AKADEMIE FÜR LEHRERFORTBILDUNG UND
PERSONALFÜHRUNG
DILLINGEN

SCHULNETZ

Qualifizierung von Systembetreuerinnen
und Systembetreuern

Basiskurs II

Medieneinsatz und Datensicherheit

– Laborübungen –

IMPRESSUM

Die Schulungsunterlagen wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren und Beratern digitale Bildung erarbeitet. Die Schulungsunterlagen sind unter der Adresse https://alp.dillingen.de/schulnetz/materialien abrufbar.

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6-7
89407 Dillingen

Dokumentation: Peter Botzenhart, Akademie Dillingen
Kurt Windberger, Gymnasium Zwiesel
Susanne Schaffer, Realschule Kulmbach
Wolf Gebele, Realschule Gemünden
Claudia Morack, Realschule Schonungen
Jürgen Knahn, Mittelschule Sulzbach-Rosenberg

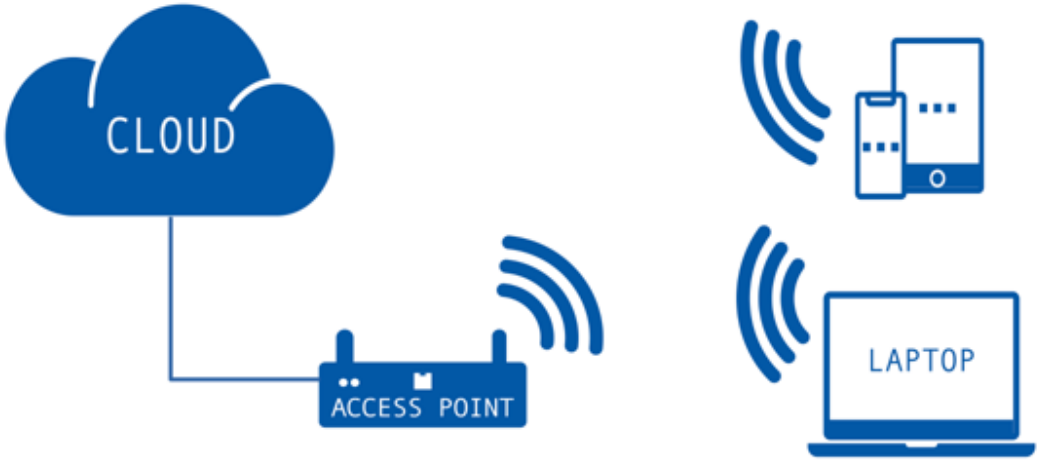
URL: https://schulnetz.alp.dillingen.de/
Mail: p.botzenhart@alp.dillingen.de
Stand: April 2023

INHALT

LABORÜBUNG 01 - DRAHTLOSES BEREITSTELLEN VON DATEIEN

Szenario

Ein Lehrer möchte seinen Schülern Dateien drahtlos zur Verfügung stellen. Er möchte kein installierbares Programm oder eine App zu verwenden.



Aufgaben

1. Erkunden Sie, welche Möglichkeiten es zur drahtlosen Dateibereitstellungen für die verschiedenen Betriebssysteme gibt. Arbeiten Sie die Unterschiede heraus.
2. Geben Sie für die verschiedenen Geräte eine Datei frei.

Hinweise

Alle Betriebssysteme haben inzwischen Möglichkeiten zur drahtlosen Dateifreigabe standardmäßig integriert. Die Techniken setzten aktiviertes Bluetooth und WLAN voraus.

HINWEISE

Verschiedene Möglichkeiten zur drahtlosen Dateibereitstellung

MacOS, iOS und iPadOS

Um Daten zwischen Apple-Geräten zu übertragen, kann das integrierte AirDrop verwendet werden.

Windows 10/11

Windows 10/11 bietet seit einiger Zeit ebenfalls die Möglichkeit zur drahtlosen Dateiübertragung per Umgebungsfreigabe über WLAN oder Bluetooth.

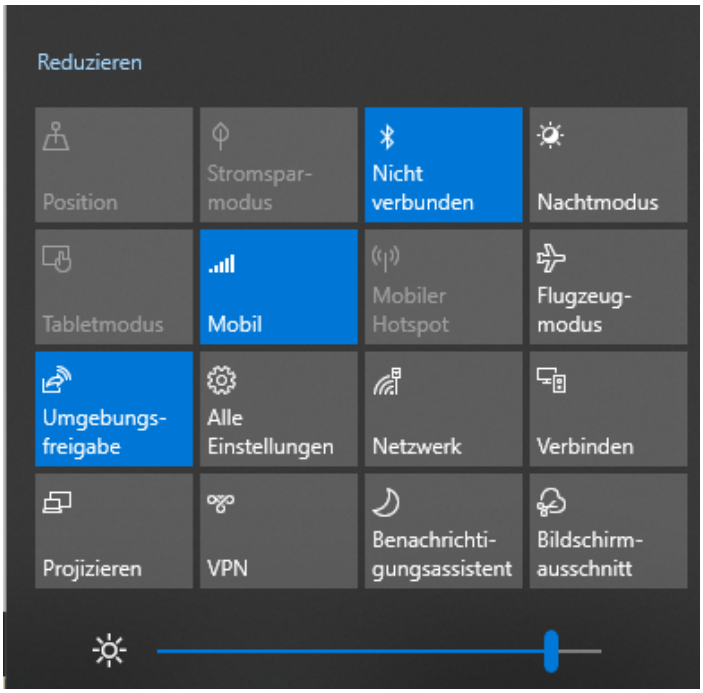
Android

Google hat Nearby Share in sein Betriebssystem Android (ab Version 6) integriert. Nearby Share befindet sich im Teilen-Menü.

Snapdrop.net

Die Webseite im Design des Apple Air Drop Interfaces bietet die Möglichkeit der drahtlosen Dateiübertragung über Betriebssystemgrenzen hinweg. So können z. B. Daten von einem iPad drahtlos auf ein Windowsgerät übertragen werden.

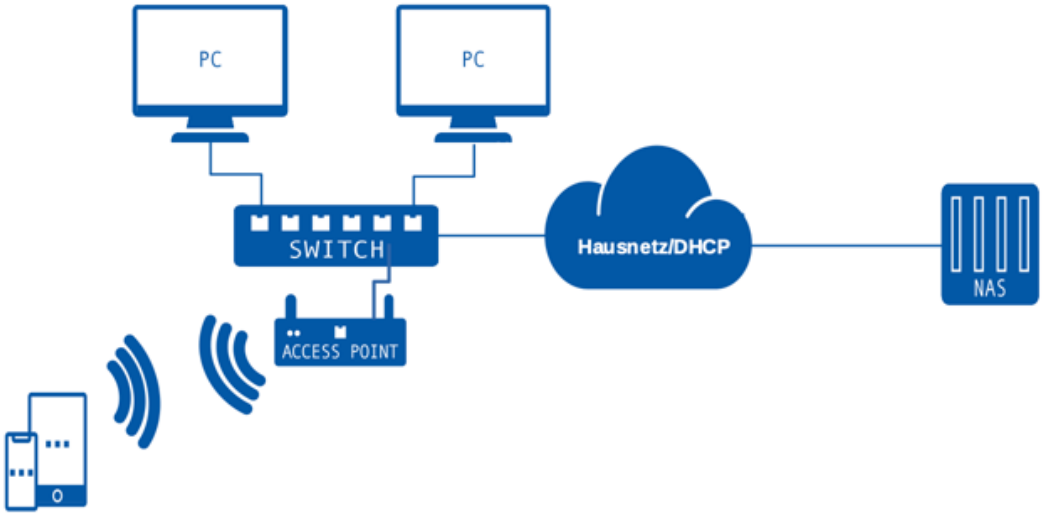
Zugriff auf die Umgebungsfreigabe unter Windows 10



LABORÜBUNG 02 - EINRICHTEN EINES DATENSPEICHERS AUF EINEM NAS-SYSTEM

Szenario

Auf einem NAS-System 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. Verwenden Sie *QNAP Finder* bzw. *Synology Assistant* zum Entdecken Ihrer NAS im lokalen Netzwerk.
2. Erstellen Sie auf dem NAS-System 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 Smartphone den Zugriff auf das NAS-System. Verwenden Sie dazu geeignete Apps.

