AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

# SCHULNETZ

Qualifizierung von Systembetreuerinnen
und Systembetreuern

# Datensicherheit
# im Unterrichtsbereich
# und in der Schulverwaltung

## – Laborübungen –

## IMPRESSUM

Die im Laborbuch Datensicherheit beschriebenen Verfahren und Übungen wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren erarbeitet. Die Handreichung ist unter der Adresse http://alp.dillingen.de/schulnetz/materialien abrufbar.


| | |
|---|---|
| Herausgeber: | Akademie für Lehrerfortbildung und Personalführung<br>Kardinal-von-Waldburg-Str. 6-7<br>89407 Dillingen |
| Dokumentation: | Georg Schlagbauer, Akademie Dillingen<br>Barbara Maier, Akademie Dillingen |
| URL: | http://alp.dillingen.de/schulnetz |
| Mail: | schlagbauer@alp.dillingen.de |
| Stand: | Juli 2018 |

# INHALT





# DATENSPEICHER

## Dateiserver

Lokale Dateiserver (Windows-Server, Linux-Server, Novell-Server) sind der klassische Weg, um Daten in einer vernetzten Umgebung abzulegen. Diese Dateiserver bieten differenzierte Möglichkeiten der Benutzerverwaltung, sind aber nicht ganz einfach zu administrieren.

## NAS-Boxen

NAS-Boxen laufen den klassischen Dateiservern immer mehr den Rang ab. Sie sind für große Datenmengen konzipiert und relativ einfach einzurichten.

## Cloud-Speicher

Cloud-Speicher im Internet sind von überall zugänglich und bieten die Möglichkeit, einzelne Dokumente oder Bereiche auch beliebigen anderen Benutzern zugänglich zu machen.

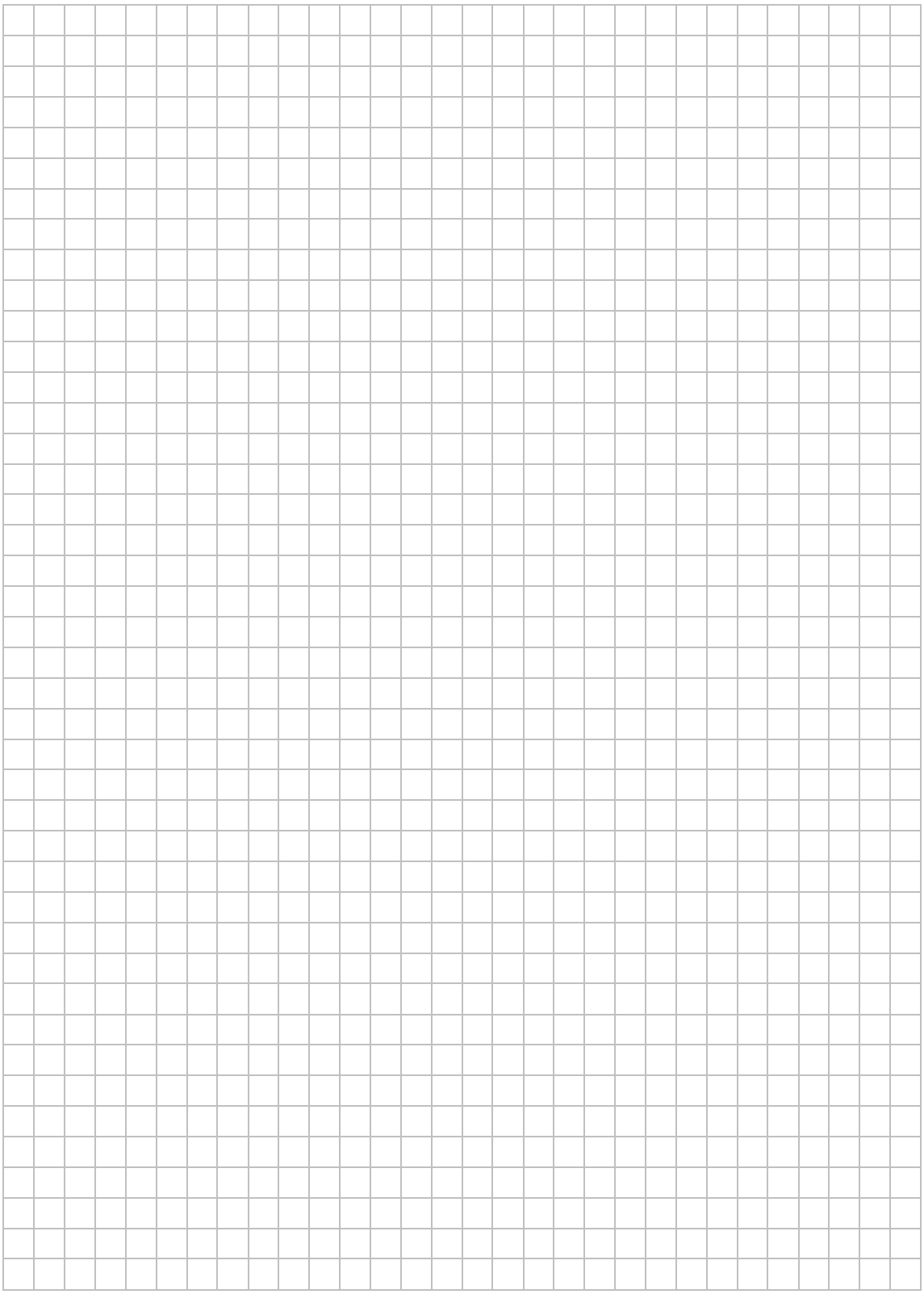
## Berechtigungen

Datenspeicher bieten die Möglichkeit, für einzelne Benutzer oder Benutzergruppen differenzierte Zugriffsberechtigungen einzurichten, z. B.

- Leserechte
- Lese- und Schreibrechte
- keine Zugriffsrechte

Die Berechtigungen sollten sehr sorgfältig gesetzt werden. Ein Virus oder Verschlüsselungstrojaner kann z. B. nur dort Schaden anrichten wo er auch Schreibrechte hat.

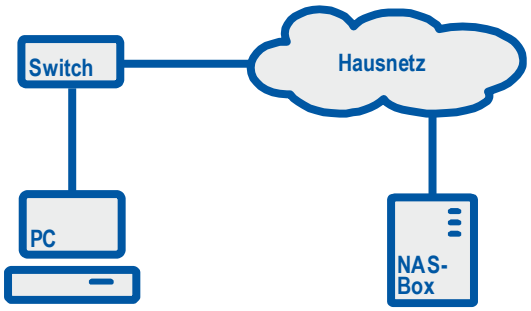
## Ihre Notizen



# LABORÜBUNG 01 - EINRICHTEN EINES DATENSPEICHERS AUF EINER NAS-BOX

## Szenario

Auf einer NAS-Box werden Freigaben erstellt, auf welche Lehrer und Schüler mit unterschiedlichen Rechten zugreifen können.




## Aufgaben

1. Überprüfen Sie die Verbindung zum zentralen Datenspeicher (NAS) auf IP-Ebene.
2. Erstellen Sie auf der NAS-Box Benutzer, ggf. Benutzergruppen (z. B. Lehrer, Schüler) und einige Freigaben (z. B. Austausch, Vorlagen). Vergeben Sie den Benutzern bzw. Benutzergruppen verschiedene Zugriffsrechte (keine Rechte, Leserechte, Schreibrechte).
3. Greifen Sie von Ihrem Computer auf die Freigaben des zentralen Datenspeichers zu und überprüfen Sie Ihre Zugriffsrechte mit unterschiedlichen Benutzer-Accounts. Testen Sie dabei auch unterschiedliche Zugriffsmethoden auf die Freigaben (z. B. Windows-Explorer, Netzlaufwerk verbinden, `net use` auf Kommandozeile).
4. Testen Sie den Zugriff auf die NAS-Box mit unterschiedlichen Benutzer-Accounts über einen Web-Browser.

## Weiterführende Aufgaben

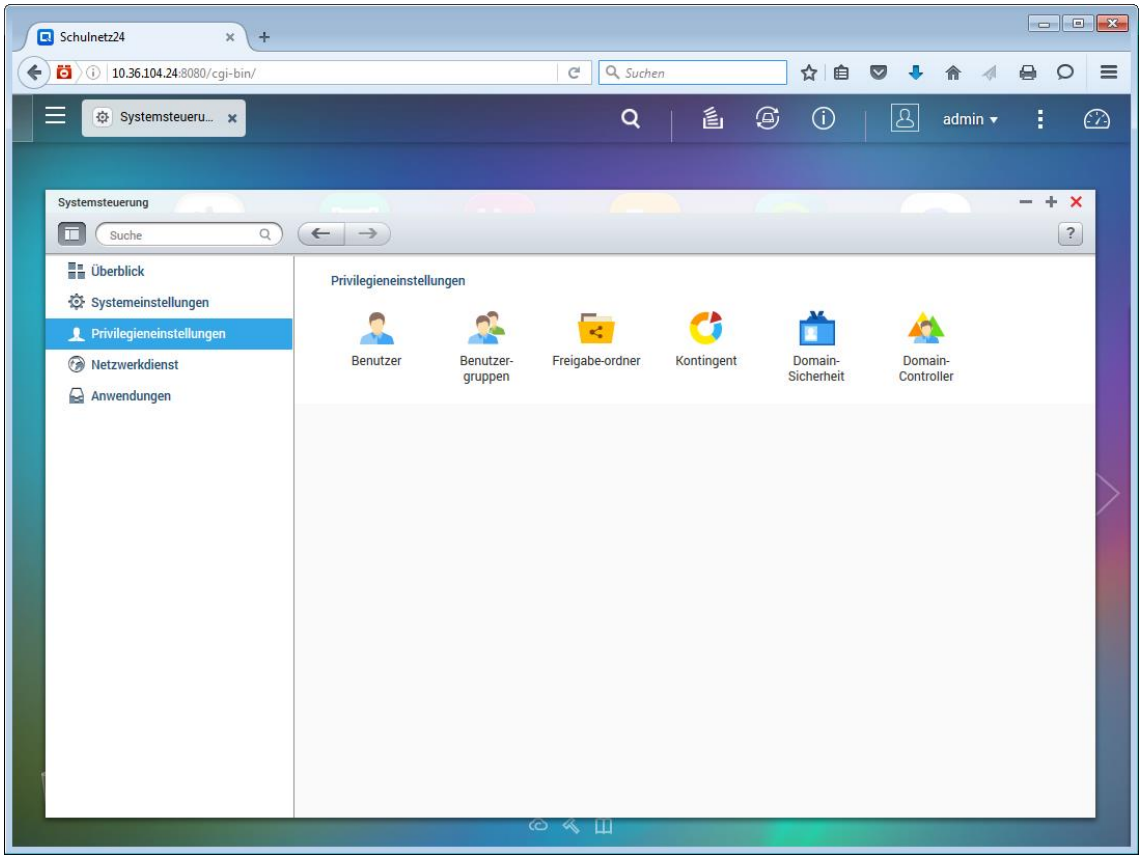
5. Testen Sie mit einem Tablet oder Ihrem Smart Phone den Zugriff auf die NAS-Box. Verwenden Sie dazu geeignete Apps (z. B. Qfile für Android oder iOS).
6. Erstellen Sie ein Foto mit dem Smartphone und speichern Sie dieses auf der NAS-Box ab.

## Ihre Notizen

# HINWEISE

## Einrichten von Freigaben auf einer NAS-Box

Über die Systemsteuerung der NAS-Box lassen sich Benutzer, Benutzergruppen und Freigaben mit unterschiedlichen Rechten einrichten.

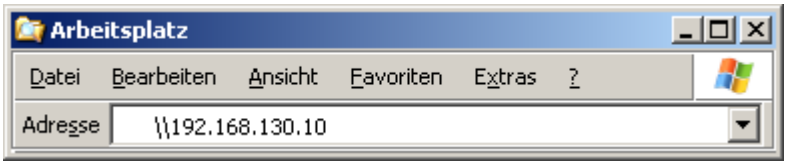



## Zugriff auf eine NAS-Box mit Smartphones

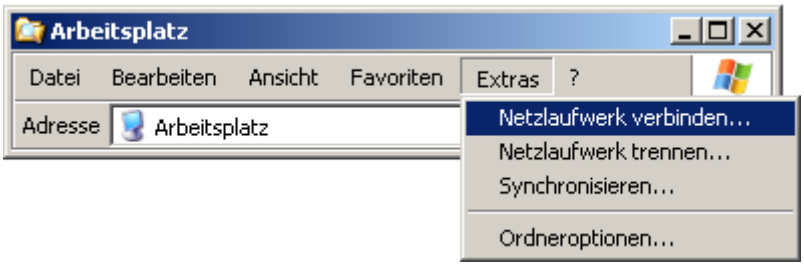
Da Smartphones keinen komfortablen Tastaturzugang besitzen, ist es praktikabel mit speziellen Apps den Zugang dauerhaft einzurichten (z. B. ES Datei Exporer, Qfile bei QNAP-NAS, DS file bei Synology-NAS).

## Zugriffe auf SMB-Freigaben unter Windows

### Adresszeile im Windows-Explorer




### Netzlaufwerk verbinden im Windows-Explorer




### Netzlaufwerk verbinden auf der Kommandozeile

`net use` *`Laufwerk`*`: \\`*`servername`*`\`*`freigabename`*

`net use x: \\192.168.130.10\Daten`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.

`net use x: \\192.168.130.10\Daten /user:l1`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung wird der Benutzername (l1) übergeben.

`net use x: \\192.168.130.10\Daten /user:l1 12345`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung werden der Benutzername (l1) und das Passwort (12345) übergeben.

`net use x: \\192.168.130.10\Daten /persistent:yes`

Die Laufwerksverbindung x: wird erstellt und bei der nächsten Anmeldung am lokalen System automatisch wieder hergestellt.

## Trennen von SMB-Verbindungen

SMB-Verbindungen sind oft sehr dauerhaft. Windows „merkt“ sich den Zugriff auf eine Freigabe und versucht, sich beim nächsten Zugriff mit den gespeicherten Anmeldeinformationen zu verbinden. Deshalb kann es bei den einzelnen Tests notwendig sein, sich am lokalen Computer abzumelden und neu anzumelden.

