrypt /q /s /wipecache
```

Erläuterungen

/q	Quit, zeige das Truecrypt-Fenster nicht an
/cache y	Speichert das Passwort im Speicher um mehrere Laufwerke einzubinden.
/auto ...	Auto-Mount
/s	Silent Mode, keine (Fehler-)Meldungen ausgeben
/wipecache	Den Passwort-Speicher wieder leeren.

> Variante 2: Batch-Datei zum Einbinden

Um die Eingabe zu verstecken, benutze ich die "ScriptPW.Password"-Funktion des Windows Scripting Host (WSH). Diese ist seit Windows XP verfügbar. Die Batch-Datei (mount_truecrypt_volumes.bat) erstellt eine VBS-Datei welche das Passwort einliest, sich dann selbst löscht und das Passwort an Truecrypt übergibt. (Quelle)

Im Beispiel wird eine Container-Datei *myData.tc* als Laufwerk E: eingebunden sowie eine verschlüsselte Partition auf der Festplatte als Laufwerk D:.

Die Pfadangaben zu den Programmen und Containern/Partitionen müssen an die eigenen Bedürfnisse angepasst werden.

```
        @ECHO OFF & setlocal

        SET "GetPW=%temp%\GetPW.vbs"
        ECHO WScript.Echo CreateObject("ScriptPW.Password").GetPassword() >
"%GetPW%"

        ECHO 1. Please enter password

        for /f "delims=" %%i in ('cscript //nologo "%GetPW%"') do set "Pass=%%i"
        del "%GetPW%"

        ECHO 2. Mounting volumes ...

        "C:\Program Files\TrueCrypt\truecrypt" /v C:\myData.tc /le /s /q /p
%Pass%
        "C:\Program Files\TrueCrypt\truecrypt" /v
\Device\Harddisk0\Partition2 /ld /s /q /p %Pass%
```

Erläuterungen

SET	Setzen der Variable GetPW, welche den Pfad zu einer VBS-Datei enthält.
ECHO ... > ...	Schreibe den Inhalt in die Datei
ECHO	Ausgabe des Textes in der Eingabeauforderung
for /f ...	Einlesen des Passworts
del	Löschen der VBS-Datei (Windows Scripting Host, WSH)
/v	Name des Volumes (Alternativ als Parameter "/volume")
C:\myData.tc	Truecrypt-Container
\Device\Harddisk0\Partition2	logische Festplatte in einer erweiterten Partition (FAT/NTFS)
/ld /le	Einbinden als Laufwerk D: bzw. E: (Alternativ als Paramter "/letter d" und "/letter e")
/s	Silent Mode, keine (Fehler-)Meldungen ausgeben (Alternativ als Parameter "/silent")
/q	Quit, zeige das Truecrypt-Fenster nicht an (Alternativ als Parameter "/quit")
/p	benutzte das folgende Passwort (Alternativ als Parameter "/password")

Weitere Parameter findet man in der Truecypt-Dokumentation

Weitere Anwendungen

> CD-ROM/DVD-Laufwerk verschieben (diskpart, ...)

Es kann passieren, dass das CD-ROM oder DVD-Laufwerk beim Windows-Start automatisch einen Laufwerksbuchstaben zugewiesen bekommt, den man eigentlich für ein Truecrypt-Laufwerk reserviert hat. (z.B: Laufwerk D: soll mittels Option "/ld" bzw. "/letter d" ein Truecrypt-Laufwerk werden aber das CD-ROM/DVD-Laufwerk hat den Buchstaben D: schon erhalten woraufhin man eine Fehlermeldung "Drive letter not available" bekommt.)

Hier kann man entweder über die Systemsteuerung > Verwaltung > Computerverwaltung > Datenträgerverwaltung > ... den Laufwerksbuchstaben ändern oder wieder ein kleines Skript und das windowseigene Programm "diskpart" zum Bearbeiten von Festplattenpartitionen und -buchstaben zu Hilfe nehmen.