6. Erstellen Sie ein Foto mit dem Smartphone und speichern Sie dieses auf dem NAS-System ab.

Dateiserver und NAS-Boxen

Lokale Dateiserver (Windows-Server bzw. Linux-Server mit SMB Freigaben) 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 laufen den klassischen Dateiservern immer mehr den Rang ab. Sie sind für große Datenmengen konzipiert und relativ einfach einzurichten.

Berechtigungen

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

- Leserechte
- Lese- und Schreibrechte
- keine Zugriffsrechte

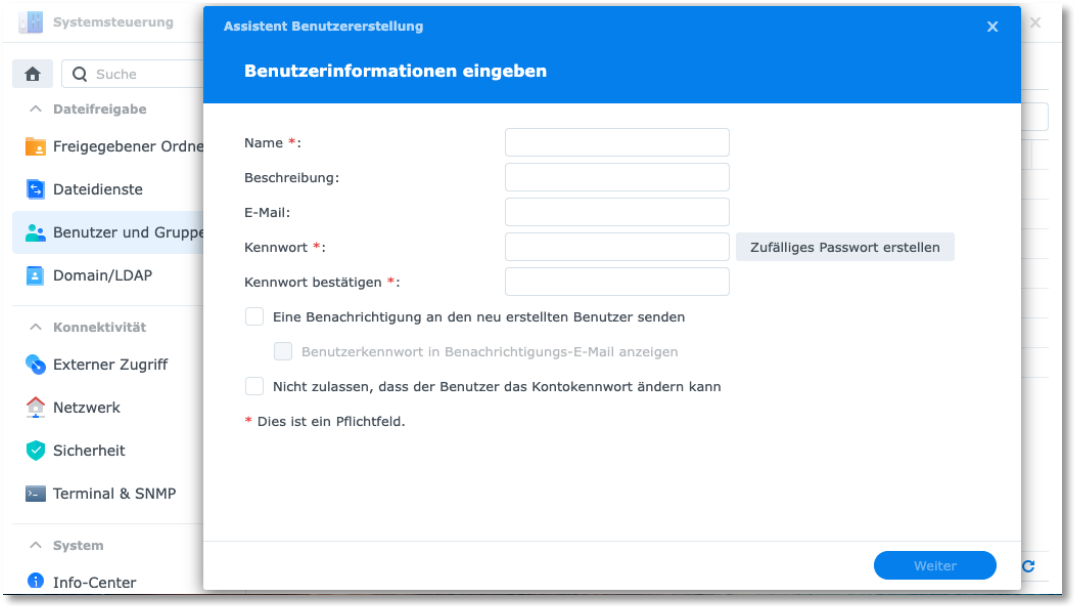
Die Berechtigungen sollten sehr sorgfältig gesetzt werden. Ein Virus oder Verschlüsselungstrojaner kann z. B. nur dort Schaden anrichten, wo er auch Schreibrechte hat.

Ihre Notizen

HINWEISE

Einrichten von Freigaben auf einem NAS-System

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

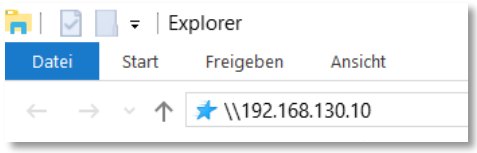


Zugriff auf ein NAS-System mit Smartphones

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

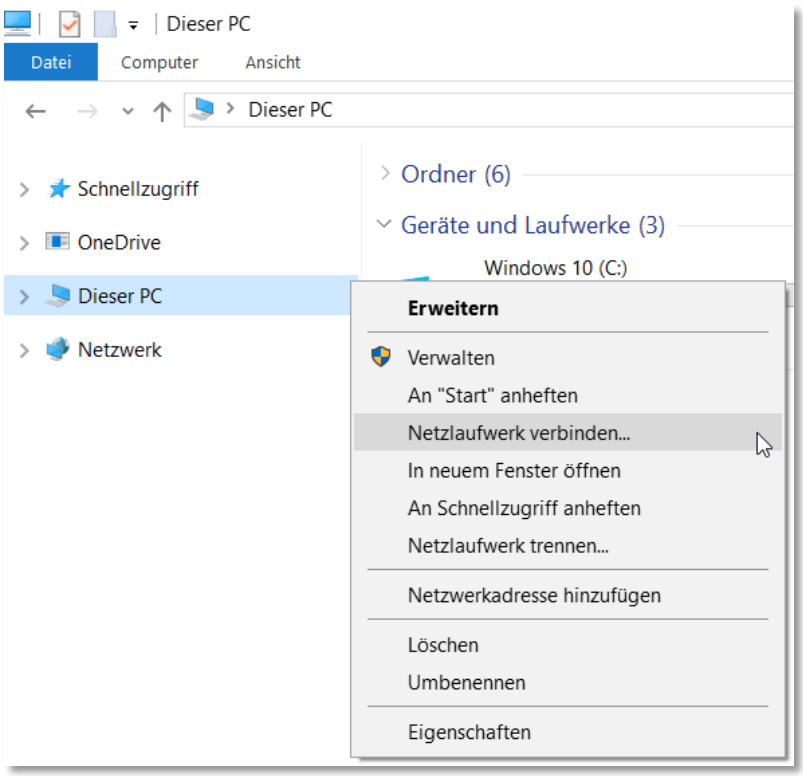
Zugriffe auf SMB-Freigaben unter Windows

Adresszeile im Windows-Explorer



Netzlaufwerk verbinden im Windows-Explorer

Dieser PC - rechter Mausklick - Netzlaufwerk verbinden.



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:Lehrer
```

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