### Windows-Explorer

Extras – Netzlaufwerk trennen

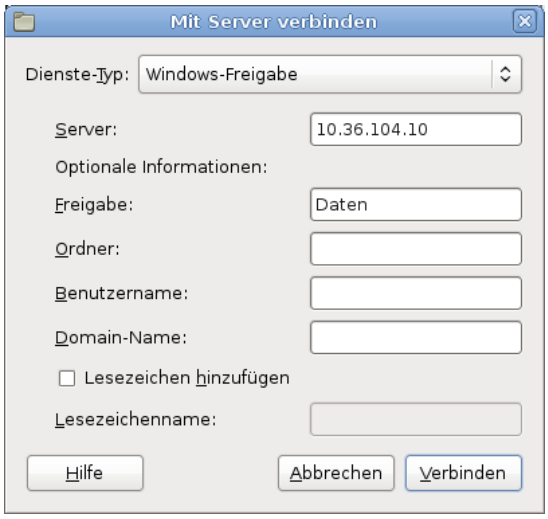
### Kommandozeile

`net use *Laufwerk*: /delete`

| | |
|---|---|
| `net use x: /delete` | Das Netzlaufwerk x: wird getrennt |
| `net use *  /delete` | Alle Netzlaufwerke werden getrennt |

## Zugriffe auf SMB-Freigaben unter Linux (Gnome)

### Menü: Orte – Verbindung zu Server

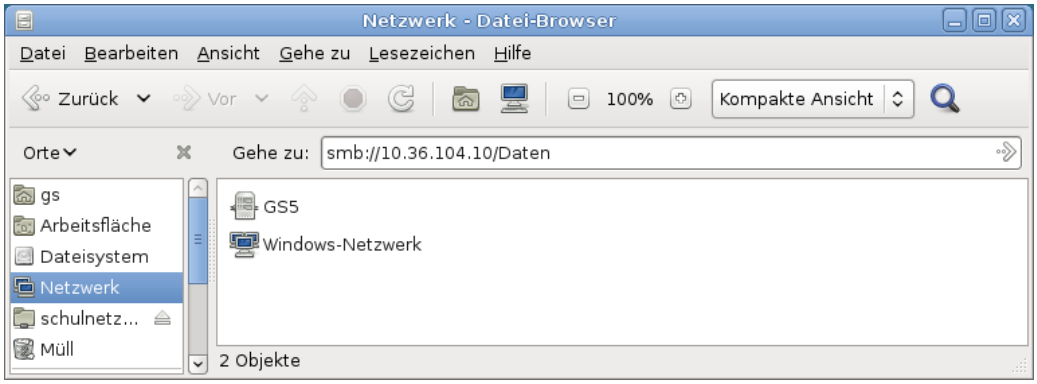



### Nautilus-Adressleiste

`smb://ip-Adresse`

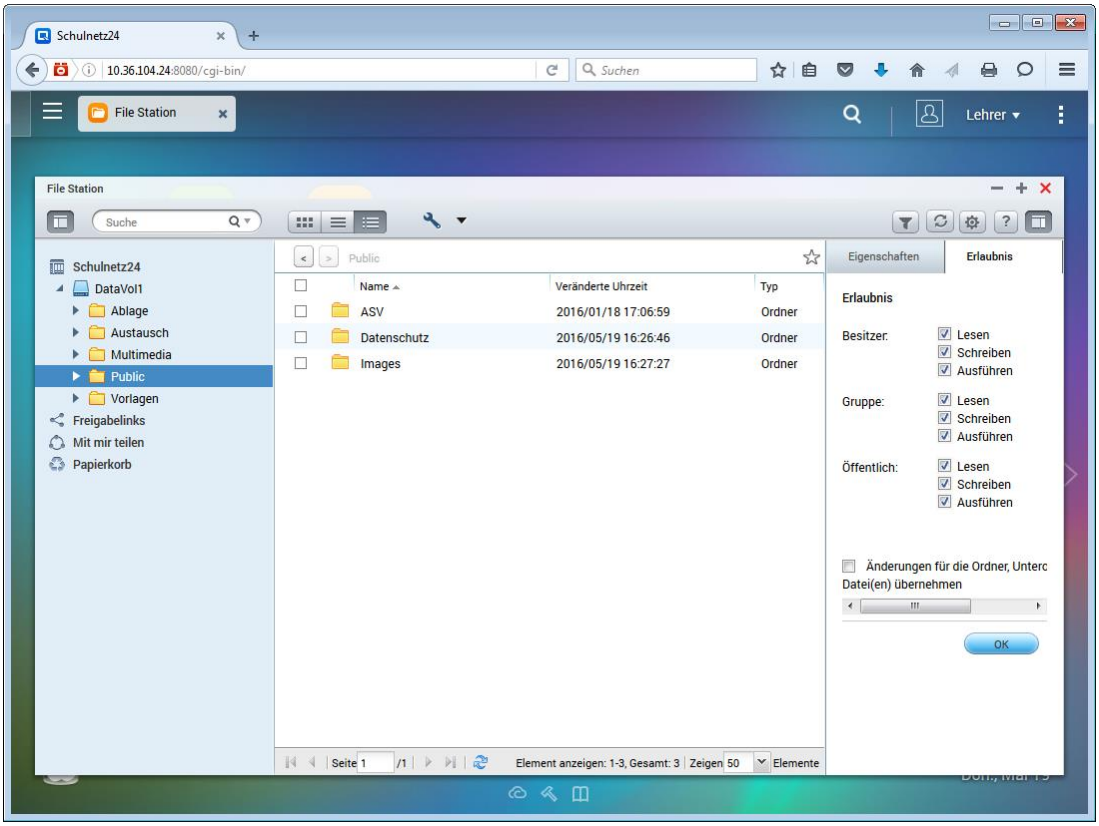
`smb://ip-Adresse/freigabe`

`smb://user@<ip-Adresse>`




Die Adressleiste beim Dateibrowser Nautilus muss ggf. mit <Strg>+L eingeblendet werden.

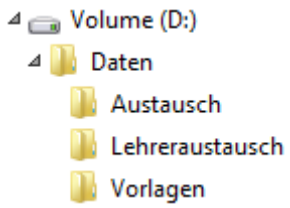
## Web-Zugriff auf die Freigaben der NAS-Box



# LABORÜBUNG 02 - SMB-ZUGRIFF UND NTFS-RECHTE BEIM WINDOWS-SERVER

## Szenario

Schüler und Lehrer sollen den Server zur Datenablage und zum Austausch von Dateien nutzen. Im Ordner Austausch sollen alle Benutzer Daten ablegen, austauschen und löschen können. Im Ordner Vorlagen stellen Lehrkräfte den Schülern Unterrichtsmaterial zur Verfügung.




## Aufgaben

1. Legen Sie auf dem Server zwei Gruppen z. B. Schueler und Lehrer an und ordnen Sie die Benutzer s1, s2, l1, l2 diesen Gruppen zu.
2. Erstellen Sie auf dem Server die angegebene Ordnerstruktur und geben Sie den Ordner *Daten* frei.
3. Im Austauschordner sollen die Schüler und Lehrkräfte lesenden und schreibenden Zugriff haben. Im Vorlagenordner können Schüler lesen, Lehrkräfte lesen und schreiben.
4. Greifen Sie vom Arbeitsplatzcomputer mit unterschiedlichen Benutzeraccounts und mit unterschiedlichen Werkzeugen auf die Freigabe am Server zu.
5. Die Freigabe soll über einen Laufwerksbuchstaben angesprochen werden.

## Hinweise

Windows ermöglicht es, NTFS-Rechte sehr differenziert zu vergeben. In den meisten Fällen genügt es jedoch, Leserechte, Lese-/Schreibrechte und Vollzugriff zu unterscheiden.

### Leserecht

Als Leserecht werden die NTFS-Rechte Lesen, Ausführen, Ordnerinhalt auflisten, Lesen zusammengefasst.

### Lese-/Schreibrecht

Beim Lese-/Schreibrecht kommen noch zusätzlich die Rechte Ändern und Schreiben hinzu.

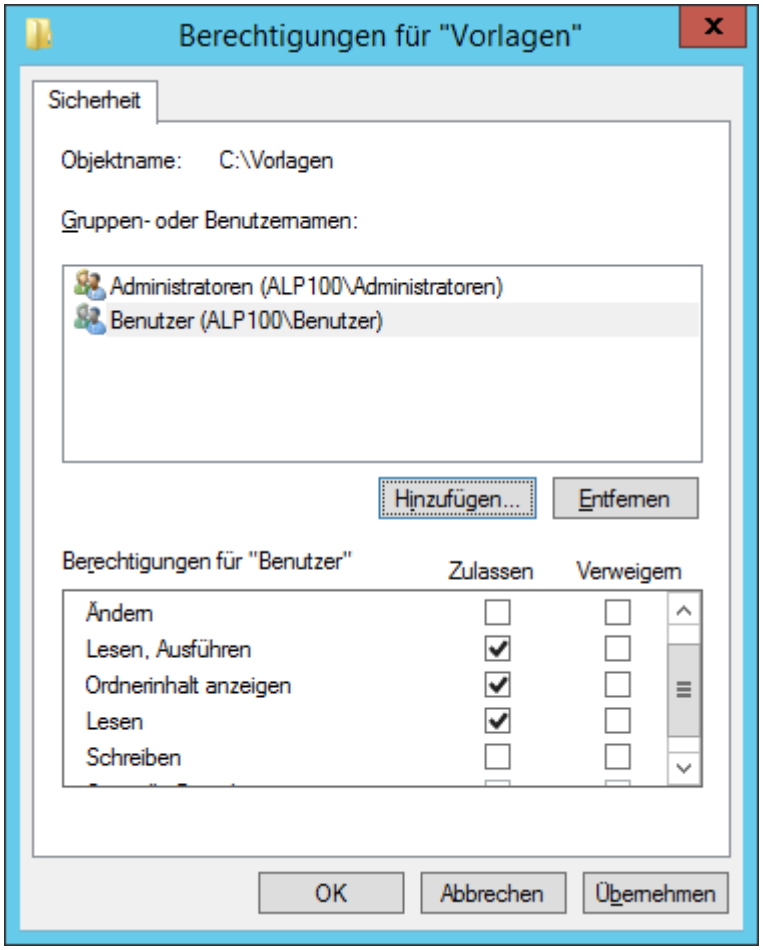
### Vollzugriff

Der Vollzugriff beinhaltet das Lese-/Schreibrecht. Zusätzlich beinhaltet er noch das Recht Rechte zu vergeben und den Besitz von Dateien zu übernehmen.

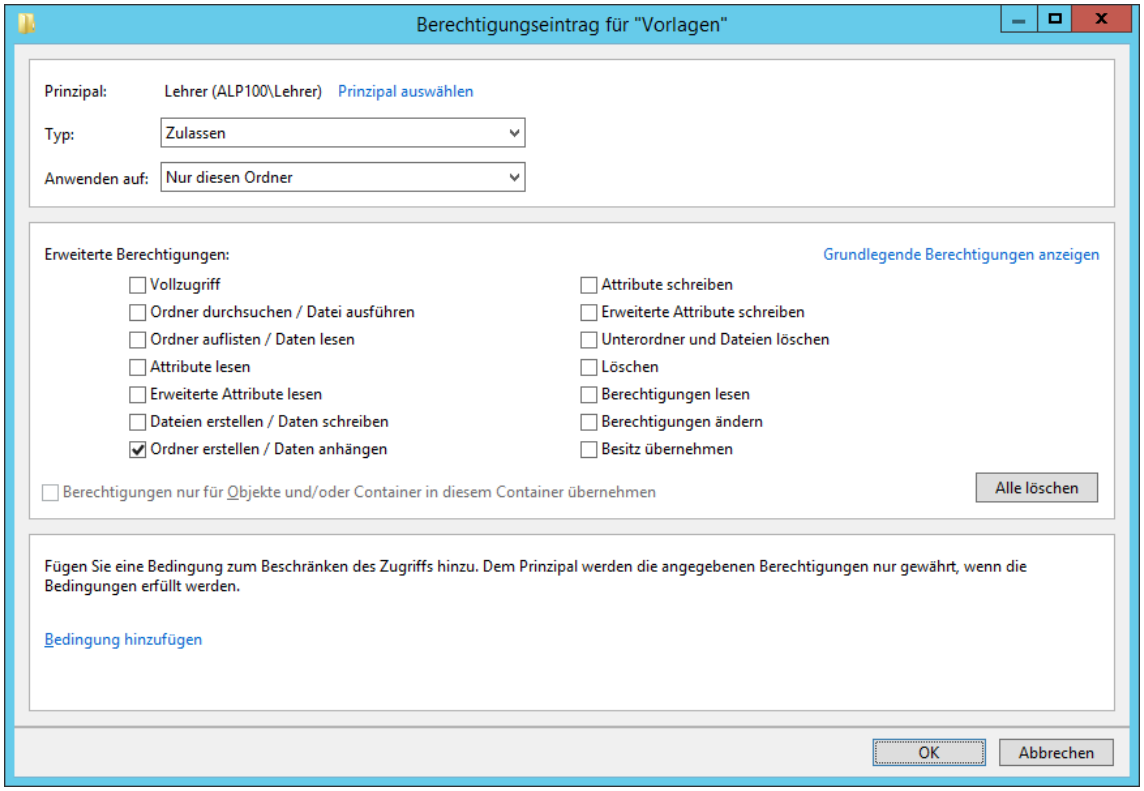
### Beispiel für die Vergabe von NTFS-Rechten

Im Vorlagenordner sollen die Lehrkräfte ihre Daten nur in selbst erstellten Ordnern ablegen können. Die Lehrkräfte sollen sich die Daten gegenseitig nicht überschreiben oder löschen können. Schüler und Lehrer können lesend auf alle Dateien zugreifen.

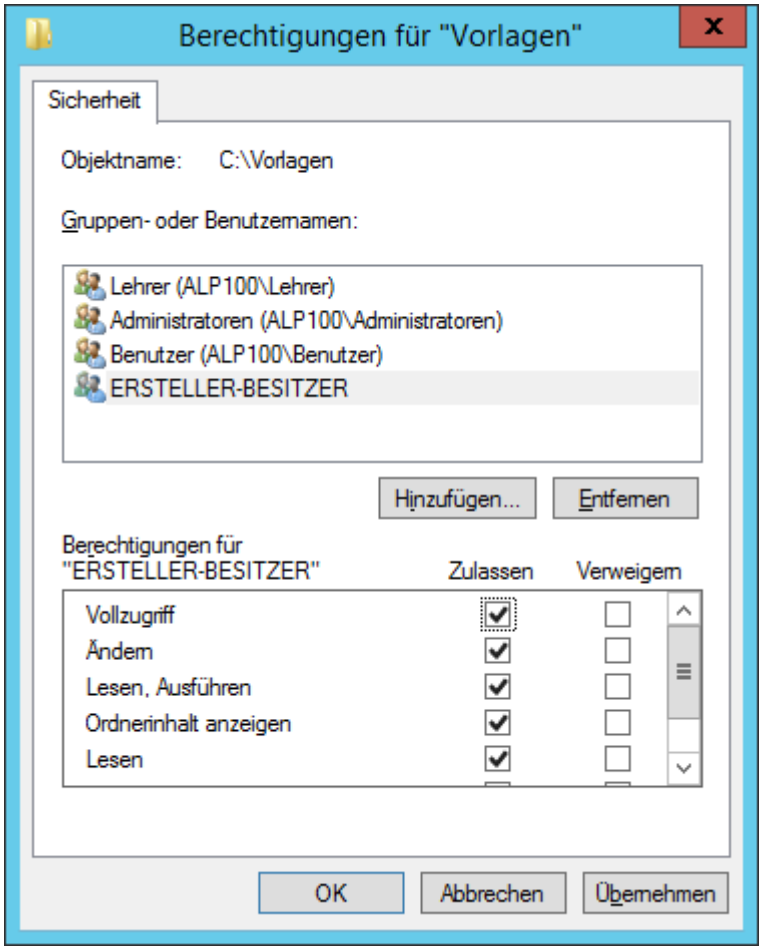
Im ersten Schritt wird für den Ordner Vorlagen die Vererbung unterbrochen und überflüssige Berechtigungen entfernt. Die Gruppe der Administratoren erhält weiterhin Vollzugriff. Die Gruppe der Benutzer erhält Leserechte. Alle Lehrer und Schüler sind in der Gruppe Benutzer enthalten.




Im zweiten Schritt wird der Gruppe Lehrer die Berechtigung gegeben, im Ordner Vorlagen Ordner zu erstellen. Damit können Lehrkräfte Ordner anlegen; sie können den Ordner jedoch nicht umbenennen und auch keine Dateien in diesen Ordner ablegen.




Im dritten Schritt wird der Gruppe „Ersteller-Besitzer“ Vollzugriff gegeben. Hat ein Lehrer einen Ordner angelegt, ist er „Ersteller-Besitzer“ dieses Ordners und hat damit Vollzugriff. Alle anderen Benutzer haben durch die Vererbung Leserechte.




## Weiterführende Informationen

### Zusammenspiel zwischen Freigaben und NTFS-Rechten

Um über das SMB- bzw. CIFS-Protokoll auf einen Windows-Server zugreifen zu können, ist eine Freigabe am Windows-Server notwendig. Diese Freigabe ist das Eingangstor zum Server.

Die Freigabe kann mit bestimmten Rechten für verschiedene Benutzer versehen werden (Freigabeberechtigungen). Diese Freigabeberechtigungen stellen die maximalen Rechte dar, die ein Benutzer haben kann, wenn er auf diesem Weg auf den Server zugreift. Durch die NTFS-Rechte können die Rechte eines Benutzers weiter eingeschränkt sein.

Eine gebräuchliche Praxis ist es, Freigaben mit den Freigabeberechtigungen „Jeder – Vollzugriff“ oder „Jeder – Ändern“ zu versehen. Die eigentlichen Beschränkungen für einen Benutzer erfolgen über die NTFS-Rechte (Sicherheitseinstellungen).


### Zugriff auf administrative Freigaben

Alle Festplattenlaufwerke sind standardmäßig mit einer administrativen Freigabe versehen (C$, D$, …). Das Windows-Verzeichnis ist standardmäßig mit der administrativen Freigaben ADMIN$ verbunden. Der Zugriff auf die administrativen Freigaben kann nur durch einen Eingriff in die Registry dauerhaft unterbunden werden.