```
diskpart /s dp-script.txt
```

dp-script.txt:

```
select volume 0
remove
assign letter=E
exit
```

Erläuterungen

diskpart /s dp-script.txt	Starte diskpart und arbeite das Skript (/s) "dp-script.txt" ab.
select volume 0	Wählt das erste Gerät aus der Liste der Laufwerke - dies kann von Computer zu Computer variieren. Bitte vorher selbst prüfen. Dazu `diskpart` auf der DOS-Eingabeaufforderung starten und "`list volume`" eingeben. Für weitere Parameter "`help`" eingeben.
remove	Entfernt den Laufwerksbuchstaben des gewählten Geräts (falls vorhanden).
assign letter=E	Vergibt den Laufwerksbuchstaben E: an das gewählte Gerät.
exit	Beendet das diskpart-Programm.

> Verzeichnis im Netzwerk freigeben (net share, ACL, ...)

Viele Freigaben für das Netzwerk könnten nach dem Einbinden des Laufwerks verloren gehen und man müsste sie jedes Mal manuell neu erstellen. Abhilfe schafft wieder eine kleine Batch-Datei.

```
::: share_folders.bat
@echo off
net share myPublic=E:\Data\Public_Folder
cacls E:\Data\Public_Folder /G Jeder:F /E /T
```

Erläuterungen

net share myPublic=E:\Data\Public_Folder	Startet die Option `share` des Programms `net` und gibt den Ordner "E:\Data\Public_Folder" unter dem Namen "myPublic" frei. Für weitere Optionen gib "`net /?`" oder "`net share /?`" ein.
cacls E:\Data\Public_Folder	Ändert die "Access Control List" (ACL) für das Verzeichnis.
/G Jeder:F	Vergibt den vollen Lese- und Schreibzugriff (F - full) für die Gruppe "Jeder". (Vorsicht - unbedingt anpassen!)
/E	ACL nur bearbeiten, nicht ersetzen.
/T	ACL für aktuelles Verzeichnis und Unterverzeichnisse bearbeiten.

> Programme/Software automatisch starten (Batch)

Nach dem Einbinden des Laufwerks möchte man vielleicht sofort seine wichtigsten Programme gestartet haben. Dazu gibt es folgende Batch-Datei.

```
::: start_programs.bat
@echo off
start "myMessenger" /min "E:\Program Files\Messenger\messenger.exe"
start "myBrowser" "E:\Program Files\Mozilla Firefox\firefox.exe"
```

Erläuterungen

start /min	Startet ein Programm minimiert. Für weitere Optionen bitte "`start /?`" eingeben.
"myMessenger", "myBrowser"	Frei zu vergebender Name für die Anwendung.
E:\Program Files\...	Pfad und Name des zu startenden Programms

Diese Batch-Datei startet die Programme sofort nach dem Einbinden der Laufwerke. Wenn Sie eine kurze Verzögerung zum Abwarten haben möchten, werfen Sie einen Blick auf mein Autostart-Skript.

Achtung! Viele Programme legen ihre Daten im Nutzerverzeichnis auf dem Laufwerk C: ab. Wenn

dieses nicht verschlüsselt ist, kann eine fremde Person leicht darauf zugreifen. Entweder man verschlüsselt sein gesamtes System (Whole Disk Encryption/Pre-Boot Authentication), ändert das Nutzerprofil in den Einstellungen des jeweiligen Programms (falls möglich) oder benutzt eine Portable-Version des Programms.

> Alle Operationen automatisch starten (Batch, Autostart)

Die gesamte Prozedur kann selbst auch beim Windows-Start ausgeführt werden. Dazu muss die folgende Batch-Datei in den Autostart-Ordner kopiert werden. (Normalerweise zu finden unter `> Start > Programme > Autostart` oder im Nutzerverzeichnis (2000, XP) `C:\Dokumente und Einstellungen\[Nutzername]\Startmenü\Programme\Autostart`) Mittels des `call`-Befehls, werden die einzelnen Dateien der Reihe nach abgearbeitet.