```
net use X: \\192.168.130.10\Daten /user:Lehrer 12345
```

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

Trennen von SMB-Verbindungen

SMB-Verbindungen sind oft 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. Grundsätzlich kann man sich an einem Server mit SMB Freigaben nur unter einem Benutzerkontext anmelden.

Windows-Explorer

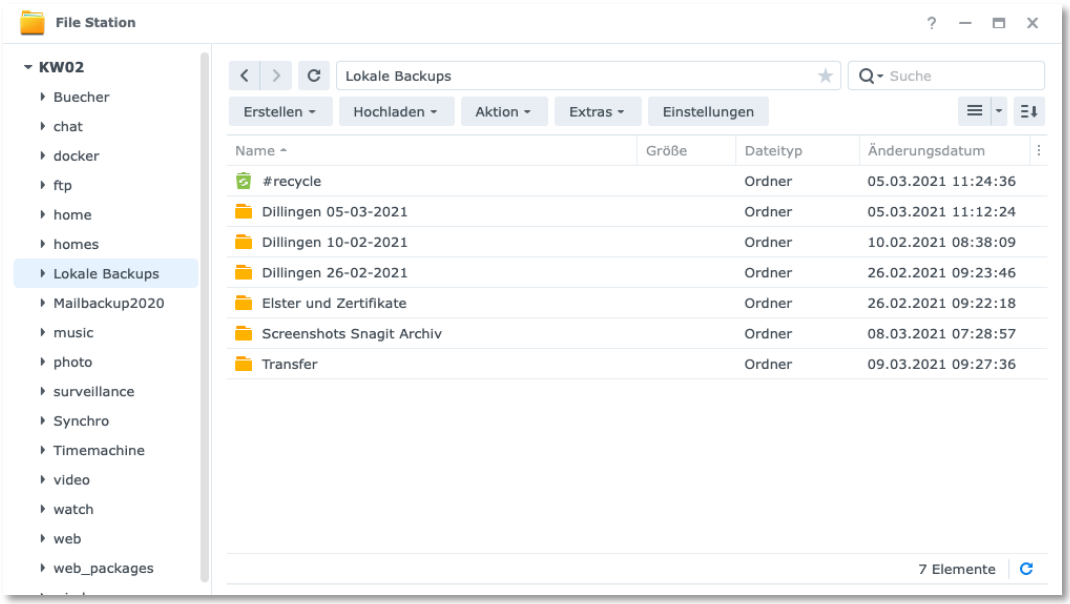
Extras – Netzlaufwerk trennen

Kommandozeile

`net use Laufwerk: /delete`

`net use X: /delete`	Das Netzlaufwerk X: wird getrennt
`net use * /delete`	Alle Netzlaufwerke werden getrennt

Web-Zugriff auf die Freigaben eines NAS-Systems

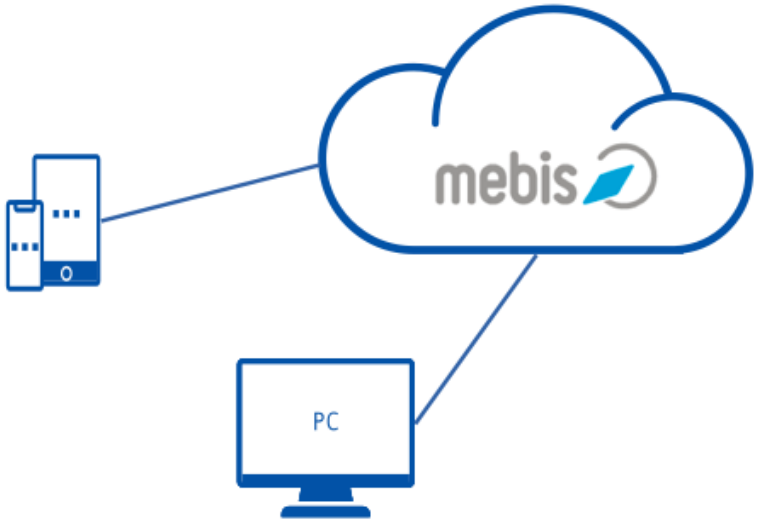


LABORÜBUNG 03 - DATENSPEICHER AUF MEBIS

Szenario

Sie möchten die **mebis** Lernplattform als Teil der BayernCloud Schule als persönlichen Cloud-Speicher nutzen.

Zusätzlich soll für die Lehrkräfte Ihrer Fachschaft ein gemeinsamer Dateipool für Arbeitsblätter entstehen. Jede Lehrkraft soll darin Schreibrechte haben.



Aufgaben

1. Loggen Sie sich in die mebis Lernplattform ein. Legen Sie unter „Meine Dateien“ Ordner an und laden Sie 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.

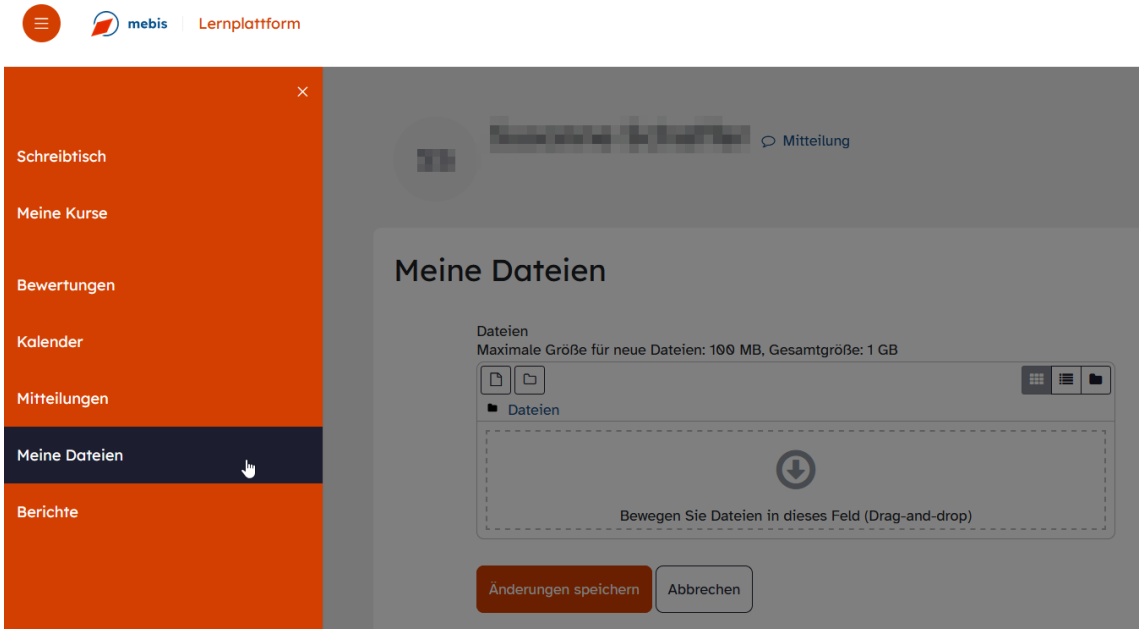
HINWEISE

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 bei einer maximalen Dateigröße von 100 MB.

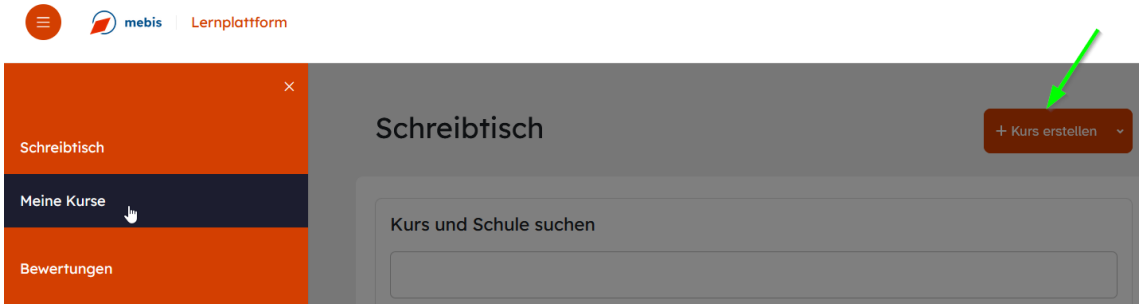


Nach dem Erstellen von Verzeichnissen oder dem Hochladen von Dateien müssen die Änderungen immer gespeichert werden.

Datenschutzrechtlich gibt es gegen die „mebis-Cloud“ keine Einwände; es dürfen auch sensible Dateien abgelegt werden. Die hier abgelegten Dateien können später sehr leicht in mebis-Kurse integriert werden.

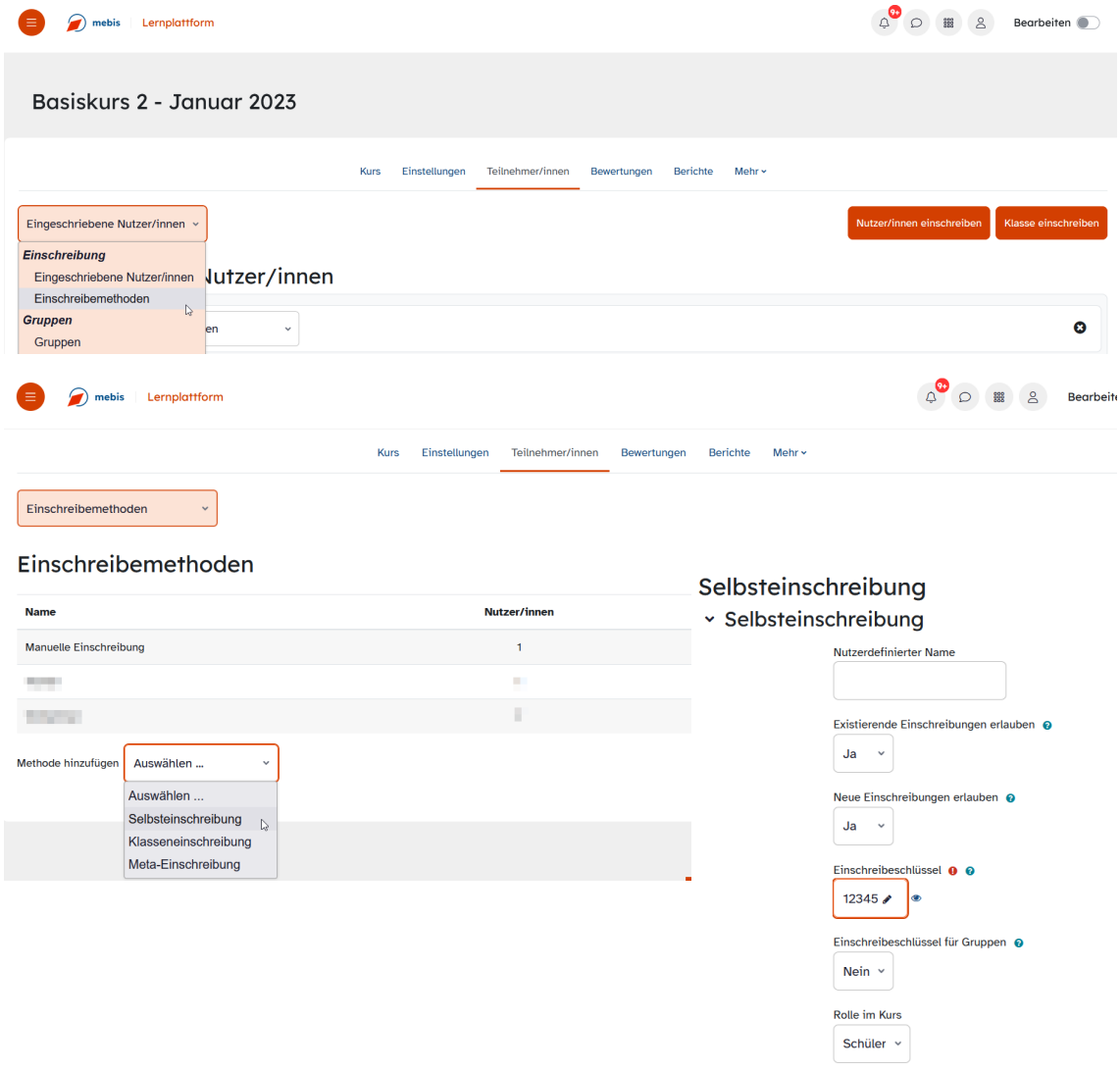
mebis – Kurs erstellen

mebis – Lernplattform – Schreibtisch – Kurs erstellen

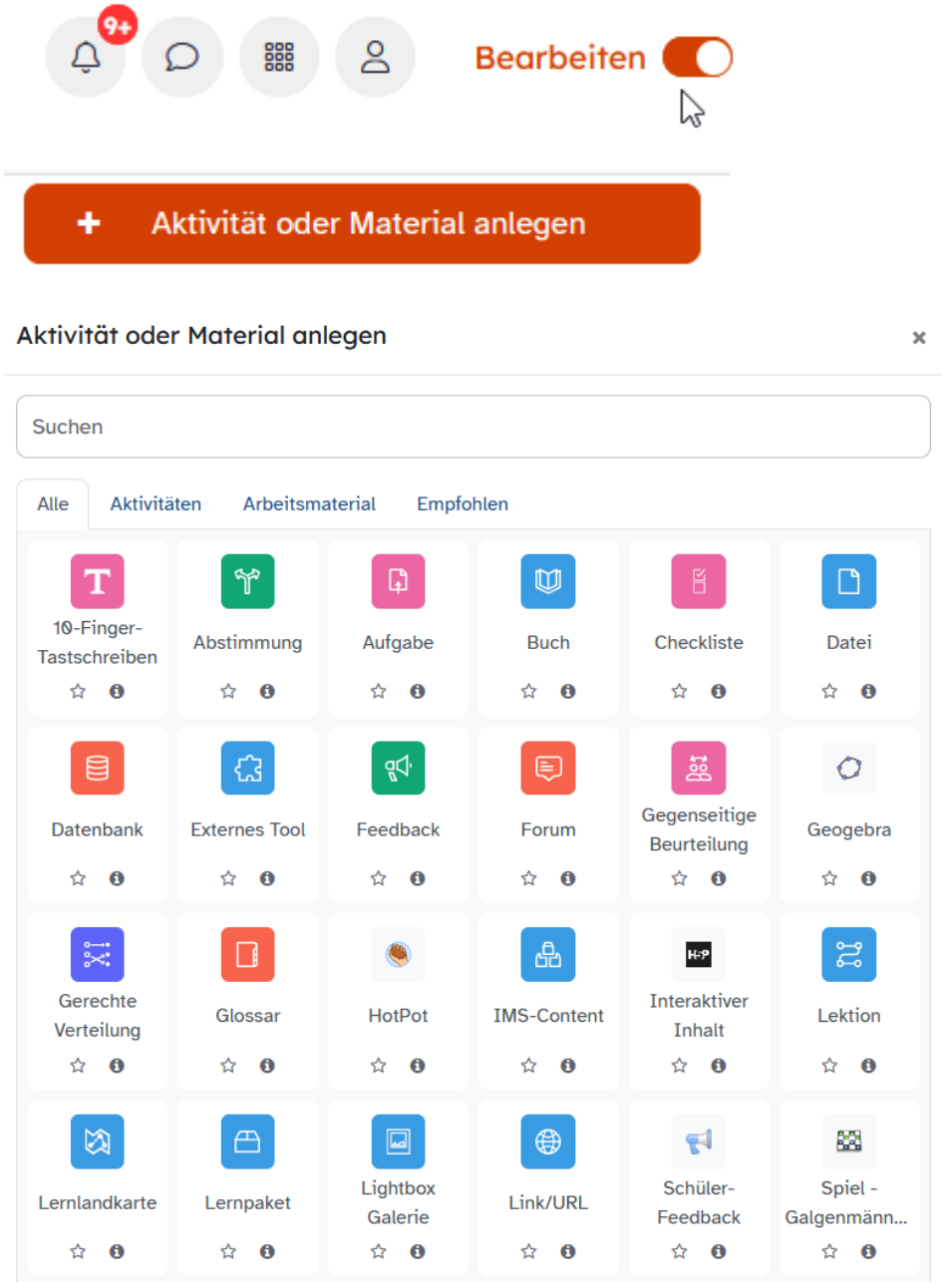


mebis – Selbsteinschreibung aktivieren

Einschreibeschlüssel festlegen und Rolle der neuen Nutzer definieren



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



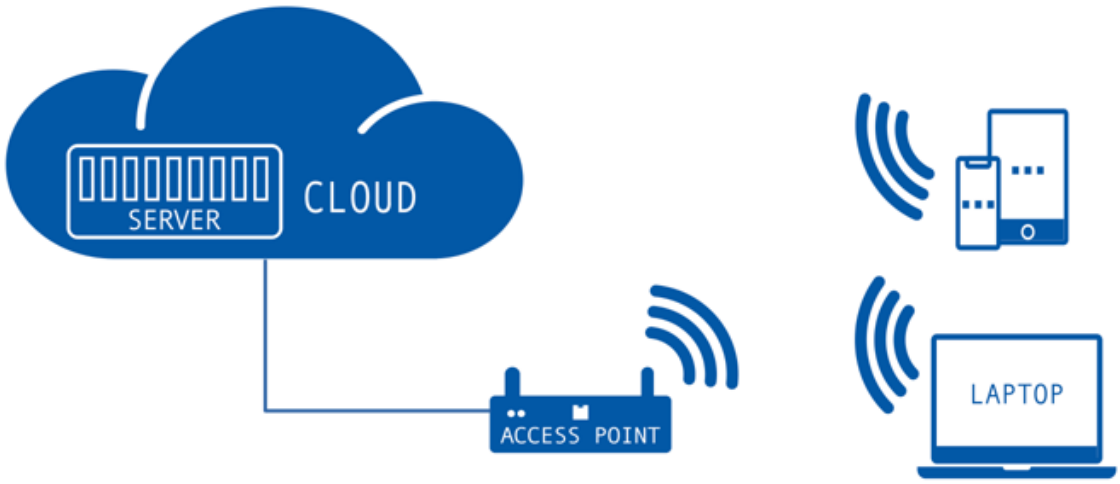
MEDIATHEK

In der mebis-Mediathek finden sich viele frei zugängliche Videos. Zudem findet sich unter https://mundo.schule die offene Bildungsmediathek der Länder.

LABORÜBUNG 04 - DATEN AUF EINEM CLOUD-SPEICHER

Szenario

Eine Lehrkraft hat bei einem Cloud-Anbieter einen Online-Speicher erworben und möchte diesen für ihre Unterrichtsvorbereitung (Arbeitsblätter, Musterlösungen) nutzen.



Aufgaben

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

Urlaubsfotos über die Cloud bereitstellen

2. Fertigen Sie mit Ihrem Smartphone einige Fotos an. Laden Sie die Fotos in einen Ordner „Urlaubsfotos“ in den Datenspeicher Ihrer Cloudlösung 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