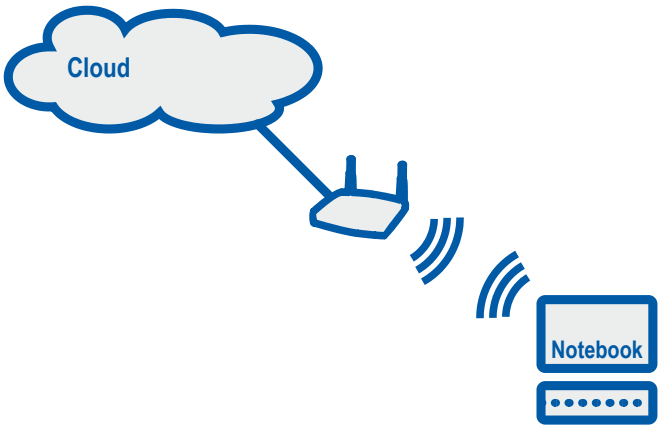
| | |
|---|---|
| `\\Server\C$` | Zugriff auf ein Laufwerk |
| `\\Server\ADMIN$` | Zugriff auf das Windows-Verzeichnis |

### Anlegen versteckter Freigaben

Versteckte Freigaben sind Freigaben, die in der Netzwerkumgebung nicht angezeigt werden. Der Benutzer muss den Freigabenamen kennen, um darauf zuzugreifen.

Versteckte Freigaben unterscheiden sich beim Anlegen von normalen Freigaben nur dadurch, dass am Ende des Freigabenamens das $-Zeichen angehängt wird.

# LABORÜBUNG 03 - DATEN AUF EINEM CLOUD-SPEICHER




## Szenario

Ein Lehrer hat bei einem Cloud-Anbieter einen Online-Speicher erworben. Diesen möchte er nutzen, damit er seine Unterrichtsvorbereitung überall zur Verfügung hat.

## Aufgaben

1. Erkunden Sie die Möglichkeiten Ihrer Cloud (z. B. Zugriffsmöglichkeiten auf den Online-Speicher, Kalender, Fotoalbum, Dateien).

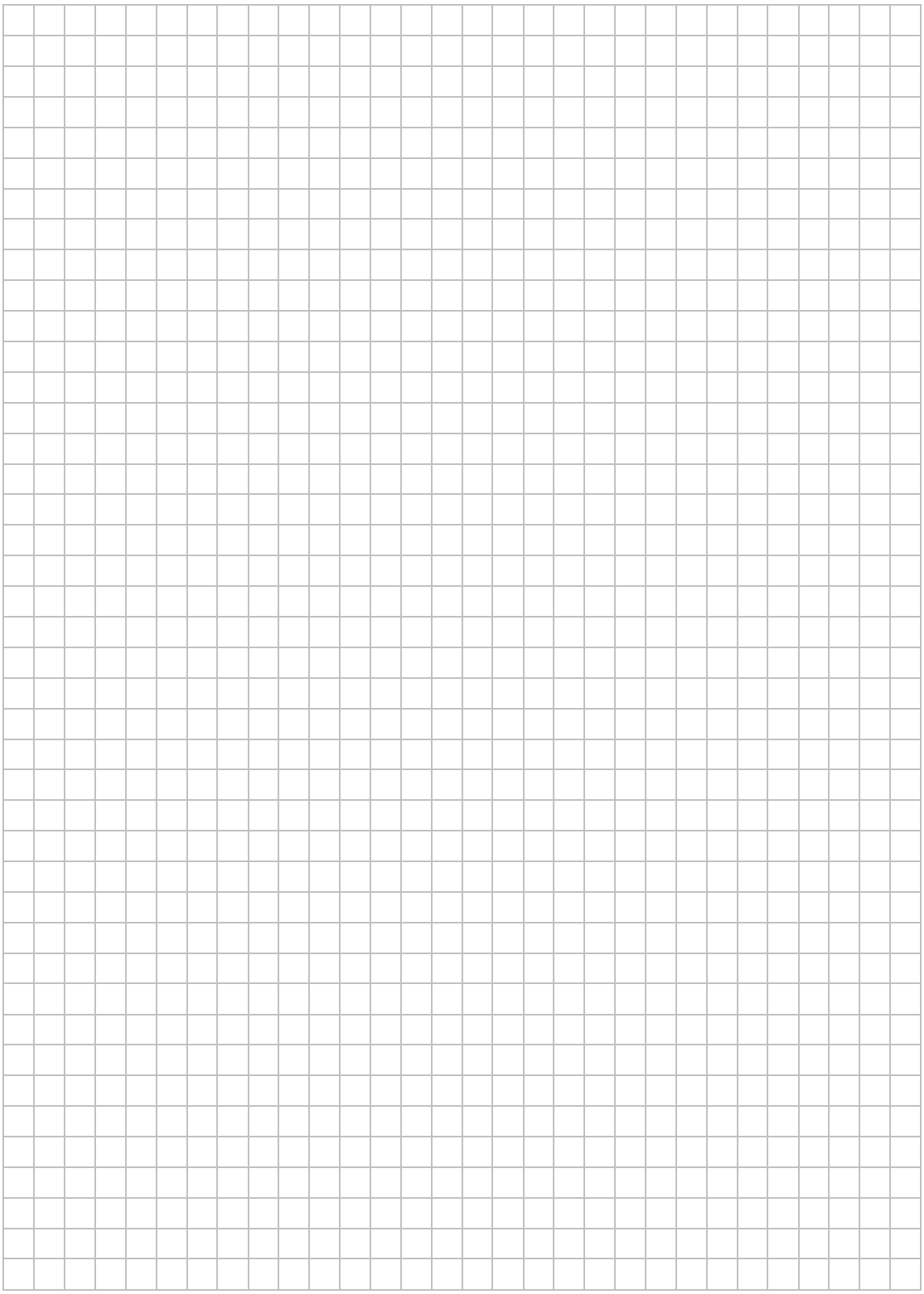
### Urlaubsfotos über die Cloud bereitstellen

2. Fertigen Sie mit Ihrem Smartphone einige Fotos an. Laden Sie die Fotos in einen Ordner „Urlaubsfotos“ auf die Cloud und geben Sie diesen Ordner über einen Link frei. Versenden Sie die Linkadresse per E-Mail.

### Unterrichtsvorbereitung in der Cloud

3. Richten Sie einen Ordner „Unterricht“ ein und synchronisieren Sie diesen Ordner mit der Unterrichtsvorbereitung auf Ihrem lokalen PC.
4. Synchronisieren Sie den Ordner „Unterricht“ mit einem mobilen Gerät (Tablet oder Notebook).

## Ihre Notizen



# HINWEISE

## Verschiedene Cloud-Lösungen

GoogleDrive – wird automatisch mit einem Google-Account erstellt

OneDrive – wird mit einem Microsoft-Konto erstellt; seit Windows 8.1 im Dateiexplorer integriert

MagentaCloud – Cloud der Telekom; Server stehen in Deutschland

iCloud – wird mit der Apple-ID angelegt

ownCloud bzw. Nextcloud – Open-Source-Lösungen, um einen eigene Cloud aufzusetzen

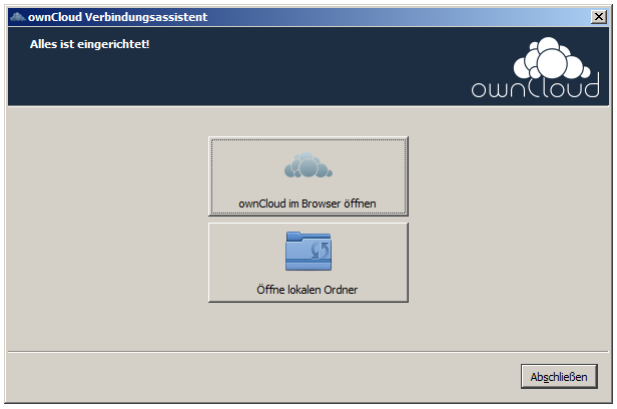
web.de-Cloud

gmx-Cloud

yahoo-Cloud

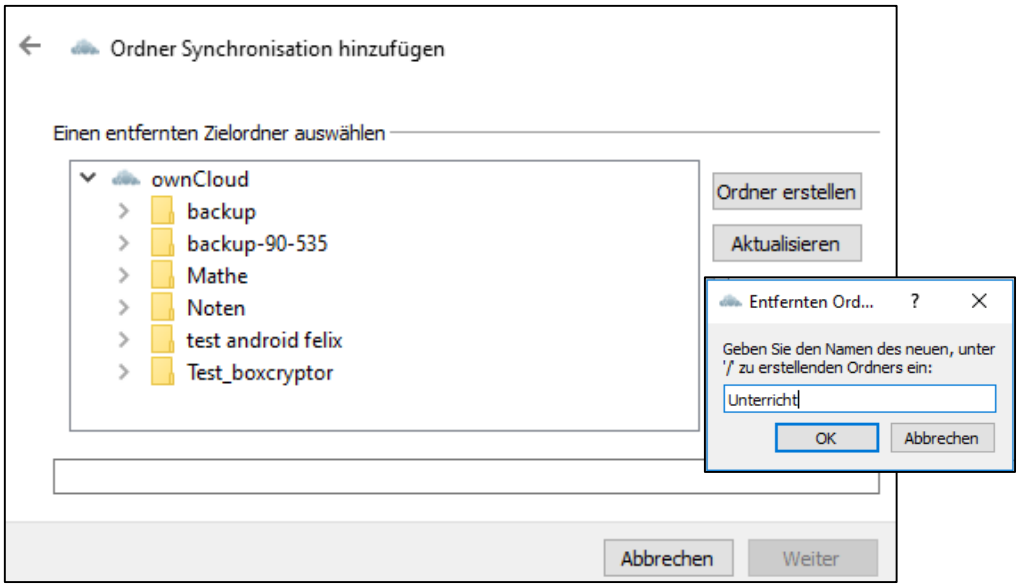
## Installation eines Clients

Nahezu alle Cloud-Anbieter stellen Clients für die unterschiedlichsten Plattformen bereit, die einen einfachen Zugang zum jeweiligen Anbieter ermöglichen.




## Hinzufügen eines Ordners zur Synchronisation

Dateien in der Cloud können mit den Dateien auf dem lokalen Computer synchron gehalten werden. Der Cloud-Speicher wird als Verzeichnis im Dateiexplorer angezeigt.




## Freigabe eines Ordners in der Cloud

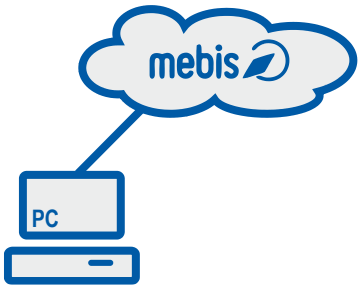

Der Ordner ist über einen kryptischen Link öffentlich zugänglich. Bei Bedarf kann ein Passwort oder ein Ablaufdatum gesetzt werden.

# LABORÜBUNG 04 - DATENSPEICHER AUF MEBIS

## Szenario

Sie möchten mebis als persönlichen Cloud-Speicher nutzen.

Zusätzlich möchten Sie für die Lehrkräfte Ihrer Fachschaft einen gemeinsam Dateipool für Arbeitsblätter aufbauen. Jede Lehrkraft soll darin Schreibrechte haben.




## Aufgaben

1. Loggen Sie sich in mebis ein. Legen Sie unter „Meine Dateien“ Ordner an und laden Dokumente in diese Ordner hoch.
2. Legen Sie in Mebis einen Kurs „Materialien für Unterricht“ in Ihrem Schulbereich an.
3. Aktivieren Sie die Selbsteinschreibung für andere Lehrkräfte, so dass diese automatisch mit der Lehrer-Rolle in den Kurs eingeschrieben werden.
4. Legen Sie Ordner an, in welche Sie und andere Lehrkräfte Dokumente hochladen können.
5. Geben Sie den Einschreibeschlüssel an andere Kursteilnehmer weiter und fordern Sie diese auf, sich in Ihren Kurs einzuschreiben und Dateien hochzuladen.

# HINWEISE

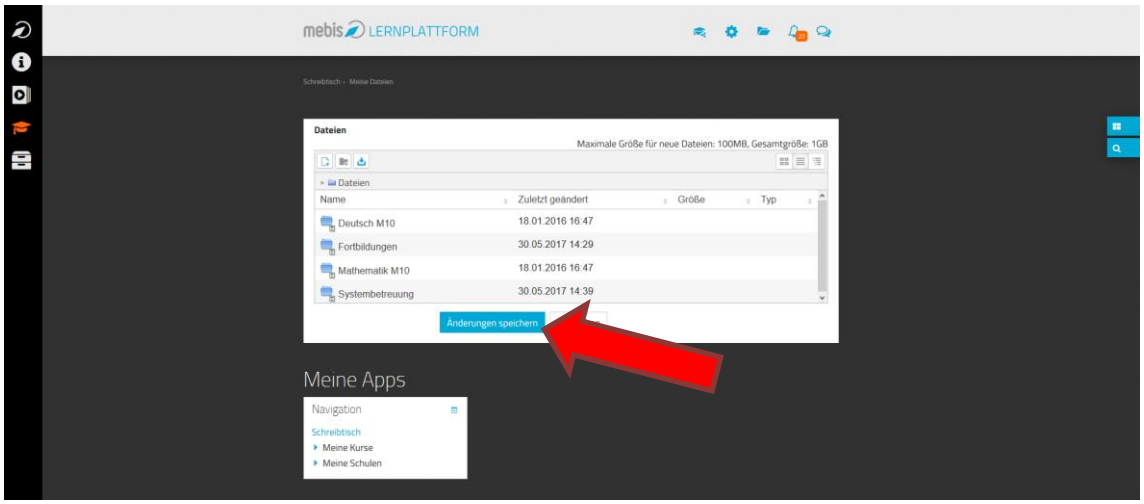
mebis kann als Cloud-Speicher genutzt werden. Hierfür gibt es zwei Möglichkeiten:

- „Eigene Dateien“ in der Lernplattform
- Speichern von Dateien in einem mebis-Kurs in der Lernplattform

## mebis – Eigene Dateien

Der Bereich „Eigene Dateien“ ist ein Teil der mebis-Lernplattform und umfasst derzeit 1 GB Speicherplatz für registrierte User.


Nach dem Erstellen von Verzeichnissen oder dem Hochladen von Dateien müssen die Änderungen immer gespeichert werden.

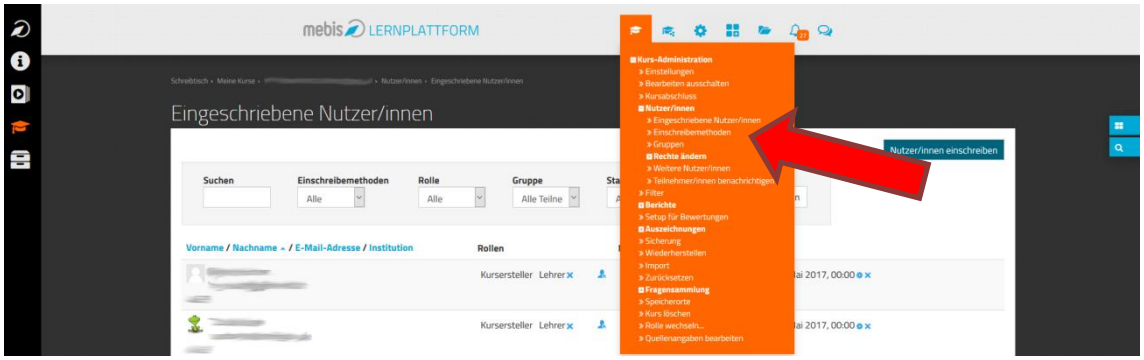


Da mebis datenschutzrechtlich freigegeben ist, dürfen in dieser „mebis-Cloud“ auch sensible Dateien abgelegt werden. Die hier abgelegten Dateien können später sehr leicht in mebis-Kurse integriert werden.