```
::: autostart_truecrypt.bat
@echo off
call "C:\My Files\move_cd-dvd-drives.bat"
call "C:\My Files\(auto)mount_truecrypt_volumes.bat"

call "E:\My Hidden Files\share_folders.bat"
call "E:\My Hidden Files\start_programs.bat"
```

Erläuterungen

move_cd-dvd-drives.bat	Batch-Datei zum Verschieben des CD- bzw. DVD-Laufwerksbuchstabens. (optional, siehe oben)
(auto)mount_truecrypt_volumes.bat	Einbinden des Truecrypt-Laufwerks - entweder per Automount oder über eine Batch-Datei. (siehe oben)
share_folders.bat	Netzwerkfreigabe. (optional, siehe oben)
start_programs.bat	Starten von weiteren Programmen. (siehe oben)

Allgemeines: Dateisystem, Login, Ausschalten, Netzwerk

> Auswahl des Dateisystems (FAT16, FAT32, NTFS gg. ext2, ext3)

Wenn man mehrere Betriebssysteme auf seinem Rechner nutzt, steht man auch vor der Frage, welches Dateisystem man den Truecrypt-Laufwerken/Containern zuweisen soll. Natürlich befindet sich Windows zumeist auf einer FAT/FAT32 oder NTFS-Partition während Linux höchstwahrscheinlich unter einem ext-Dateisystem zu finden ist. Allen anderen Dateien ist es aber herzlich egal, auf welchem System sie abgespeichert werden.

Beide Betriebssysteme sind mittels Treibern in der Lage das jeweils andere Dateisystem zu lesen. Man kann mit dem "Ext2 Installable File System For Windows" auf ext2- und ext3-Laufwerke unter Windows zugreifen und mittels "ntfs-3g" eine NTFS-Partition unter Linux lesen. (Ntfs-3g ist heute schon Teil vieler Linux-Distributionen und muss nicht extra installiert werden, so dass die NTFS-Unterstützung meist sofort klappt. Funktionierende Windows-Treiber für ext4 sind mir noch nicht bekannt und habe ich auch noch nicht näher untersucht.)

Um das richtige Dateisystem für seine verschlüsselten Laufwerke zu bestimmen, sollte man sich im Klaren sein, welches Betriebsystemsystem man wofür und wie häufig nutzt. (z.B. Linux für Internet -> ext3, Windows für Spiele -> NTFS)

Wer ein Windows-Dateisystem auswählt, muss wissen wie groß das Laufwerk ist und ob große Dateien darauf abgelegt werden sollen. FAT16 unterstützt 2GB Dateien auf höchstens 2GB Laufwerken (z.B. USB-Laufwerk), FAT32 kann mit 4GB Dateien auf bis zu 8TB Laufwerken umgehen (z.B. Video-DVD auf Festplatte kopieren) und NTFS erlaubt 16TB Dateien auf 16TB Laufwerken (z.B. DVD-ISO-Dateien auf Festplatte). (1TB = 1.000GB [dezimal]) Das Linux ext3-Dateisystem ist ein verbessertes ext2 mit Zusatzfunktionen wie z.B. einem besseren Schutz vor Datenverlust nach einem Systemabsturz. Beide ext-Dateisysteme können 2TB große Dateien verarbeiten, ext3 sogar noch größere.

Truecrypt unter Windows kann lediglich FAT und NTFS-Dateisysteme erstellen. Truecrypt unter Linux kann jedoch sowohl FAT als auch ext2 und ext3-Dateisystem erzeugen.

> Hinweis zur Benutzung des Loginpassworts (Windows/Linux)

Das Passwort welches bei der Anmeldung benutzt wird, kann im Prinzip **nicht** gleichzeitig/sofort als Passwort für das TrueCrypt-Laufwerk/Container übergeben werden. Dies widerspräche ja auch dem Sicherheitskonzept des Betriebssystems, wenn ein Programm das Anmeldepasswort auslesen könnte oder das Passwort noch irgendwo im Speicher zu finden wäre.
(Das heißt natürlich nicht, dass man sein Loginpasswort nicht auch als Entschlüsselungspasswort benutzen könnte. Man muss es aber dennoch zweimal eingeben und hoffen, dass das Login-Passwort nicht geknackt wird.)

Alternativ kann man unter Windows und Linux die "Whole Disk Encryption" (Pre-Boot Authentication) benutzen und sich danach die Anmeldung ersparen. Unter Linux kann man

stattdessen auch sein HOME-Verzeichnis mittels Pluggable Authentication Module (PAM) einbinden.

> Schnelles Aushängen der Laufwerke (Windows/Linux)

Normalerweise kann man seinen Rechner ganz gewöhnlich herunterfahren (nicht einfach ausschalten!) ohne die Laufwerke vorher zu entfernen.

Um jedoch alle eingebundenen Truecrypt-Laufwerke auf einmal auszuhängen, ruft man Truecrypt mit dem Parameter "d" bzw. "dismount" auf.