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

GoogleDrive – wird automatisch innerhalb des Google Workspace beim Anlegen eines Google Kontos erstellt.

OneDrive – wird als Installationsoption beim Erstellen eines privaten Microsoft Kontos angeboten. OneDrive integriert sich in den Windows Datei Explorer.

MagentaCloud – Cloudlösung der Telekom mit Serverstandort in Deutschland

iCloud Drive – wird automatisch mit der Erstellung einer Apple ID zur Verfügung gestellt.

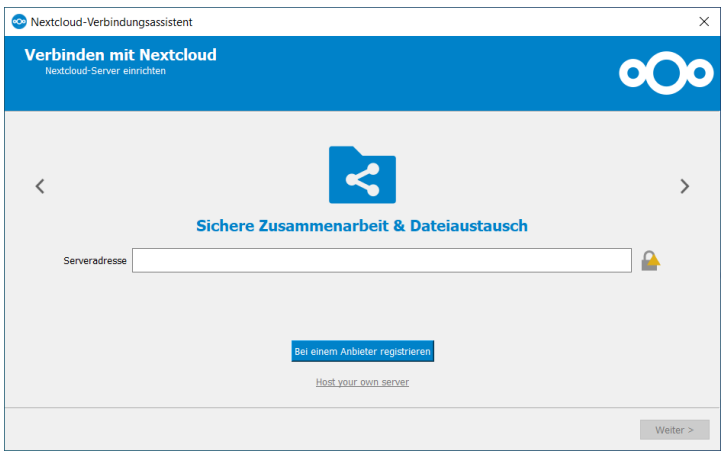
ownCloud bzw. **Nextcloud** – Open-Source-Lösungen, um eine eigene Cloudlösung aufzusetzen. Der Zugriff erfolgt dann webbasiert oder über einen entsprechenden Client.

Strato Hi Drive – Onlinespeicher mit professionellen Optionen (z.B. automatisierten Backup) und Serverstandort Deutschland.

Dropbox – gut skalierende Cloudspeicherlösung mit umfangreichen Optionen für Teams oder Einzelpersonen. Es kann ein entsprechender Client lokal für den Zugriff installiert werden.

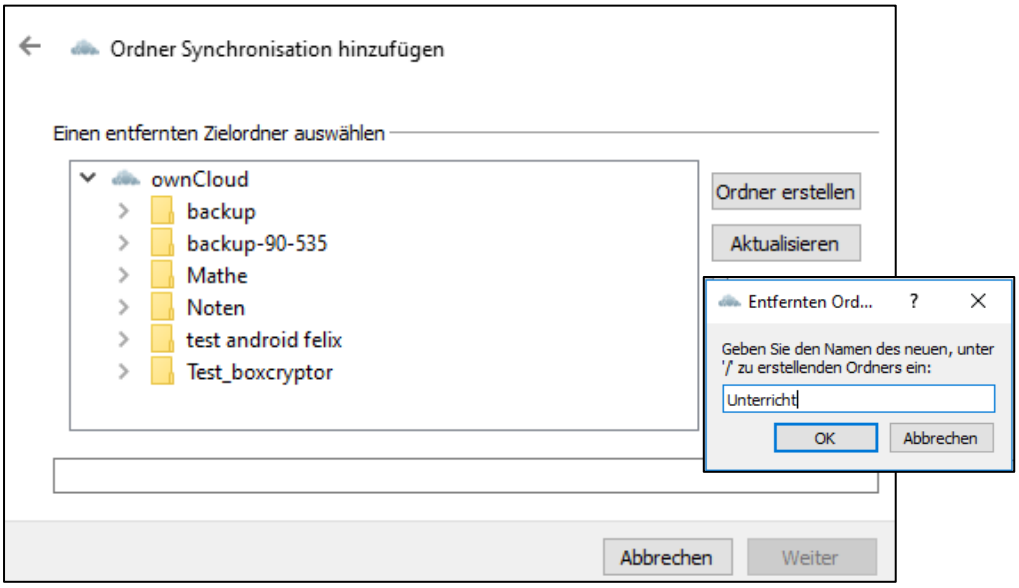
Installation eines Clients

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

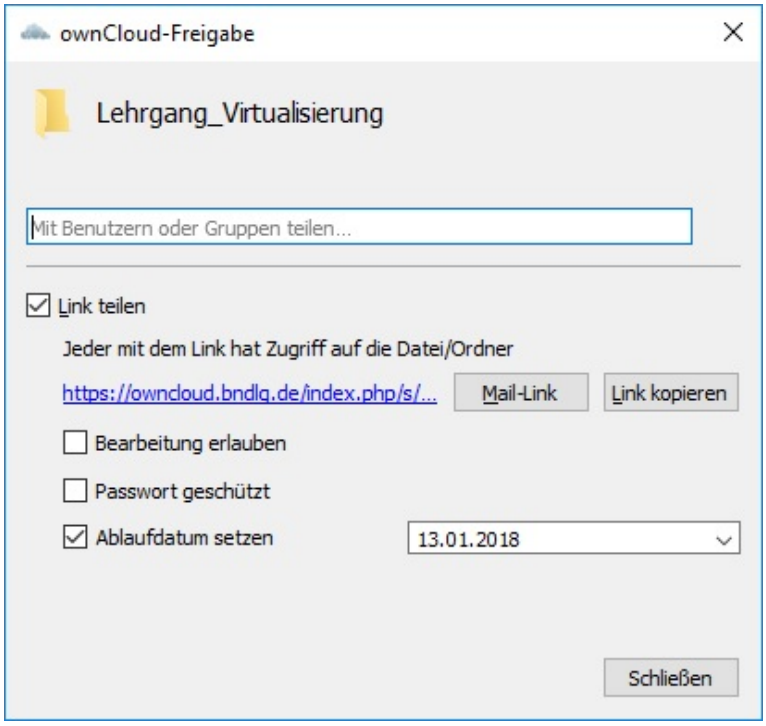


Hinzufügen eines Ordners zur Synchronisation

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.

DATENSICHERHEIT UND IT-GRUNDSCHUTZ

Viele nützliche Dienstleistungen wie Online-Banking, E-Commerce oder Clouddienste werden heute über das Internet angeboten und genutzt. Dieser Trend wird sich in der Zukunft noch verstärken und die Schulen zunehmend erfassen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones oder Tablets, mit denen diese Dienste auch unterwegs genutzt werden können.

Aus den genannten Gründen sollte man sich verstärkt über den Schutz der Geräte gegen Schadenspotentiale aus dem Internet kümmern. Im schulischen Umfeld wird das Netzwerk in der Regel über eine Firewall für geschützt. Heimische Router verfügen ebenfalls über eine Firewall. Allerdings sollten auch die Schutzmöglichkeiten der Clients in das Konzept der Schule einbezogen werden.

Jeder Benutzer muss sich über einige grundsätzlichen Fragestellungen klarwerden, wie z. B.

- Welchen Gefahren setze ich mich aus, wenn ich einen Internetzugang benutze?
- Wie kann ich einen Grundschutz gegen Angriffe aus dem Internet realisieren?
- Wie kann ich meine persönlichen Daten sichern, um sie bei einem Schadensfall nicht zu verlieren?

Hinweise zur Geräteabsicherung

VIRENSCHUTZPROGRAMM UND DESKTOPFIREWALL

Beide stellen einen Basisschutz gegen bereits bekannte Schadsoftware und gegen möglicherweise unerwünschte Anwendungen dar. Im Funktionsumfang von Windows 10 ist bereits mit Windows Defender ein ausreichend wirksamer Virenschutz enthalten.