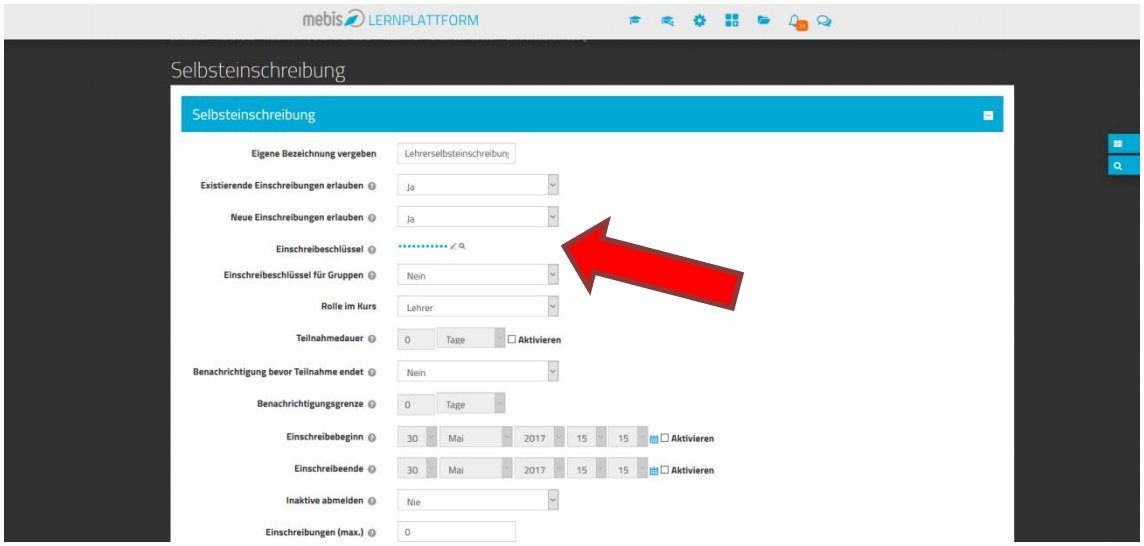
## mebis – Kurs erstellen

mebis – Lernplattform – Kurs erstellen

## mebis – Selbsteinschreibung aktivieren




Einschreibeschlüssel festlegen und Rolle der neuen Nutzer definieren




Verzeichnis hinzufügen: Bearbeiten einschalten – Material oder Aktivität hinzufügen – Verzeichnis - Hinzufügen

# VERSCHLÜSSELUNG VON VERTRAULICHEN DOKUMENTEN

Wenn vertrauliche Daten an Orten gespeichert werden sollen, die eventuell auch nicht berechtigten Personen zugänglich werden könnten, macht es Sinn diese Daten zu verschlüsseln.

Ebenso macht es Sinn, vertrauliche Daten oder auch Datenträger zu verschlüsseln, wenn diese auf einem nicht vertrauenswürdigen Weg transportiert werden.

Wenn die Verschlüsselung gut ist, können die Daten ohne den Schlüssel (Wiederherstellungsschlüssel) nicht wiederhergestellt werden. In vielen Fällen begnügt man sich mit einem Passwort, aus dem das jeweilige Programm den Wiederherstellungsschlüssel generiert. In diesem Fall ist die Verschlüsselung nur so gut wie das Passwort.

Der Vorteil einer Verschlüsselung ist gleichzeitig deren größter Nachteil. Ohne das Passwort oder den Wiederherstellungsschlüssel und ohne das zugehörige Programm sind die Daten nicht mehr zugänglich. Wer Daten verschlüsselt speichert, muss sich immer auch überlegen, wie er diese wieder entschlüsseln kann:

- Welche Programme sind erforderlich?
- Wo sind die Passwörter oder Schlüssel gespeichert?
- Können die Daten notfalls auch auf einem anderen Computer oder auf einem anderen System wiederhergestellt werden?
- Funktioniert die Wiederherstellung auch in einigen Jahren noch?

Häufig gibt es bessere Alternativen zu einer Verschlüsselung:

- Daten nur an sicheren Orten aufbewahren
- Sichere Netzwerkstruktur mit Zugriffsschutz
- Sensible Daten nicht elektronisch speichern

## Ihre Notizen

## Programme zur Verschlüsselung

### Office-Programme

Nahezu alle Office-Programme (z.B. Microsoft Office, Libre Office, Open Office) bieten die Option „Passwortschutz“. Dabei wird das jeweilige Office-Dokument mit dem Passwort geschützt und verschlüsselt. Bisher ist bei aktuellen Office-Versionen kein Verfahren bekannt, wie man ohne dieses Passwort den Inhalt lesen kann.

Dieses Verfahren eignet sich, wenn einzelne vertrauliche Dokumente geschützt werden sollen.

### BitLocker

Bitlocker ist ein Windows-Programm, das Datenträger (Partitionen oder Volumes) verschlüsselt. Es eignet sich sehr gut zur Verschlüsselung von mobilen Datenträgern (z. B. USB-Sticks), wenn mit Windows gearbeitet wird. Zur erstmaligen Einrichtung der Verschlüsselung ist eine der Professional-Versionen von Windows (Professional, Enterprise, etc.) nötig, die anschließende Nutzung ist mit beliebigen Windows-Versionen möglich.

BitLocker eignet auch sich sehr gut zur Verschlüsselung von Datenpartitionen bei Laptops mit Windows Professional-Versionen.

### 7-Zip

7-Zip ist ein Open Source Programm, das für alle Betriebssysteme erhältlich ist.

7-Zip ist ein Kompressionsprogramm mit dem Dateien oder Ordner komprimiert in einer Datei gespeichert und optional auch verschlüsselt werden können.

7-Zip eignet sich sehr gut, wenn Dateien oder Ordner mit vertraulichen Inhalten verschlüsselt archiviert oder transportiert werden sollen (z.B. Speichern von vertraulichen Daten, Ablage in einer Cloud, E-Mail-Anhänge).

### SecurStick

SecurStick wurde entwickelt, um Daten auf einem USB-Stick verschlüsselt zu transportieren. SecurStick ist betriebssystemunabhängig und erfordert keine Installation von Software oder Treibern auf den Computern, deshalb sind beim Einrichten und Ausführen keine administrativen Rechte notwendig.

SecurStick verwendet WebDAV. Unter Windows ist die Dateigröße beim Kopieren über WebDAV standardmäßig auf 47 MB beschränkt. Die Verschlüsselung großer Dateien dauert relativ lange.

SecurStick eignet sich zur Verschlüsselung von USB-Sticks, wenn die genannten Einschränkungen keine Rolle spielen.

### VeraCrypt

VeraCrypt ist das Nachfolgeprogramm von TrueCrypt und ist in der Bedienung und Anwendung nahezu identisch. Es arbeitet mit verschlüsselten Containern, die beim Öffnen ein Passwort erfordern.

VeraCrypt gewährleistet, dass auch während der Bearbeitung keine unverschlüsselten Textteile auf der Festplatte oder in einer temporären Datei abgelegt werden und bietet daher eine sehr hohe Sicherheit. Der Container kann auch auf einem Netzlaufwerk liegen, ohne dass bei der Bearbeitung unverschlüsselte Dokumente auf diesem Netzlaufwerk liegen.

Nachteilig ist, dass die Container-Größe von vorneherein festgelegt werden muss und (z.B. zur Datensicherung) auch bei geringfügigen Änderungen immer der gesamte Container kopiert werden muss.

### AxCrypt

AxCrypt ist ein Windows-Programm. Es wird als kostenlose Version und als kommerzielle Version mit erweitertem Funktionsumfang angeboten.

AxCrypt verschlüsselt die einzelnen Dokumente. Der Dateiname ist (in der kostenlosen Version) im Klartext sichtbar. Beim Öffnen eines Dokuments wird der Benutzer einmalig nach dem Passwort gefragt. Alle weiteren Dokumente, die mit demselben Passwort verschlüsselt wurden, lassen sich danach ohne erneute Passwortabfrage öffnen. Die Dateien können auch auf einem Netzlaufwerk liegen, ohne dass bei der Bearbeitung unverschlüsselte Daten auf diesem Netzlaufwerk liegen.

AxCrypt eignet sich, wenn es genügt, Dokumente einzeln zu verschlüsseln

### BoxCryptor

BoxCryptor ist ein kommerzielles Verschlüsselungsprogramm, das eine Unterstützung für alle gängigen PC-, Tablet- und Smartphone-Betriebssysteme und alle gängigen Cloud-Dienste bietet. Eine eingeschränkte Version (Nutzung von zwei Geräten) ist kostenlos.

### Cryptomator

Cryptomator verschlüsselt Dateien einzeln und ermöglicht die Synchronisierung mit Cloud-Speichern. Die Software stellt den verschlüsselten Ordner entschlüsselt als virtuelles Laufwerk zur Verfügung. Die Version für Windows, Mac, Linux und Android ist kostenlos nutzbar. Die IOS-Version ist kostenpflichtig.

# LABORÜBUNG 05 - PASSWORTSCHUTZ UND VERSCHLÜSSELUNG VON OFFICE-DOKUMENTEN

## Szenario

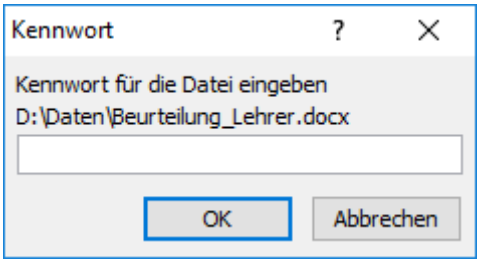
Ein vertrauliches Office-Dokument soll mit einem Passwort geschützt werden.

## Aufgaben

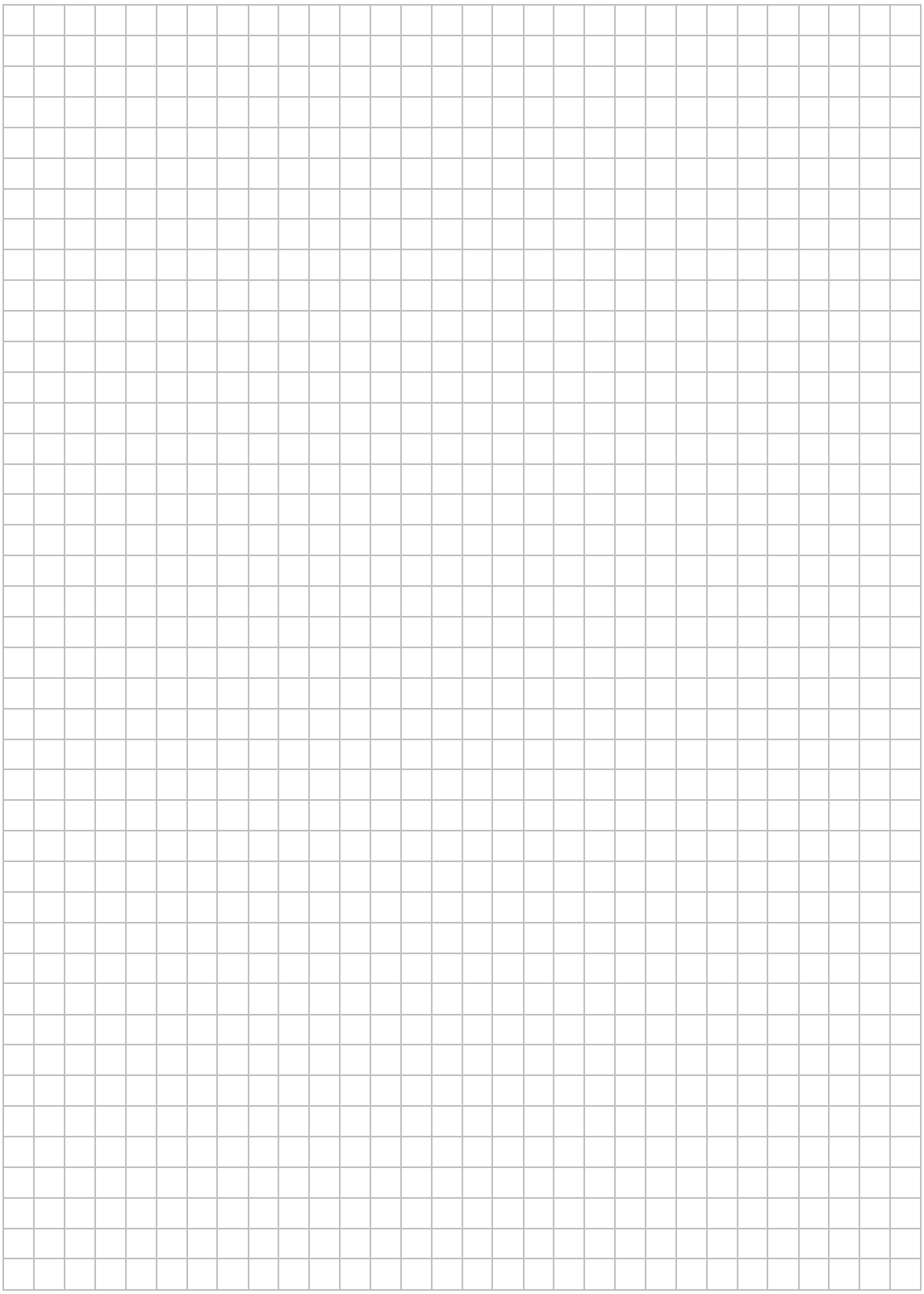
1. Erstellen Sie ein Office-Dokument (z. B. mit Microsoft-Office oder Libre-Office) und versehen Sie das Dokument mit einem Passwort.
2. Zeigen Sie, dass ohne dieses Passwort das Office-Dokument nicht geöffnet werden kann und auch mit einem anderen Programm der Inhalt nicht gelesen werden kann.

## Hinweise

Alle Office-Programme bieten die Option „Passwortschutz“. Dabei wird das jeweilige Office-Dokument mit dem Passwort geschützt und verschlüsselt. Bisher ist bei aktuellen Office-Versionen kein Verfahren bekannt, wie man ohne dieses Passwort den Inhalt lesen kann.



## Ihre Notizen



# LABORÜBUNG 06 - VERSCHLÜSSELUNG VON USB-STICKS MIT BITLOCKER

## Szenario

USB-Sticks der Lehrkräfte sollen für den Transport sensibler Daten verschlüsselt werden.

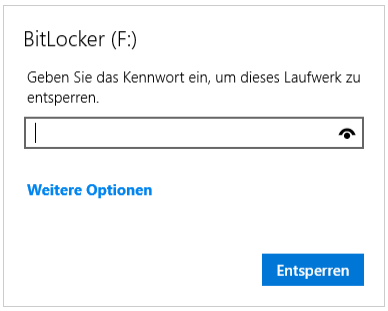
Der Systembetreuer der Schule bietet für die Lehrkräfte eine Schulung an und zeigt, wie die USB-Sticks verschlüsselt werden und wie mit den verschlüsselten USB-Sticks umgegangen wird. Für nicht IT-affine Lehrkräfte stellt der Systembetreuer USB-Sticks zur Verfügung, die mit BitLocker verschlüsselt sind und weist die Lehrkräfte in die Bedienung ein.