```
LINUX:
truecrypt --dismount

WINDOWS:
trucrypt /dismount
```

Falls noch Lese-/Schreiboperationen auf dem Laufwerk stattfinden, kann das Laufwerk nicht sofort ausgehangen werden. Wenn dies aber unbedingt sein muss, kann man den Parameter "force" hinzufügen.
Achtung: Dabei können Daten verloren gehen!

```
LINUX:
truecrypt --dismount --force

WINDOWS:
truecrypt /dismount /force
```

Wenn nur ein bestimmtes Laufwerk ausgehängt werden soll, kann dies an den Paramter übergeben werden.

```
LINUX:
truecrypt --dismount /media/Data
truecrypt -d /dev/sda5

WINDOWS:
truecrypt /dismount Z:
truecrypt /d X:
```

> Ein Truecrypt-Laufwerk im Netzwerk einbinden

Truecrypt-Laufwerke können auch eingebunden werden, wenn sie auf einem Server im Netzwerk liegen. Das benutzte Betriebssystem auf beiden Seiten ist dabei vollkommen egal. Hierfür gibt es zwei Möglichkeiten.

1. Man entschlüsselt den Container oder die Partition schon auf dem Server und gibt das Laufwerk frei. Vorteil ist, dass alle Nutzer jetzt auf ein "normales" Laufwerk zugreifen können und dort sowohl lesen auch schreiben können. Nachteil ist, dass die Verbindung übers Netzwerk unverschlüsselt erfolgt. Jedoch kann man mittels Netzwerktechniken wie SSL, TLS oder VPN die Verbindung schützen.

Um das Laufwerk nach einem Neustart des Servers manuell wieder einzubinden, sollte man am besten direkten Zugriff auf das System haben. Wer keinen physischen Zugang zum Gerät hat, kann auch mittels Fernsteuerungssoftware wie VNC arbeiten. (Man könnte das Laufwerk auch automatisch mittels einer Batchdatei oder eines Skripts im Autostart einbinden. Aber weil das Passwort dabei im Klartext abgespeichert wird, entsteht hier ein unnötiges Sicherheitsrisiko.)

2. Man gibt eine Container-Datei im Netzwerk frei und die Nutzer müssen die Datei selbst einbinden. (Dies funktioniert also nicht mit Partitionen!) Vorteil ist, dass die Verbindung nun verschlüsselt erfolgt, eine zusätzliche Netzwerkverschlüsselung kann jedoch nicht schaden. Nachteil ist, dass auf das Laufwerk nur lesend aber nicht schreibend zugegriffen werden kann, weil es sonst zu Datenverlust kommen könnte.

Weitere Informationen finden sich in der Truecrypt Hilfe.

Wenn es sich jedoch lediglich um einen **Fileserver** handelt, ist eine Lösung mittels Free NAS oder Crypto NAS möglicherweise einfacher und schneller. (NAS: Network-Attached Storage)