Auf einen zusätzlichen Virenschutz kann verzichtet werden. Der Windows Defender ist automatisch aktiviert, sofern kein anderer Virenwächter auf dem PC installiert wird. Zudem bietet das Windows Sicherheitscenter eine Client-Firewall und eine App- und Browsersteuerung.

In MacOS ist ebenfalls eine Firewall und ein Virenscanner integriert und standardmäßig aktiviert.

Betriebssysteme von mobilen Endgeräten verfügen über interne Schutzmaßnahmen, die regelmäßig nach Schadsoftware auf dem Gerät suchen. Sofern nur Apps aus den bekannten Appstores geladen werden, sind diese Schutzmaßnahmen als ausreichend anzusehen.

SOFTWARE

Angreifer nutzen gerne Schwachstellen verbreiteter Software aus. Dabei gilt, dass jede zusätzliche Software ein mögliches Sicherheitsrisiko bildet. Aus diesem Grund sollten Updates für das Betriebssystem und die installierte Software möglichst zeitnah eingespielt werden.

Zentrale Angriffspunkte bilden, neben dem Betriebssystem, der E-Mail-Client und der Browser. Hier sollte unbedingt darauf geachtet werden, stets aktuelle Versionen verwendet werden.

Auf mobilen Endgeräten sollte Software ausschließlich aus den offiziellen App-Stores bezogen werden oder per MDM zentral auf die schuleigenen Geräte verteilt werden.

BENUTZERKONTEN

Schadprogramme haben die gleichen Rechte auf dem Endgerät wie das Benutzerkonto, über das sie auf den Rechner gelangen. Daher sollten normale Benutzer über keinerlei Administratorenrechte verfügen. Im Administratorkontext sollte nur gearbeitet werden, wenn dies unbedingt erforderlich ist.

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. Der administrative Aufwand bei Vorliegen defekter Hardware kann sehr hoch sein. (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

- Festplatteneinsatz im RAID-Verbund
- Erneuerung der Hardware nach spätestens 3 bis 5 Jahren
- Geeigneter Standort der zentralen Geräte (Temperatur, Staubbelastung)
- Überwachung (Monitoring) der Server bzw. zentralen Geräte

Ransomware (Verschlüsselungstrojaner)

Verschlüsselungstrojaner verschlüsseln lokale Daten. Für die mögliche Entschlüsselung der Daten muss der Betroffene im Voraus bezahlen, wobei keineswegs sichergestellt ist, dass die Entschlüsselung überhaupt funktioniert. Der Emotet Schädling hat beispielsweise u. a. eine Universität in Hessen lahmgelegt.

Der übliche Verbreitungsweg für Verschlüsselungstrojaner sind E-Mail-Anhänge. Wenn ein solcher Anhang (z. B. ausführbare exe-Datei, Office-Dokument mit Makros) ausgeführt wird, aktiviert sich der Trojaner. 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.
- Niemand arbeitet mit Administratorberechtigung, sondern als normaler Benutzer.
- Jeder Benutzer hat nur dort Schreibrechte, wo er sie wirklich benötigt.
- Die Programmausführung kann auf bestimmte Verzeichnisse beschränkt werden.