## Aufgaben

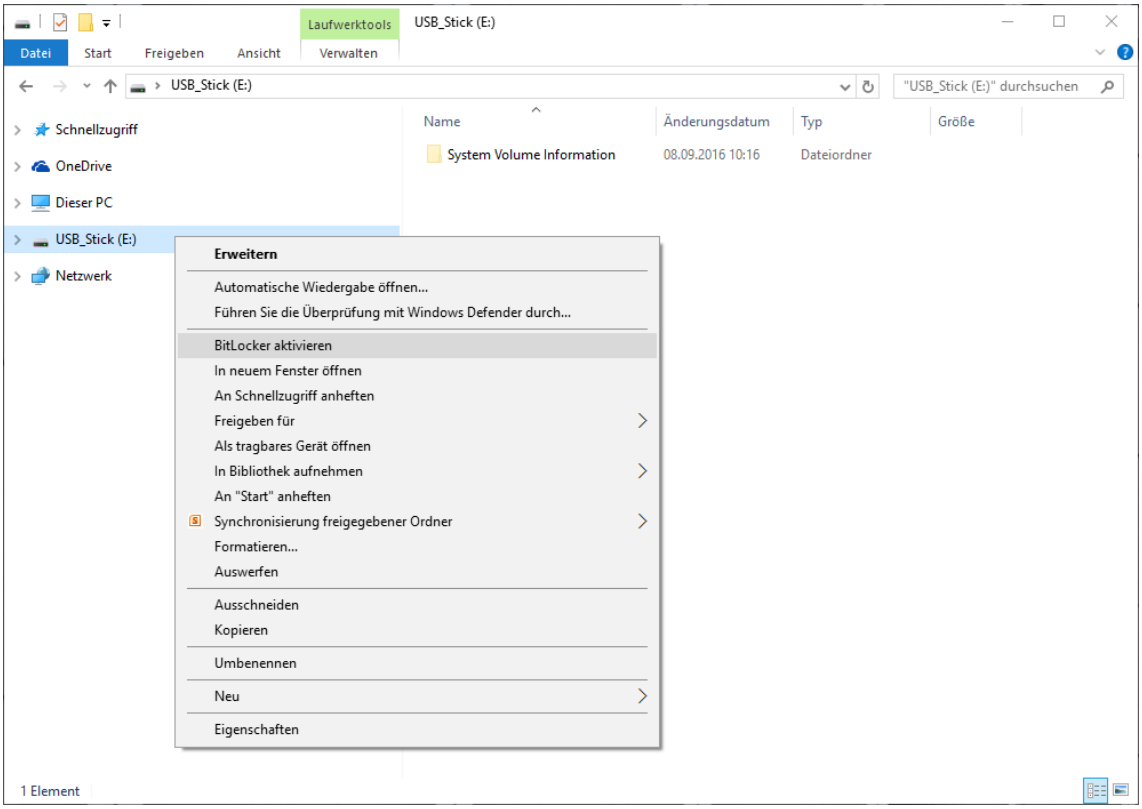
1. Verschlüsseln Sie einen USB-Stick an einem Windows-PC mit Bitlocker (Windows-Professional, Enterprise). Notieren Sie das Kennwort und drucken Sie den Wiederherstellungsschlüssel aus.
2. Testen Sie den Umgang mit dem verschlüsselten USB-Stick an verschiedenen Windows-Computern (z. B. auch an Home-Versionen von Windows).
3. Entwerfen Sie ein Schulungskonzept, wie Sie die Lehrkräfte Ihrer Schule in den Umgang mit verschlüsselten USB-Sticks einweisen (Schulungsinhalte, Zeitrahmen).

## Hinweise

Um einen USB-Stick mit BitLocker zu verschlüsseln ist eine Professional-Version von Windows (Professional, Enterprise, etc.) erforderlich. Die Benutzung eines verschlüsselten USB-Sticks ist jedoch auf allen Windows-Versionen möglich.




Die Bitlocker-Verwaltung ist im Kontextmenü eines Laufwerks zugänglich.

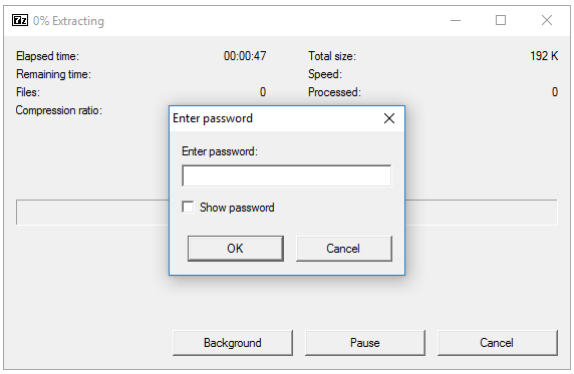



Bitlocker eignet sich auch, um z. B. Datenpartitionen auf mobilen Windows-Computern (mit Windows-Professional oder Enterprise) zu verschlüsseln.

# LABORÜBUNG 07 - VERSCHLÜSSELUNG VON DATEIEN UND ORDNERN MIT 7-ZIP

## Szenario

Mehrere vertrauliche Dokumente sollen per E-Mail versandt werden. Dazu werden die Dokumente in einem 7-Zip-Archiv gepackt, das mit einem Passwortschutz versehen wird. Das Passwort wird telefonisch übermittelt.

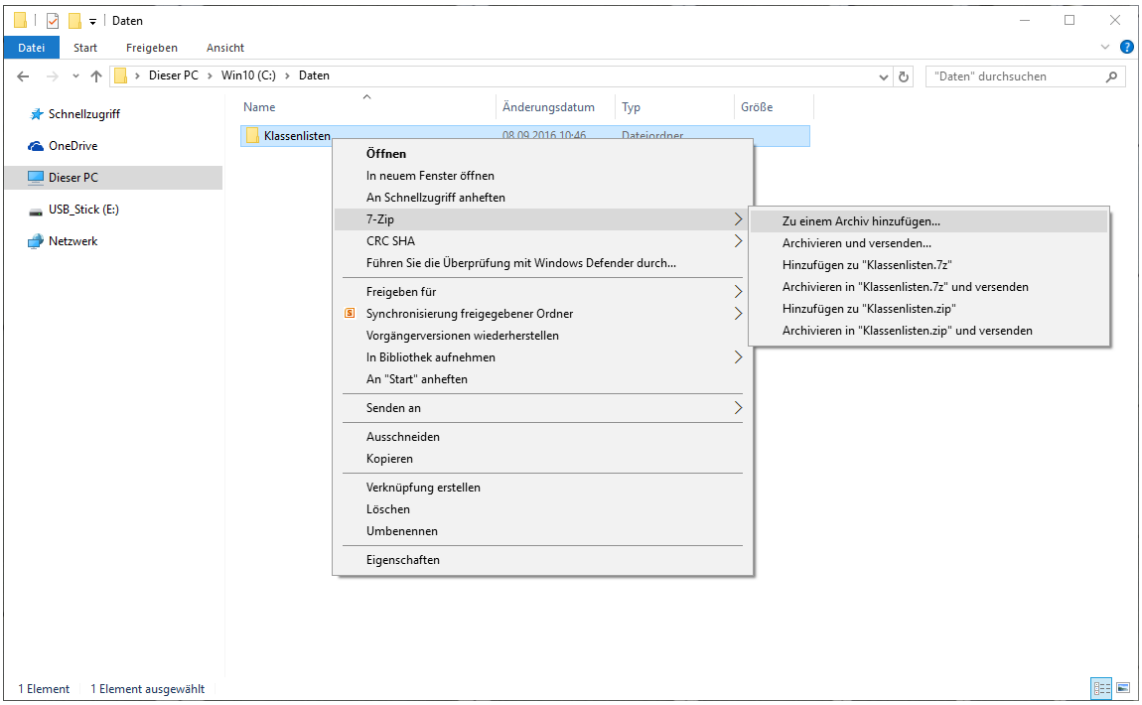


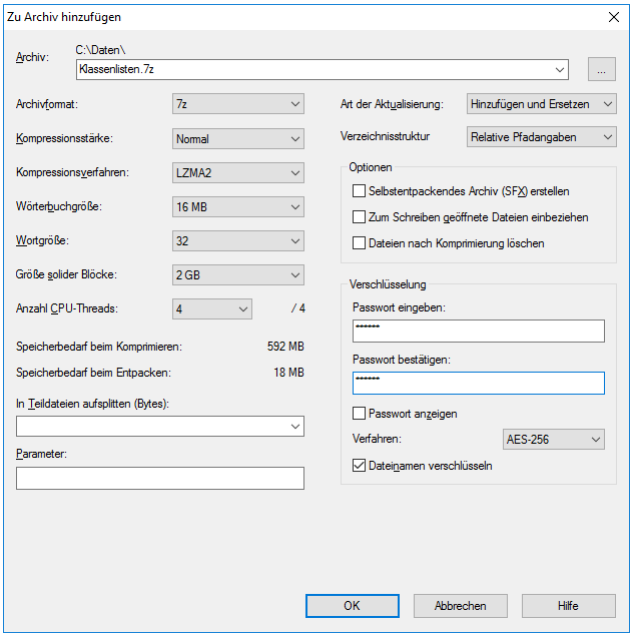

## Aufgaben

1. Packen Sie den Inhalt eines Ordners mit vertraulichen Dokumenten in ein Archiv mit 7-Zip und setzen Sie ein Passwort für die Verschlüsselung.
2. Testen Sie verschiedene Optionen (z. B. „Selbstentpackendes Archiv erstellen“, „Dateinamen verschlüsseln“) und das jeweilige Verhalten beim Auspacken des Archivs.

## Hinweise

7-Zip ist nach der Installation im Kontextmenü von Dateien und Ordnern zugänglich.



# LABORÜBUNG 08 - VERSCHLÜSSELTE CONTAINER MIT VERACRYPT

## Szenario

Vertrauliche Daten, auf die regelmäßig zugegriffen werden soll, sollen in einem Container besonders geschützt werden. Es soll gewährleistet sein, dass zu keinem Zeitpunkt unverschlüsselte Daten auf der Festplatte zu finden sind.

## Aufgaben

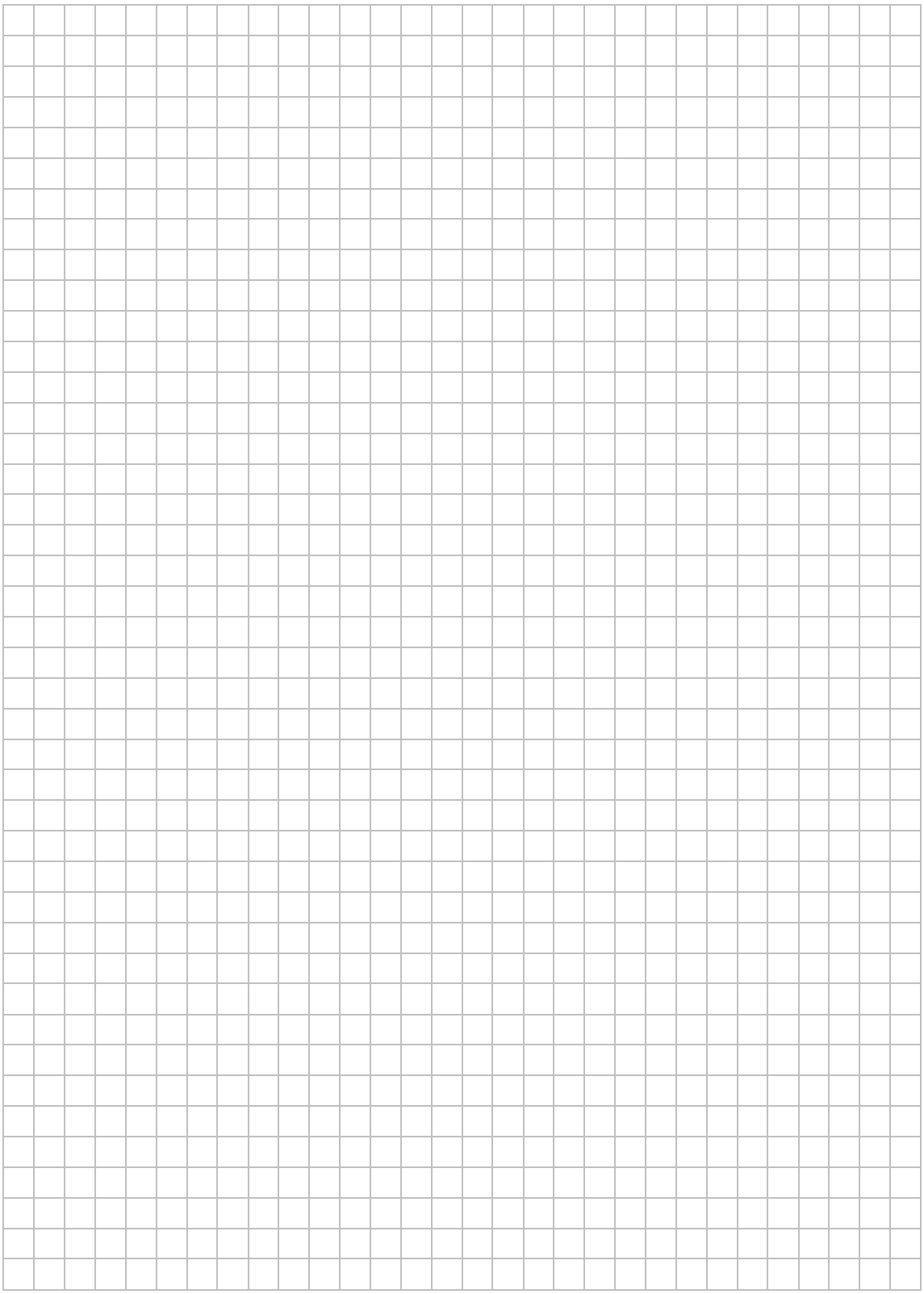
1. Erstellen Sie mit Veracrpyt einen verschlüsselten Container und legen Sie dort daten ab. Prüfen Sie die Vorgehensweise zum Entsperren und Versperren des Containers.
2. Erstellen Sie ein Batch-Skript, bei dem der lokale Tresor komfortabel nur durch die Eingabe des Passworts entsperrt wird.
3. Legen Sie den verschlüsselten Tresor auf einem Netzlaufwerk ab und prüfen Sie den Zugriff. An welcher Stelle wird der Container entsperrt?

## Hinweise

Die Bedienung von Veracrypt ist ausführlich in einem eigenen Dokument beschrieben.

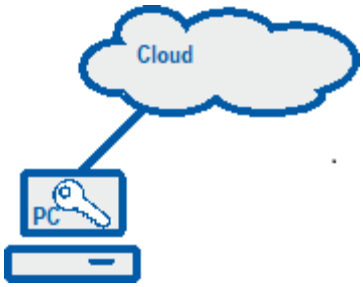
(http://alp.dillingen.de/schulnetz/materialien/Veracrypt.pdf)

## Ihre Notizen



# LABORÜBUNG 09 - VERSCHLÜSSELUNG VON DATEN IN DER CLOUD MIT CRYPTOMATOR

## Szenario




Ein Lehrer möchte neben seiner Unterrichtsvorbereitung auch sensible Daten (Proben, Lösungen, Noten, Informationen zum Lernstand) in seinem Online-Speicher ablegen. Diese sollen sowohl lokal als auch in der Cloud verschlüsselt werden.

## Aufgaben

1. Erstellen Sie einen lokalen Tresor und legen Sie dort Dateien ab. Überprüfen Sie anschließend die Verschlüsselung.

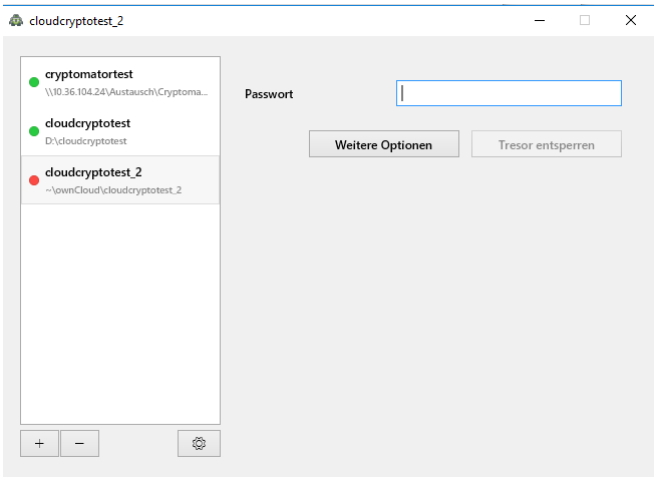
Verschlüsselung in einem Netzwerkspeicher

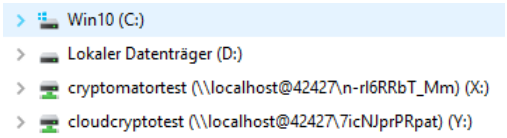
2. Testen Sie einen weiteren Speicherort (z. B. Netzwerkfreigabe) für Tresore und greifen Sie von einem anderen Rechner auf die verschlüsselten Daten zu.

Verschlüsselung in der Cloud

3. Legen Sie den Tresor im lokalen Ordner, der mit der Cloud synchronisiert wird, an. Greifen Sie von einem anderen PC auf die verschlüsselten Daten zu.
4. Testen Sie, in wieweit Sie mit anderen Systemen (z.B. Android, IOS, Smartphone, Tablet) auf die verschlüsselten Daten in der Cloud zugreifen können.