Bei der Datensicherung muss man darauf achten, dass der Verschlüsselungstrojaner keinen Zugriff auf die Datenträger hat, auf denen die Sicherung gespeichert ist.

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

Diebstahl von Hardware

Werden Geräte gestohlen, sind auch die Daten auf dem Gerät (Dateien, Kontakte, Passwörter, Bilder, Videos, ...) verloren.

Die Vorbeugung muss hier in verschiedene Richtungen gehen:

- Physikalischer Schutz der zentralen Komponenten einer Schule (Serverraum)

- Evtl. hardwareverschlüsselte Datensicherung an unterschiedlichen Orten
- Verschlüsselung der Daten auf Geräten, bei denen Diebstahl eine reale Gefahr darstellt (z. B. Notebook mit vertraulichen Daten, NAS-Systeme zur Datensicherung, USB-Stick mit vertraulichen Daten)

Katastrophen

Bei größeren Schadensereignissen (Brand, Blitzschlag, Überschwemmung, Gasexplosion) können gespeicherte Daten, Datensicherungen und auch ganze Netzwerke betroffen sein.

USV-Anlagen bieten einen gewissen Schutz gegen Blitzschläge.

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, 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 cloudbasierte Backup-Lösungen angeboten, die als Ergänzung für eine Datensicherung innerhalb der Schule sinnvoll sein können. Dabei sind die datenschutzrechtlichen Bestimmungen und auf eine ausreichende Bandbreite des Internetanschlusses zu achten. Hier sollte darauf geachtet werden, dass nachdem Backup nur noch Änderungen des Datenbestandes in die Cloud gesichert werden.

Bei der Datenarchivierung muss vor allem auf die Langlebigkeit der verwendeten Technik und der Medien geachtet werden. Hier bieten sich auch noch CD- oder DVD-ROMs an, da sie eine längere Lebenszeit haben als externe Festplatte.

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 Sicherungskonzept 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.). Unter Windows 10 kann ein Systemabbild über die Systemsteuerung erstellt werden. Im Gegensatz zu Wiederherstellungspunkten speichert ein Systemabbild Ihre Windows-Festplatte 1:1 mit Betriebssystem und allen dazugehörigen Einstellungen. 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 wiedereingerichtet 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).

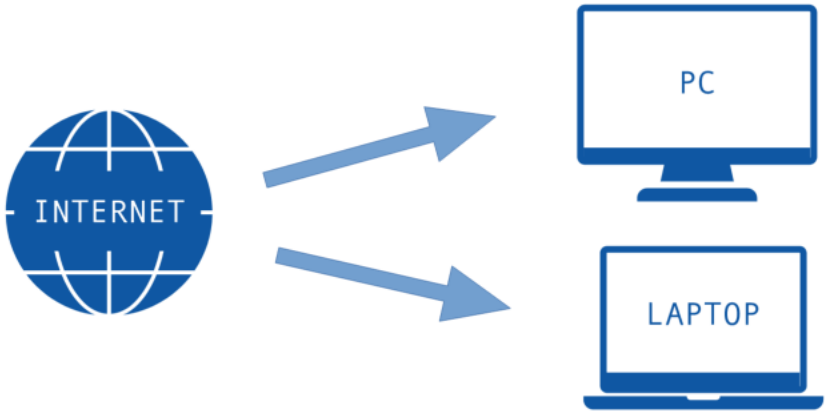
Automatisierung der Datensicherung

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 05 - ABSICHERN EINES WINDOWS 10/11 PC

Szenario

Sie erhalten von Ihrem Arbeitgeber einen neuen Dienst-PC und sollen diesen nun gegen Angriffe aus dem Internet absichern.



Aufgaben

1. Überprüfen Sie, ob für Ihren Rechner Windows Updates zu installieren sind.
2. Kontrollieren Sie, ob im Windows-Sicherheitsbereich der Windows-Defender und die Firewall aktiviert sind.