## Hinweise


cloudcryptotest_2
cryptomatortest
cloudcryptotest
D:\cloudcryptotest
cloudcryptotest_2
Passwort
Weitere Optionen
Tresor entsperren


Win10 (C:)
Lokaler Datenträger (D:)
cryptomatortest (\\localhost@42427\n-rl6RRbT_Mm) (X:)
cloudcryptotest (\\localhost@42427\7icNJprPRpat) (Y:)

# LABORÜBUNG 10 - VERSCHLÜSSELN VON DATEN AUF EINER NAS-BOX

## Szenario

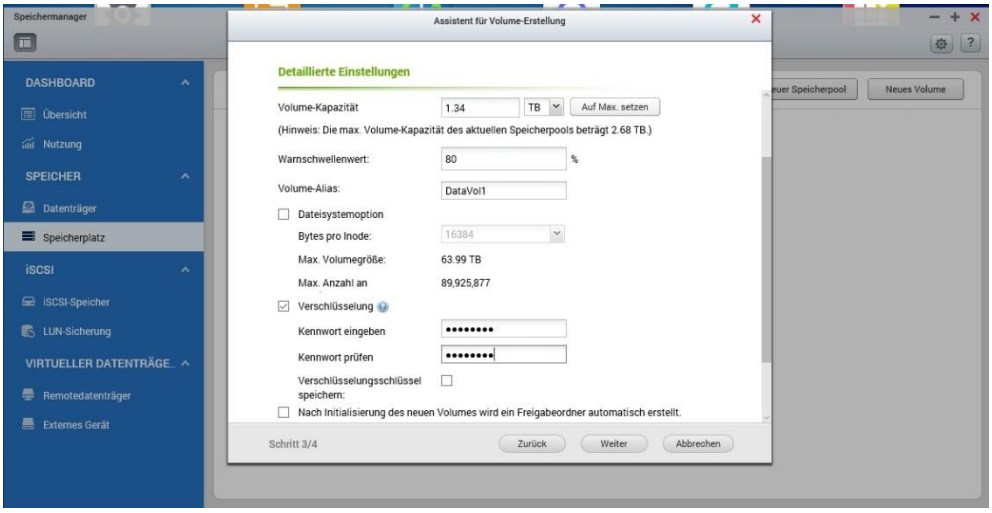
Um die Daten auf einer NAS-Box bei einem eventuellen Diebstahl der NAS-Box zu schützen, sollen diese in einem verschlüsselten Bereich abgelegt werden. Bei einem Neustart der NAS-Box muss erst ein Passwort eingegeben werden, damit auf die Daten zugegriffen werden kann.


## Aufgaben

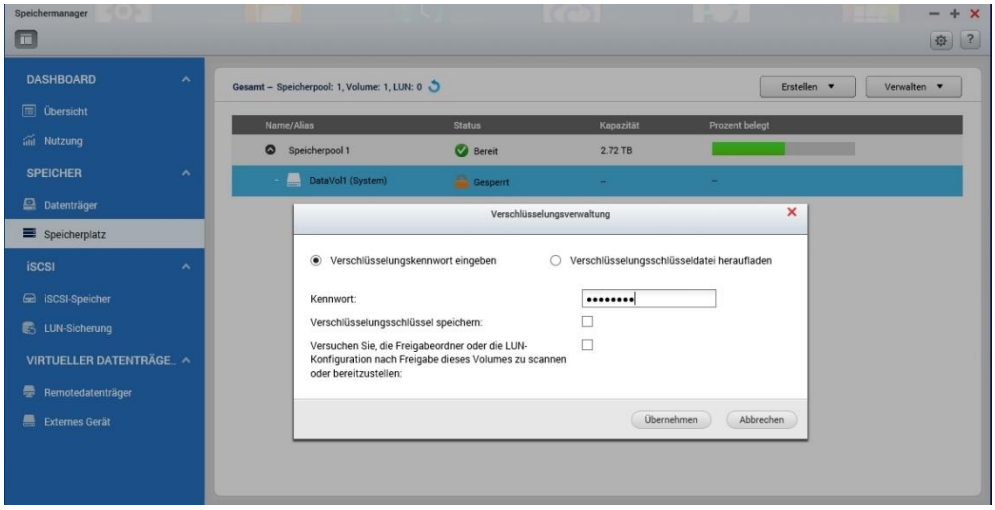
1. Erstellen Sie auf der NAS-Box ein neues Volume. Das Volume soll verschlüsselt sein. Der Schlüssel wird nicht gespeichert.
2. Entsperren Sie das Volume, erstellen eine Freigabe, verbinde diese mit dem PC und speichern einige Testdaten darauf.
3. Starten sie die NAS-Box neu.
4. Versuchen Sie auf die Freigabe zuzugreifen.
5. Loggen Sie sich auf der NAS-Box ein und entsperren das Volume. Verbinden Sie sich jetzt mit der Freigabe.

# HINWEISE

Das gesamte Volume einer NAS-Box soll verschlüsselt werden. Dies geschieht beim Erstellen eines neuen Volumes. Eine nachträgliche Verschlüsselung ist nicht möglich. Der Verschlüsselungschlüssel wird nicht gespeichert.




Beim Entsperren eines gesperrten Volumes ist der Verschlüsselungsschlüssel einzugeben. Der Schlüssel wird nicht gespeichert.



# DATENSICHERUNG

Elektronisch gespeicherte Daten können verloren gehen. Die Gründe dafür sind vielfältig:

### Versehentliches Löschen von Daten

Das versehentlich Löschen oder Überschreiben von Daten ist vermutlich die häufigste Ursache für einen Datenverlust. Wenn man den Datenverlust sofort bemerkt, kann man auf die letzte Datensicherung zurückgreifen. Diese sollte sinnvollerweise nicht zu lange zurückliegen.

Eine andere Situation ergibt sich, wenn man den Datenverlust erst nach längerer Zeit bemerkt. Hier muss man auf eine länger zurückliegende Sicherung zugreifen (Datenarchivierung).

### Defekte Hardware

Defekte Hardware, speziell defekte Festplatten waren bisher ein Hauptgrund, auf die Notwendigkeit der Datensicherung hinzuweisen. Gleichzeitig wird die Datensicherung vernachlässigt, da die Hardware relativ zuverlässig und langlebig ist.

Defekte Hardware erfordert natürlich eine Datensicherung, dennoch ist der administrationsaufwand bei einer defekten Hardware sehr hoch. (Server müssen z. B. neu installiert werden.) Es lohnt sich deshalb – neben der Datensicherung – vorbeugende Maßnahmen zu treffen, damit es möglichst selten zu einem Ausfall der Hardware kommt. Dazu gehören:

- Server-Festplatten, die für den Dauerbetrieb geeignet sind
- Festplatten im RAID-Verbund
- Erneuerung der Hardware nach spätestens 5 Jahren
- Geeigneter Standort der zentralen Geräte (Temperatur, Staubbelastung)
- Überwachung (Monitoring) der Server bzw. zentralen Geräte

### Verschlüsselungstrojaner

Verschlüsselungstrojaner sind ein aktuelles Problem, da einige Personen erkannt haben, dass es in vielen Betrieben oder Verwaltungen keine Datensicherung gibt und dass man deshalb nach dem Verschlüsseln von Daten für die Herausgabe des Schlüssels Geld verlangen kann.

Der übliche Verbreitungsweg für Verschlüsselungstrojaner sind E-Mail-Anhänge. Wenn ein solcher Anhang (z. B. ausführbare exe-Datei, Java-Script-Datei, Office-Dokument mit Makros) ausgeführt wird, wird der Trojaner aktiv. Er kann prinzipiell auf alles zugreifen, auf das der jeweilige Benutzer schreibenden Zugriff hat (lokale Dokumente, angeschlossene USB-Laufwerke, Serverlaufwerke, Cloud-Anbindungen).

Durch Schulung der Anwender kann man die Gefährdung reduzieren, wirklich verhindern kann man sie nicht. In Client/Server-Umgebungen kann man die Auswirkungen begrenzen, indem man den Benutzern nicht in allen Bereichen Schreibrechte gewährt. Viele schon seit Jahrzehnten propagierten Grundregeln für die Arbeit am Computer gewinnen wieder neue Bedeutung:

- Unbekannte Dokumente oder Mail-Anhänge werden nicht geöffnet.
- Man arbeitet nicht als Administrator sondern als normaler Benutzer
- Jeder Benutzer hat nur dort Schreibrechte, wo er sie wirklich benötigt.

Bei der Datensicherung muss man darauf achten, dass der Verschlüsselungstrojaner keinen Zugriff auf die Datensicherung hat.

Ein Testbericht eines Verschlüsselungstrojaners ist unter
http://alp.dillingen.de/schulnetz/materialien/Verschluesselungstrojaner.pdf
veröffentlicht.

### Gezielte Sabotage

Im Gegensatz zu einem Verschlüsselungstrojaner, der mehr oder weniger ungezielt Daten verändert, nutzt eine gezielte Sabotage bewusst Schwachstellen oder Eigenheiten des jeweiligen Systems aus.

### Diebstahl von Hardware

Werden Geräte gestohlen, sind natürlich auch die Daten weg, auch wenn dies vermutlich nicht der eigentliche Zweck des Diebstahls war.

Die Vorbeugung muss hier in verschiedene Richtungen gehen:

- Physikalischer Schutz der zentralen Komponenten einer Schule (Serverraum)
- Datensicherung an unterschiedlichen Orten
- Verschlüsselung der Daten auf Geräten, bei denen Diebstahl eine reale Gefahr darstellt (z. B. Notebook mit vertraulichen Daten, NAS-Box zur Datensicherung, USB-Stick mit vertraulichen Daten)

### Katastrophen

Bei größeren Schadensereignissen (Brand, Blitzschlag, Überschwemmung, Gasexplosion) können gespeicherte Daten und auch die Datensicherung betroffen sein.

Von einem Blitzschlag können alle angeschlossenen Geräte betroffen sein. USV-Anlagen können hier einen gewissen Schutz bieten. Gegen Wasserschäden kann man vorbeugen, indem man die zentralen Geräte nicht im Keller und in Bodennähe aufstellt. Gegen andere größere Schadensereignisse helfen nur räumlich getrennte Systeme.

## Ihre Notizen

## Konzepte zur Datensicherung

Wenn elektronisch gespeicherte Daten eine Bedeutung haben, sollte man über das Thema „Datensicherung“ nachdenken.

### Auswahl der zu sichernden Daten

Nicht alle Daten sind gleich wichtig. In der Schule kann man sich beispielsweise entscheiden, die Homeverzeichnisse von Schülern und Lehrkräften nicht zu sichern, während Daten aus der Schulverwaltung in ein Sicherungskonzept eingebaut werden.

Zu Hause kann man sich entscheiden, Videofilme oder Musikdownloads nicht zu sichern, aber die Unterrichtsvorbereitung regelmäßig zu sichern.

### Auswahl der Backup-Medien

In großen Rechenzentren und Verwaltungsumgebungen gibt es eigene Systeme zur Datensicherung, die für Schulen oder einzelne Lehrkräfte zu groß ausgelegt sind.

Zur Datensicherung in der Schule stellen externe Festplatten bzw. SSD-Speicher, NAS-Systeme (Network-Attached-Storage), eine redundante Verteilung der Daten auf mehrere Server oder Backup-Server sinnvolle Möglichkeiten dar. Professionelle Bandlaufwerke sind für einzelne Schulen überdimensioniert und erfordern auch eine entsprechende Betreuung.

Zunehmend werden auch Cloud-basierte Backup-Lösungen angeboten, die als Ergänzung für eine Datensicherung innerhalb der Schule sinnvoll sein können. Dabei sind die datenschutzrechtlichen Bestimmungen zu beachten.

Bei der Datenarchivierung muss vor allem auf die Langlebigkeit der verwendeten Technik und der Medien geachtet werden. Dafür eignen sich derzeit auch noch CD-Brenner oder DVD-RAM-Brenner.

### Häufigkeit der Sicherung

In der Schulverwaltung (z. B. ASV) sind ein Jahr alte Daten nutzlos. Die Fotosammlung zu Hause (z. B. Urlaubsfotos) muss hingegen nicht täglich gesichert werden. Eine Datenarchivierung ist hier wesentlich sinnvoller.

### Datenbanksicherung

Datenbanken werden üblicherweise nicht dateiweise sondern über einen Dump (mysqldump, pgdump) zunächst lokal gespeichert. Dieser Dump wird in das Sicherungskonept eingebaut.

### Systemsicherung eines PC oder Notebooks

Die Einrichtung eines PC kann sehr viel Arbeit gemacht haben, so dass es sinnvoll ist, diese Installation zu speichern. Wenn der PC nicht mehr richtig läuft (z. B. durch fehlerhafte Programme oder einen Virusbefall) kann die Systemsicherung zurückgespielt werden. In Frage kommen dazu Imaging-Programme (z. B. Drive Snapshot, Acronis, Part-Image etc.). Um eine Systemsicherung wieder zurückzuspielen benötigt man eventuell weitergehende Kenntnisse (Startmedium, Einrichten des Bootmanagers, etc.).

### Systemsicherung eines Servers

Am einfachsten ist die Serversicherung bei virtualisierten Servern (ESXi, Hyper-V). Die virtuellen Maschinen können automatisiert gesichert werden (z.B. Ghetto-VCB unter ESXi). Das Virtualisierungssystem selbst muss nicht gesichert werden, da es bei Bedarf sehr schnell wieder eingerichtet ist.

### Sicherung von Daten mit Berechtigungen

Auf einem Server liegen Benutzerdaten in den Home-Verzeichnissen der einzelnen Benutzer. Sollen diese Daten gesichert werden, müssen auch die Dateirechte mitgesichert werden, da ansonsten die eventuelle Wiederherstellung sehr aufwändig wird.

Die Sicherung muss dazu entweder auf einem gleichartigen System (z. B. NTFS-Partition mit robocopy) erfolgen oder in einem Archiv, in dem die Berechtigungen erhalten bleiben (z.B. tar unter Linux, 7zip oder proprietäres Archiv unter Windows).

### Automatisierung der Datensicherung

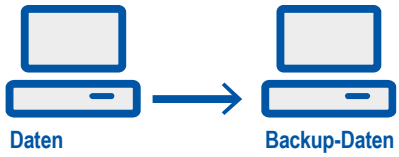
Die regelmäßige Datensicherung sollte automatisiert und ohne Benutzereingriffe erfolgen. Nur so ist gewährleistet, dass sie auch durchgeführt wird. Sinnvoll ist es auch, wenn der Administrator automatisch über den Erfolg der Datensicherung informiert wird.



# LABORÜBUNG 11 - SZENARIEN ZUR DATENSICHERUNG

## Szenario

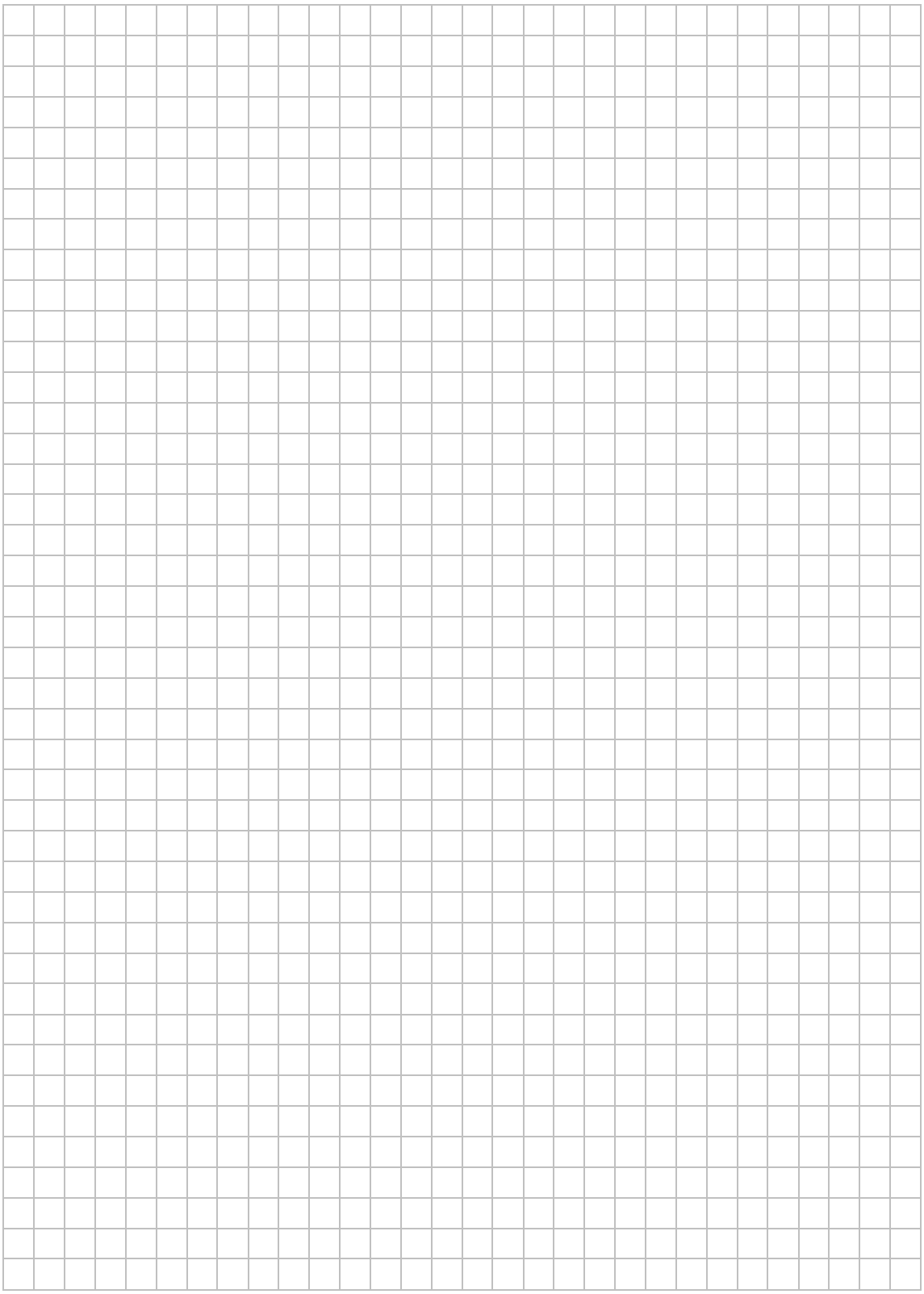
Verschiedenen Szenarien von möglichen Datenverlusten soll mit geeigneten Sicherungsstrategien begegnet werden.




## Aufgaben

1. Sammeln Sie verschiedene realistische Szenarien für mögliche Datenverluste.
2. Entwerfen Sie geeignete Maßnahmen, um zukünftig Datenverluste zu vermeiden oder zu reduzieren.
3. Entwerfen Sie ein Sicherungskonzept für Sie zu Hause, für Ihre Schule oder für Ihren Verantwortungsbereich.
   - Was wird gesichert?
   - Wie häufig wird gesichert? (nur bei bestimmten Anlässen, Tagesbackup, Wochenbackup, Archivierung, …)
   - Wohin wird gesichert? (zweite Festplatte, Backupserver, USB-Platte, …)
   - Wie automatisiert erfolgt die Sicherung? (vollständig automatisiert, auf Knopfdruck, …)
   - Wie können die Daten gegebenenfalls wiederhergestellt werden?

## Ihre Notizen



## Fallbeispiele zur Datensicherung

## Der Lehrerarbeitsplatz zu Hause

Die Unterrichtsvorbereitung liegt lokal auf einem Desktop-Computer oder auf einem Notebook. Für die Unterrichtsvorbereitung soll eine Datensicherung eingerichtet werden.

### Datensicherung auf externe USB-Festplatten

Zur Datensicherung sind mehrere USB-Festplatten verfügbar. Die Datensicherung erfolgt auf die USB-Festplatten, die abwechselnd benutzt werden und nach der Datensicherung vom Computer getrennt werden. Wenn die USB-Festplatten groß genug sind, können auch mehrere Datensicherungs-Versionen gespeichert werden (Datenarchivierung).

Die Datensicherung erfolgt halbautomatisch auf „Knopfdruck“ (USB-Festplatte anstecken – Vorbereitetes Desktop-Icon zum Start der Datensicherung drücken – Nach Beendigung USB-Festplatte entfernen).

## Unterrichtsnetz einer kleinen Schule

Als zentraler Ablageort im Unterrichtsnetz dient eine NAS-Box. Auf dieser existieren Vorlagen- und Austauschlaufwerke mit unterschiedlichen Schreib- und Leseberechtigungen für Lehrkräfte und Schüler sowie ggf. persönliche Ablageorte der einzelnen Lehrkräfte. Die größte Datenmenge beanspruchen die Systemimages, die zur Wiederherstellung der Computer im Unterrichtsnetz dienen.

### Datensicherung NAS-to-NAS

Als Backupserver dient eine zweite NAS-Box (automatische NAS-to-NAS-Sicherung). Gegebenenfalls können einzelne Sicherungen umbenannt werden (z. B. Backup_20161006), so dass dieser Zustand erhalten bleibt.

## Schulverwaltung einer kleineren Schule

Als zentraler Ablageort dient ein Windows-Server (ASV-Server und Datei-Server), auf den die Schulleitung und das Sekretariat Zugriff haben. Alle relevanten Daten befinden sich auf diesem Server.

### Vertrauliche Daten der Schulleitung

Die Schulleitung speichert vertrauliche Daten in einer verschlüsselten Form auf dem Server ab. Dadurch werden diese Daten gesichert, sind aber nur lesbar, wenn das Passwort bekannt ist.

### ASV-Backup

Die relevanten Daten der ASV sind in einer Postgres-Datenbank gespeichert. Diese Datenbank wird täglich mit einem Dump (pgdump) gesichert, der Datenbank-Dump wird im Datenbereich des Servers abgelegt, so dass dieser in die normale Sicherungskette integriert ist.

### Datensicherung auf eine NAS-Box

Der Datenbereich des Servers wird täglich auf eine NAS gesichert, (Tagessicherung, Monatssicherung). Die Tagessicherung wird täglich überschrieben, gelegentlich wird eine Tagessicherung umbenannt (z. B. Backup_2018_01_24), so dass dieser Zustand erhalten bleibt.

Die NAS-Box befindet sich nicht im selben Raum, wie der Server der Schule. Das Datenvolume der NAS-Box ist verschlüsselt und mit einem Passwort gesichert (Schutz der Daten bei einem Diebstahl der NAS).

### Zusätzliche Datensicherung auf USB-Festplatten

Zusätzlich gibt es mehrere USB-Festplatten, die als Ergänzung zur Datensicherung des Servers benutzt werden (manuelle oder halbautomatische Sicherung).



# LABORÜBUNG 12 - DATENSICHERUNG AUF MOBILEN FESTPLATTEN

## Szenario


Auf dem Arbeitsplatzcomputer eines Lehrers liegen im Verzeichnis „Daten“ alle relevanten Daten für die Unterrichtsvorbereitung. Der Lehrer möchte dieses Verzeichnis regelmäßig auf zwei mobilen USB-Festplatten sichern, die er abwechselnd benutzt.

## Aufgaben

1. Kopieren Sie die das Verzeichnis „Daten“ mit dem Windows-Explorer auf die mobile Festplatte. Verändern Sie einige Dokumente und wiederholen Sie den Kopiervorgang.
2. Testen Sie die Datensicherung mit dem Programm Synctoy auf zwei verschiedenen USB-Festplatten oder USB-Sticks.
3. Testen Sie das Kommandozeilenwerkzeug robocopy zur Datensicherung. Erstellen Sie ein Skript, das die Datensicherung „auf Knopfdruck“ ausführt.

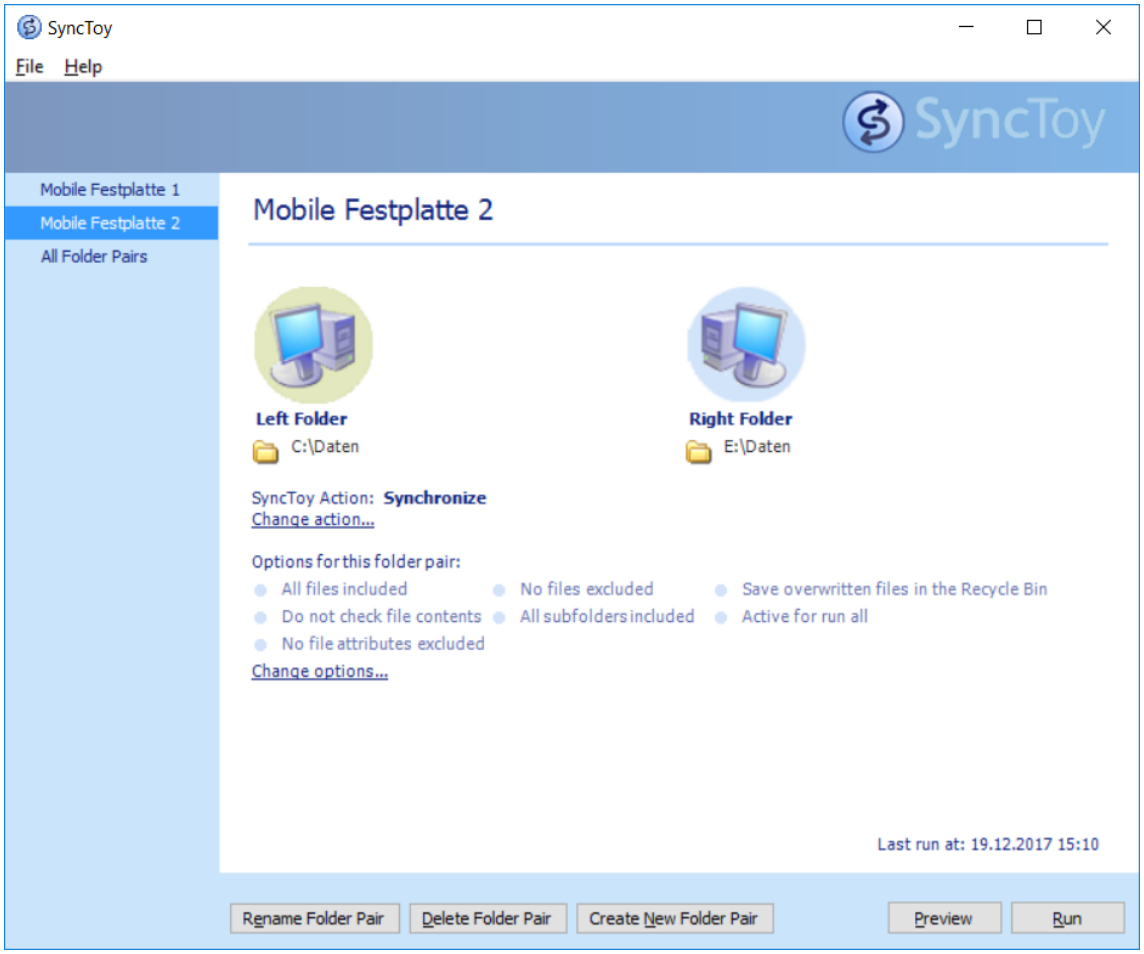
## Hinweise

Im Prinzip können statt der mobilen USB-Festplatten auch USB-Sticks verwendet werden, wenn diese genügend Platz bieten.

## Synchronisation von Daten mit SyncToy

Das von Microsoft zur Verfügung gestellte Programm SyncToy kann Daten zwischen zwei Orten (z. B. PC und mobile Festplatte) synchronisieren. Diese Synchronisation kann auch so eingerichtet werden, dass sie in beiden Richtungen funktioniert.

An Grenzen stößt die Synchronisation, wenn Daten gleichzeitig an verschiedenen Orten (z. B. durch unterschiedliche Benutzer) bearbeitet werden.



### Synctoy bietet 3 Verfahren an:

- Synchronisation (in beide Richtungen)
- Echo (Quelle -> Ziel; gelöschte Daten in Quelle werden auch im Ziel gelöscht)
- Contribute (Quelle -> Ziel; gelöschte Daten in Quelle bleiben im Ziel erhalten)

### Probleme beim Löschen von Daten im Zielordner (Echo und Contribute).

Wird eine Datei im Zielordner gelöscht, dann wird sie beim nächsten Sicherungsvorgang nicht mehr berücksichtigt und somit nicht mehr gesichert.

### Erkennen von Veränderungen

SyncToy vergleicht nur das Sicherungsdatum. Inhaltliche Veränderungen bei einem mit Veracrypt angelegten Container werden vom Programm nicht erkannt.

## Kopieren von Daten mit robocopy

Die Kommandozeilen-Tool *robocopy.exe* (Nachfolger von xcopy) ist seit Windows Vista im Betriebssystem enthalten. Eine ausführliche Dokumentation findet man in der Datei *robocopy.doc* oder mit *robocopy /?*. Zu robocopy gibt es auch grafische Benutzeroberflächen zum Download (Suchbegriff: robocopy gui).

```
robocopy <Quelle> <Ziel> <Optionen>
robocopy <Quelle> <Ziel> /MIR              vollständige Kopie
```

**Achtung:** Die Option `/MIR` (Mirror) kopiert eine Verzeichnisstruktur mit allen Dateien und Unterverzeichnissen und löscht auch im Zielverzeichnis alle Dateien, die im Quellverzeichnis nicht vorhanden sind.

## Einfaches Beispielskript für eine Datensicherung auf einem USB-Laufwerk

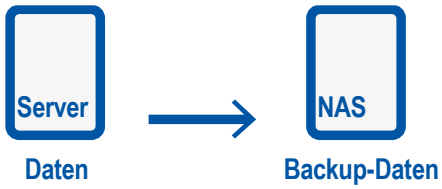
Bei der Sicherung auf einen USB-Laufwerk ist es wichtig vor der Sicherung zu überprüfen, ob die richtige USB-Festplatte angeschlossen ist. Die Datensicherung bricht deshalb ab, wenn das Ziellaufwerk nicht existiert.

```
@ECHO OFF

set Quelle=D:\Daten\
set Ziel=E:\Daten\

IF NOT EXIST %Quelle% color CF & echo %Quelle% exist. nicht & goto Fehler
IF NOT EXIST %Ziel%   color CF & echo %Ziel% existiert nicht & goto Fehler

robocopy %Quelle% %Ziel% /MIR

pause
exit

:Fehler
pause
exit
```

# LABORÜBUNG 13 - SICHERUNG VON DATEN EINES WINDOWS-SERVERS MIT DUPLICATI

## Szenario

Auf einem Windows-Server liegen im Verzeichnis „Daten“ alle relevanten Daten (z. B. für die Schulverwaltung oder für die Unterrichtsvorbereitung der Lehrkräfte etc.). Das Verzeichnis Daten soll täglich auf eine NAS-BOX gesichert werden.




## Aufgaben

1. Richten Sie auf Ihrem Windows-PC (der den Server simulieren soll) ein Verzeichnis „Daten“ ein und legen Sie einige Dokumente in diesem Verzeichnis ab.
2. Das Ziel der Datensicherung soll eine Freigabe auf einer NAS-Box sein.
3. Richten Sie mit Duplicati einen Sicherungsjob ein, der die Daten regelmäßig sichert
   - Grundsicherung,
   - inkrementelle Sicherungen (alle 2 Minuten in der Testphase),
   - vollständige Sicherung nach einem bestimmten Zeitrahmen,
   - automatisches Löschen älterer Sicherungen}.
4. Simulieren Sie das Arbeiten im Datenverzeichnis (Dokumente anlegen, Dokumente verändern, Dokumente löschen).
5. Stellen Sie eine bestimmte Version eines Dokumentes wieder her.

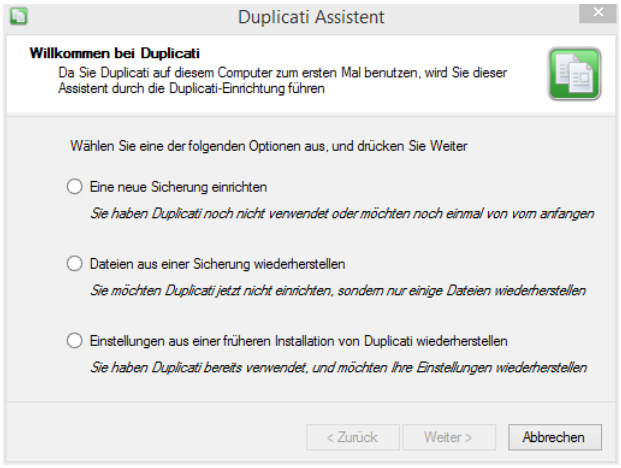
## Hinweise

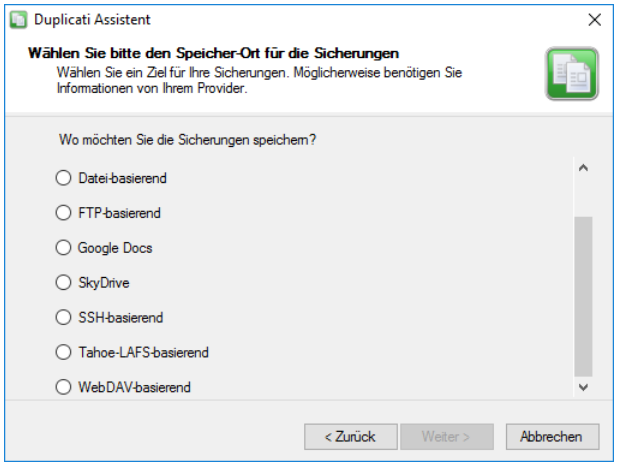
### Eigenschaften von Duplicati

- Duplikate kennt sehr viele mögliche Sicherungsziele (Windows-Systeme, Linux-Systeme, NAS-Boxen, Cloud-Dienste) und Übertragungsprotokolle (z. B. smb, FTP, webdav, ssh).
- In der Version 1 keine Sicherung der NTFS-Rechte.
- Eine Erfolgskontrolle der Sicherung ist nur durch einen Test oder durch das Sicherungsprotokoll möglich.