3. Aktivieren Sie den Zugriffsschutz auf Ihren Rechner mit der Tastenkombination Windows + L. Stellen Sie zudem ein, dass sich der Windows Desktop bei Inaktivität automatisch nach einer gewissen Zeit gesperrt wird.
4. Sorgen Sie dafür, dass nicht mehr Diagnosedaten an Microsoft übermittelt werden als notwendig.
5. Führen Sie einen manuell angepassten Virenscan durch. Stellen Sie hierzu sicher, dass die aktuellen Virendefinitionen installiert sind.

Weiterführende Übungen

6. Passen Sie die Optionen des *Zuverlässigkeitsbasierter Schutz* an.
7. Informieren Sie sich zu den Familienoptionen in Windows.
8. Aktivieren Sie das isolierte Browsen im Edge-Browser. Installieren Sie hierzu den Microsoft Defender Application Guard.

Ihre Notizen

LABORÜBUNG 06 - BROWSER ABSICHERN

Szenario

Sie wollen Ihren Browser auf Ihrem mobilen Endgerät gegen Gefahren aus dem Internet absichern.

Aufgaben

1. Vergewissern Sie sich, dass für Ihren Browser (z. B. Chrome, Firefox) alle Updates installiert sind.
2. Wählen Sie die datenschutzfreundlichsten und sichersten Optionen bei Ihrem Browser aus!

Hinweise

Heutzutage werden viele Anwendungen im Browser ausgeführt und er bildet eine der zentralen Arbeitsanwendungen im Schulumfeld. Deswegen muss bei der Absicherung eines Endgeräts besondere Aufmerksamkeit hierauf gelegt werden.

Zudem möchten Werbeanbieter möglichst zielgenaue Werbung für den Endnutzer ausspielen, weswegen sie auf Tracking und Fingerprinting zur Analyse des Surfverhaltens des Nutzers nutzen. Dazu werden u. a. auch Cookies (kleine Textdateien) genutzt, die auf dem lokalen Computer gespeichert werden und beim erneuten Ansurfen der Webseite ausgelesen werden. Cookies werden aber auch beispielsweise zum Speichern von Anmeldedaten genutzt.

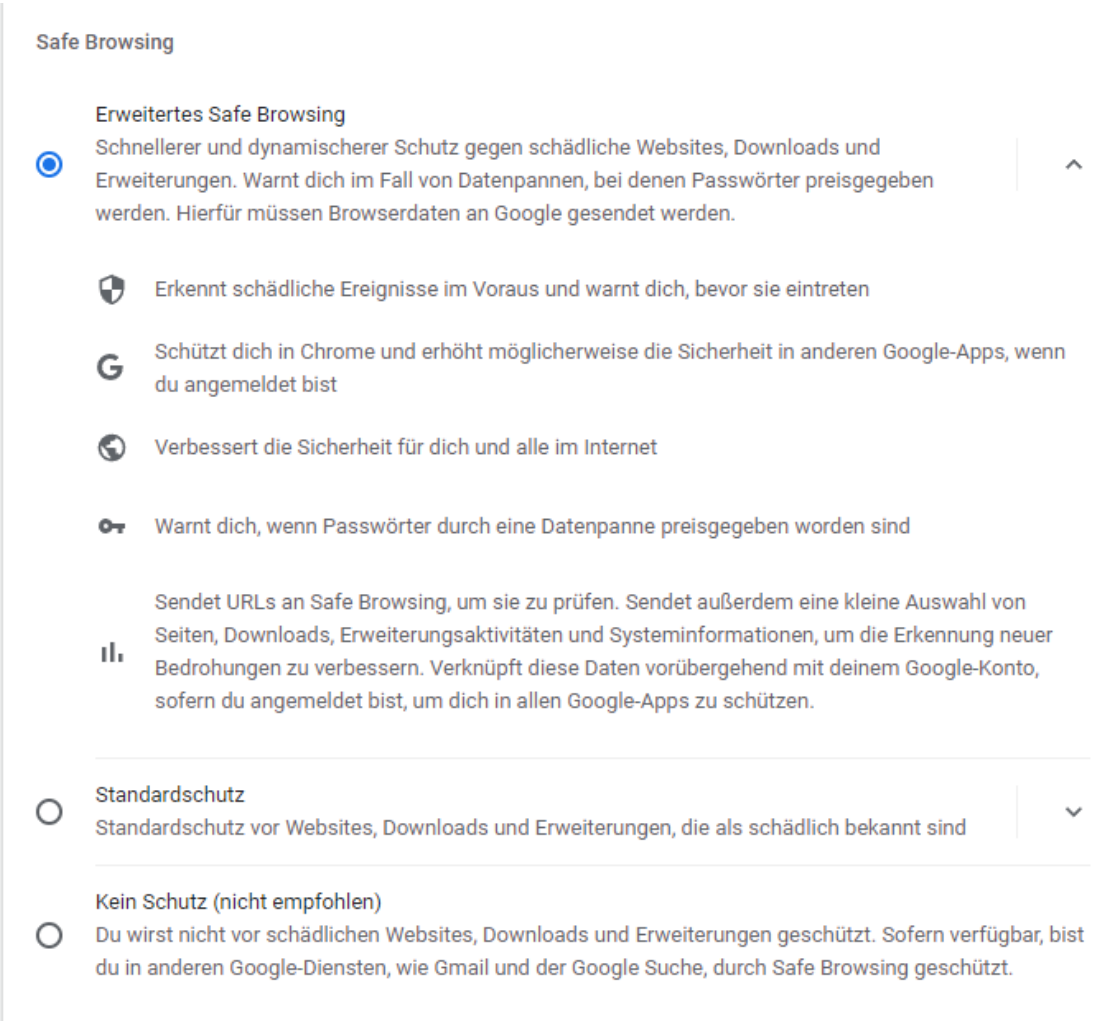
Mögliche Gegenmaßnahmen gegen Tracking sind die Installation von Addons, wie z. B. uBlock Origin oder Adblock Plus im Browser. Das Nachladen extern gehosteter Websites-Komponenten verhindert die Erweiterung Decentraleyes.

Browser bieten i. d. R. die Möglichkeit eines Private bzw. Inkognito Modus an. Dabei werden keine Daten (z. B. Cookies oder Browserverläufe) auf dem Computer gespeichert. Dies bietet sich vor allem an Geräten an, die von verschiedenen Personen genutzt werden. Der Modus bietet keinen Schutz vor Tracking durch Werbetreibende im Internet.

Chrome

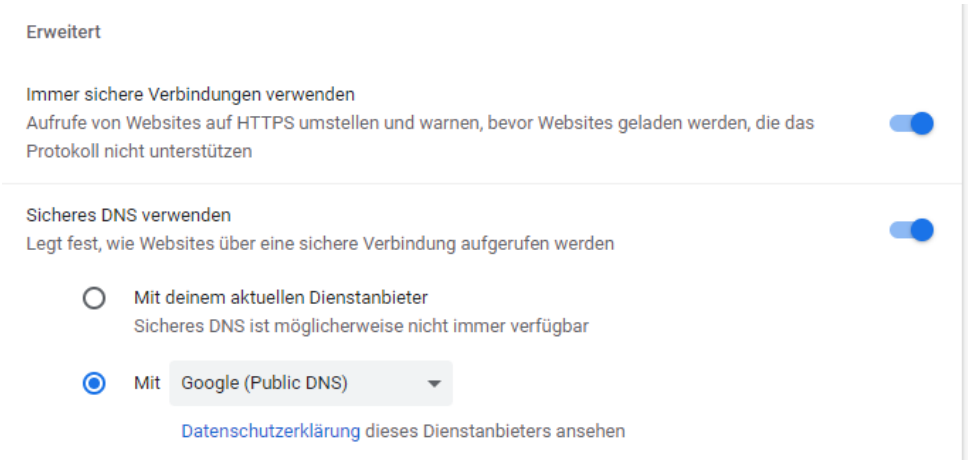
In den Browser-Einstellungen sollten alle Optionen unter *Google und ich* deaktiviert sein. Dadurch wird verhindert, dass sich Chrome automatisch mit dem eigenen Google-Konto verknüpft, sobald man sich damit auf einer Google-Seite einloggt.

Unter *Datenschutz und Sicherheit/Sicherheit* kann man die Standardeinstellungen aktiv lassen oder für sicheres Browsen die höhere Stufe auswählen. Allerdings werden dann URLs zur Überprüfung an Google geschickt.