## Datensicherung mit Duplicati

Nach der Installation von Duplicati kann mit Unterstützung eines Assistenten ein Sicherungsauftrag erstellt werden.

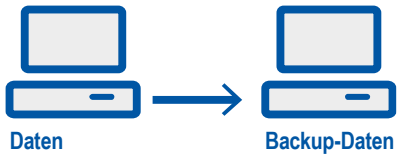


# LABORÜBUNG 14 - SICHERUNG VON DATEN EINES WINDOWS-SERVERS MIT ROBOCOPY

## Szenario

An einem Server sind alle sicherungsrelevanten Benutzerdaten im Ordner *Daten* abgelegt. Dieser Ordner soll regelmäßig und automatisiert mit robocopy gesichert werden.




## Aufgaben

1. Schreiben Sie ein Skript, das den Ordner *Daten* in den Ordner *Backup_Daten* (zunächst am gleichen Computer) sichert. Achten Sie gegebenenfalls darauf, dass die NTFS-Berechtigungen mit gesichert werden.
2. Geben Sie den Ordner *Backup_Daten* lesend frei, so dass alle Benutzer (mit entsprechenden Berechtigungen) auf die gesicherten Daten zugreifen können.
3. Automatisieren Sie die Datensicherung mit dem Windows-Taskplaner, so dass der Ordner *Daten* automatisch einmal am Tag (in der Testphase alle 2 Minuten) gesichert wird.
4. Definieren Sie einen Ihrer Computer als Backup-Server und schreiben Sie ein Skript, das den Ordner *Daten* über das Netzwerk auf dem Backup-Server sichert. Automatisieren Sie diese Datensicherung.

# HINWEISE

### Eigenheiten von robocopy

- Robocopy sichert jede Datei einzeln. Die Wiederherstellung von einzelnen Dateien ist dadurch sehr einfach. Wenn das Zielverzeichnis NTFS-Rechte unterstützt, können diese mitgesichert werden.
- Mit Robocopy sind keine inkrementellen Sicherungen möglich. Der Netzzugriff muss bereits existieren oder muss mit anderen Werkzeugen hergestellt werden.

## Datensicherung mit robocopy

Die Kommandozeilen-Tool *robocopy.exe* ist seit Windows Vista im Betriebssystem enthalten. Eine ausführliche Dokumentation findet man in der Datei *robocopy.doc* oder mit *robocopy /?*. Zu robocopy gibt es auch grafische Benutzeroberflächen zum Download (Suchbegriff: robocopy gui).

```
robocopy <Quelle> <Ziel> <Optionen>
robocopy <Quelle> <Ziel> /MIR              vollständige Kopie
robocopy <Quelle> <Ziel> /MIR /COPYALL     kopiert auch NTFS-Rechte
```

Die Option `/MIR` (Mirror) kopiert eine Verzeichnisstruktur mit allen Dateien und Unterverzeichnissen und löscht auch im Zielverzeichnis alle Dateien, die im Quellverzeichnis nicht vorhanden sind.

Für das Quell- und Zielverzeichnis können auch Netzwerkpfade angegeben werden:

```
robocopy D:\Daten \\server\freigabe\Backup_Daten /MIR
```

Der Befehl kopiert den Inhalt von *D:\Daten* auf den Server in den Ordner *Backup_Daten*. Dort werden veraltete Daten ersetzt, fehlende ergänzt und überzählige Dateien und Ordner gelöscht.

In Skripten können noch weitere Optionen von Interesse sein:

| | |
|---|---|
| `/R:n` | Anzahl der Versuche bei fehlerhaften Kopiervorgängen (Standard 1 Million) |
| `/W:n` | Wartezeit zwischen den Versuchen (Standard 30 Sekunden) |
| `/LOG:Logdatei` | schreibt die Ausgabe in eine Logdatei (ersetzt eine vorhandene Logdatei) |

| | |
|---|---|
| `/LOG+:Logdatei` | schreibt die Ausgabe in eine Logdatei (ergänzt eine vorhandene Logdatei) |
| `/TEE` | schreibt die Ausgabe in eine Logdatei und auf den Bildschirm |

## Beispielskript für eine Datensicherung auf einen Backupserver

Die Datensicherung sollte automatisiert täglich ablaufen (Windows-Taskplaner). In einer Logdatei wird protokolliert, ob die Datensicherung erfolgreich war. Über errorlevel können mögliche Fehler abgefangen werden.

```
@ECHO OFF

set Logfile=D:\logfile.log
set Quelle=D:\Daten\

net use x: \\BackupServer\Freigabe /user:<Benutzer> <Passwort>
if errorlevel 1 (
   echo ... (Fehlermeldungen)  >> %Logfile%
   goto Ende
)
set Ziel=x:\Backup_Daten\

echo.                                                 >> %Logfile%
echo ------------------------------------------------  >> %Logfile%
echo Datensicherung: %computername%, %date% %time%  >> %Logfile%
echo.                                                 >> %Logfile%

robocopy %Quelle% %Ziel% /MIR /R:3 /W:3 /TEE /LOG+:%Logfile%

net use x: /del

:Ende
pause
exit
```

Falls der Zugriff auf das Ziellaufwerk bereits existiert, kann der net use-Befehl entfallen. Der pause-Befehl ermöglicht es, in der Testphase das Skript zu überprüfen. Danach sollte der pause-Befehl entfernt werden.



### Errorlevel

Jedes Kommando gibt einen Errorlevel zurück, der in Skripten oder Batch-Programmen mit *%errorlevel%* oder mit *if errorlevel zahl* abgefragt werden kann.

| | |
|---|---|
| `if errorlevel 0` | gibt immer true zurück, wenn der errorlevel >= 0 ist. |
| `if errorlevel 1` | gibt immer true zurück, wenn der errorlevel >= 1 ist. |
| `if errorlevel 2` | gibt immer true zurück, wenn der errorlevel >= 2 ist. |

## Beispiel für ein Skript zur Datenarchivierung

Im Unterschied zur Datensicherung wird bei der Datenarchivierung eine vorhandene Sicherung nicht überschrieben. Es wird ein neues Zielverzeichnis angelegt, das auch das Datum (und ggf. die Uhrzeit) der Sicherung enthält.

```
@ECHO OFF

for /f "tokens=1 delims=." %%i in ('echo %date%') do set Tag=%%i
for /f "tokens=2 delims=." %%i in ('echo %date%') do set Monat=%%i
for /f "tokens=3 delims=." %%i in ('echo %date%') do set Jahr=%%i
for /f "tokens=1 delims=:" %%i in ('echo %time%') do set Stunde=%%i
for /f "tokens=2 delims=:" %%i in ('echo %time%') do set Minute=%%i

set Quelle=D:\Daten\
set Ziel=G:\Backup_Daten_%Jahr%_%Monat%_%Tag%\

robocopy %Quelle% %Ziel% /MIR
```

## Automatisieren eines Skriptes mit der Windows-Aufgabenplanung

Mit der Windows-Aufgabenplanung (Taskplaner) lassen sich Skripte zeitgesteuert ausführen. Vor dem Automatisieren muss das Skript so weit getestet werden, dass es ohne Benutzereingriffe läuft.

# LABORÜBUNG 15 - SICHERUNG VON DATEN EINES LINUX-SERVERS MIT RSYNC

Auf einem Linux-Server sollen die relevanten Daten (z. B. aus dem Verzeichnis „/home“) regelmäßig auf eine NAS-BOX gesichert werden.


## Aufgaben

1. Auf einem Linux-Server soll das Verzeichnis /home auf einer NAS-Box gesichert werden.

## Hinweise

Die Datensicherung unter Linux mit rsync ist ausführlich im Laborbuch Linux-Server beschrieben.

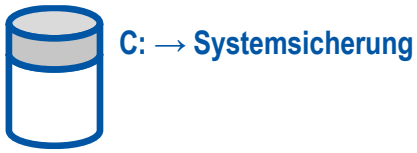
(http://alp.dillingen.de/schulnetz/materialien/Laborbuch_Linux_Server.pdf)

## Ihre Notizen

# LABORÜBUNG 16 - BACKUP EINES WINDOWS-COMPUTERS MIT DRIVE SNAPSHOT

## Szenario

Auf einem Windows-Computer oder einem Windows-Server soll eine vollständige Partition (System- oder Datenpartition) gesichert werden.




## Vorbereitung

- Drive Snapshot (aktuelle Testversion)
- Ggf. Aufteilung des Windows-Computers in mehrere Partitionen (Systempartition, Datenpartition, Ablagepartition)

## Aufgaben

1. Kopieren Sie die Imaging-Software Drive Snapshot auf Ihren PC und erstellen Sie damit ein Backup (Image) der Windows-Partition oder einer Datenpartition. Speichern Sie das Backup auf der Ablagepartition oder im Netz auf einer NAS-Box.
2. Binden Sie das erstellte Image als Laufwerk ein und greifen Sie auf einzelne Dateien zu.

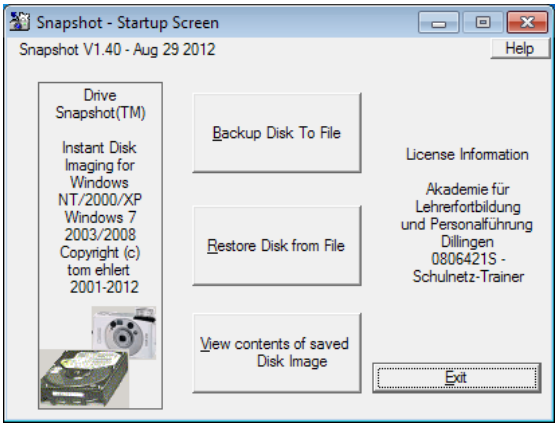
## Weiterführende Aufgaben

3. Führen Sie das Programm Drive Snapshot auf Kommandozeile aus und erstellen Sie damit inkrementelle Sicherungen.
4. Automatisieren Sie die Datensicherung, so dass diese automatisch einmal am Tag (in der Testphase häufiger) durchgeführt wird.
5. Spielen Sie die Daten- oder Systemsicherung wieder zurück und überschreiben Sie dazu ihr aktuelles System mit der Datensicherung.

# HINWEISE

## Drive Snapshot

Drive Snapshot fertigt Images von System- oder Datenpartitionen an.




## Systemsicherung

Das beschriebene Vorgehen eignet sich auch für die Systemsicherung und Systemwiederherstellung eines einzelnen Computers.

Drive Snapshot erlaubt (wie alle aktuellen Imaging-Programme) das Sichern der Windows-Partition aus dem laufenden Windows-Betriebssystem. Auch das Zurückspielen funktioniert aus dem laufenden System heraus.

Sollte Windows nicht mehr lauffähig sein oder wurden Einstellungen im Bootmanager verändert, ist es notwendig, Drive Snapshot aus einem Live-System (WinPE) zu starten und ggf. den Bootmanager zu restaurieren.

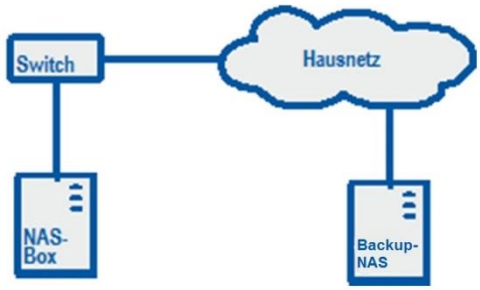
Details dazu sind unter http://alp.dillingen.de/schulnetz/materialien veröffentlicht.

# LABORÜBUNG 17 - SICHERUNG VON DATEN EINER NAS-BOX AUF EINE BACKUP-NAS

Viele NAS-Boxen unterstützen eine komfortable Backup-Funktion (NAS to NAS) zwischen NAS-Boxen des gleichen Herstellers.

## Szenario

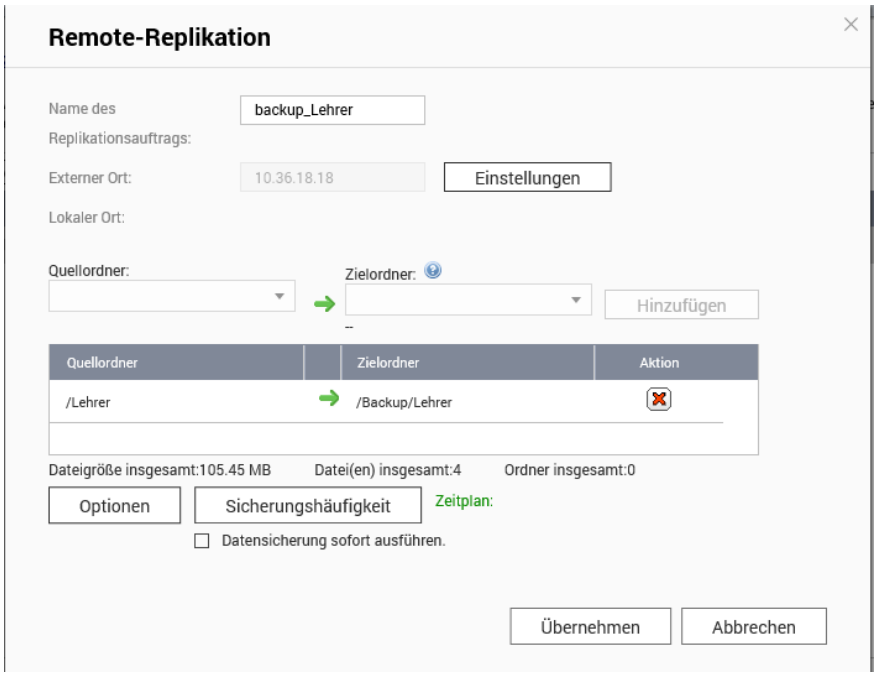
Auf einem NAS gibt es die Freigabe Lehrer. Der Inhalt dieser Freigabe soll täglich auf ein Backup-NAS in der Schule gesichert werden.




## Aufgaben

1. Richten Sie auf einem NAS die Freigabe Lehrer und auf dem Backup-NAS die Freigabe Backup und das Unterverzeichnis Lehrer ein.
1. Richten Sie auf der NAS-Box die NAS zu NAS Sicherung ein: Geben Sie unter externer Ort das Backup-NAS (IP-Adresse, Benutzername, Passwort) ein und wählen sie die Quell- und die Zielordner aus.
2. Konfigurieren Sie die Sicherungshäufigkeit und die Optionen (nur Dateien kopieren, die sich unterscheiden; Zusatzdateien löschen). Zum Testen kann man den Auftrag sofort ausführen.
3. Einige Sicherungen sollen archiviert werden. Benennen Sie zur Datenarchivierung den Zielordner Backup/Lehrer um (z.B. in Backup\Lehrer_2016_12_24) Überprüfen Sie, ob bei der nächsten Sicherung der Ordner Backup\Lehrer erneut angelegt wird.

# HINWEISE


Remote-Replikation
Name des Replikationsauftrags:
backup_Lehrer
Externer Ort:
10.36.18.18
Einstellungen
Lokaler Ort:
Quellordner:
Zielordner:
Hinzufügen
Quellordner
Zielordner
Aktion
/Lehrer
/Backup/Lehrer
Dateigröße insgesamt:105.45 MB
Datei(en) insgesamt:4
Ordner insgesamt:0
Optionen
Sicherungshäufigkeit
Zeitplan:
Datensicherung sofort ausführen.
Übernehmen
Abbrechen