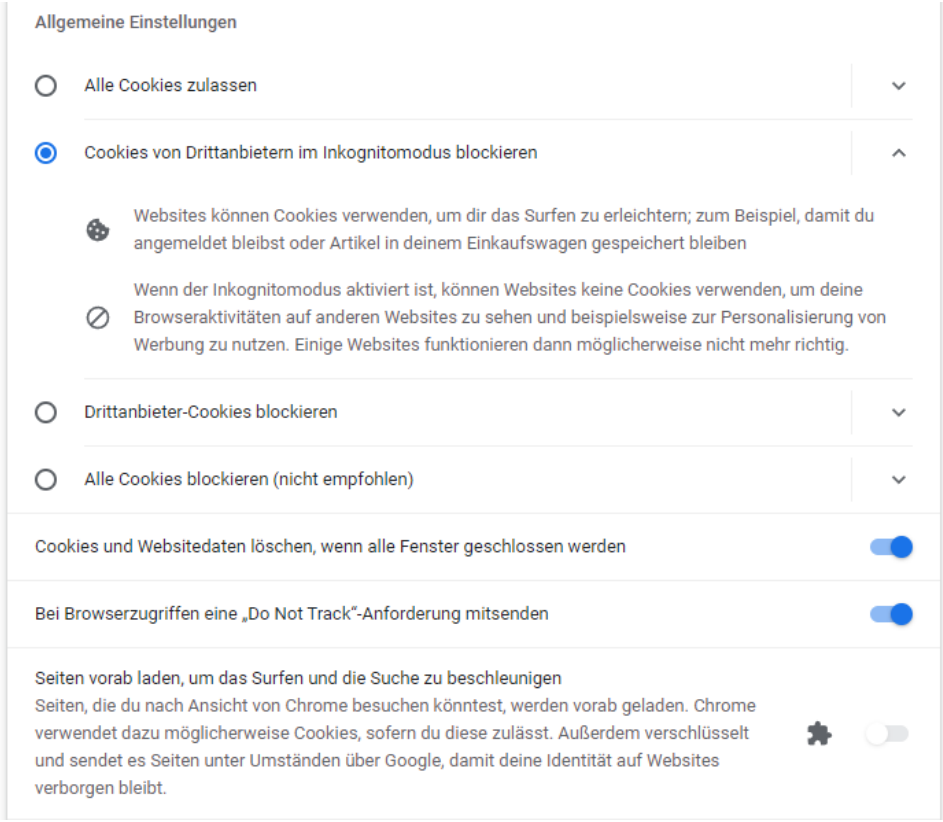


Die Option *Immer sichere Verbindung verwenden* sorgt dafür, dass beim Webseiten-Aufruf immer zuerst versucht wird, eine https-Verbindung aufzubauen. Sofern dies nicht möglich ist, wird man davor gewarnt, dass die Verbindung nicht sicher ist. Die Option sollte unbedingt aktiviert sein.

Normalerweise werden DNS-Anfragen unverschlüsselt über den Port 53 versendet. *Sicheres DNS* bedeutet, dass die eigene DNS-Anfrage verschlüsselt wird und nicht einfach ausgelesen werden kann.



Unter *Datenschutz und Sicherheit/Cookies* kann entschieden werden, ob Cookies beim Beenden gelöscht werden und Cookies von Drittanbietern standardmäßig blockiert werden.



Weitere Browser:

- Mozilla Firefox
- Microsoft Edge
- Safari Browser
- Brave Webbrowser
- Tor Browser

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 (automatische NAS-to-NAS-Sicherung). Gegebenenfalls können einzelne Sicherungen umbenannt werden (z. B. Backup_20220114), 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, dieser Datenbank-Dump wird im Datenbereich des Servers abgelegt, so dass dieser in die normale Sicherungskette integriert ist.

Datensicherung auf einem NAS-System

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_2022_01_14), so dass dieser Zustand erhalten bleibt.

Das NAS-System befindet sich nicht im selben Raum, wie der Server der Schule. Das Datenvolume benutzt ein verschlüsseltes Dateisystem und ist mit einem starken Passwort gesichert (Schutz der Daten bei einem Diebstahl der NAS).

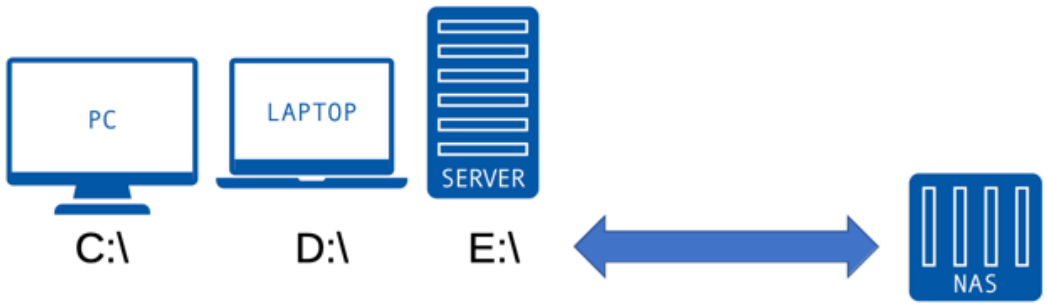
Zusätzliche Datensicherung auf USB-Festplatten

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

LABORÜBUNG 07 - DATEIEN UND ORDNER AUF EINEM WINDOWS 10 PC SICHERN

Szenario

Auf einem Windows-Computer oder einem Windows-Server soll ein automatisiertes Backup von einzelnen Ordnern und Dateien eingerichtet werden.



Aufgaben

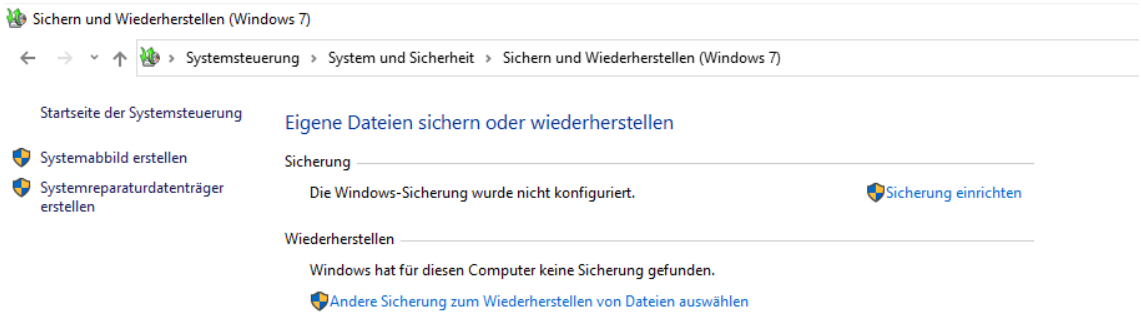
1. Entwickelnd Sie ein Backup-Konzept:
   - Was wird gesichert?
   - Wie häufig wird gesichert? (nur bei bestimmten Anlässen, Tagesbackup, Wochenbackup, Archivierung, …)
   - Wohin wird gesichert? (zweite Festplatte, Backupserver, USB-Platte, …)
   - Wie automatisiert soll die Sicherung erfolgen? (vollständig automatisiert, auf Knopfdruck, …)
   - Wie können die Daten gegebenenfalls wiederhergestellt werden?
2. Wählen Sie entsprechende Ordner und Dateien aus, die gesichert werden sollen.
3. Eruieren Sie welche integrierten Möglichkeiten es zur Erstellung eines Backups in Windows gibt.
4. Erstellen Sie ein Backup der Dateien und wählen Sie einen geeigneten Zeitplan zur automatisierten Sicherung der Dateien.

Weiterführende Aufgabe

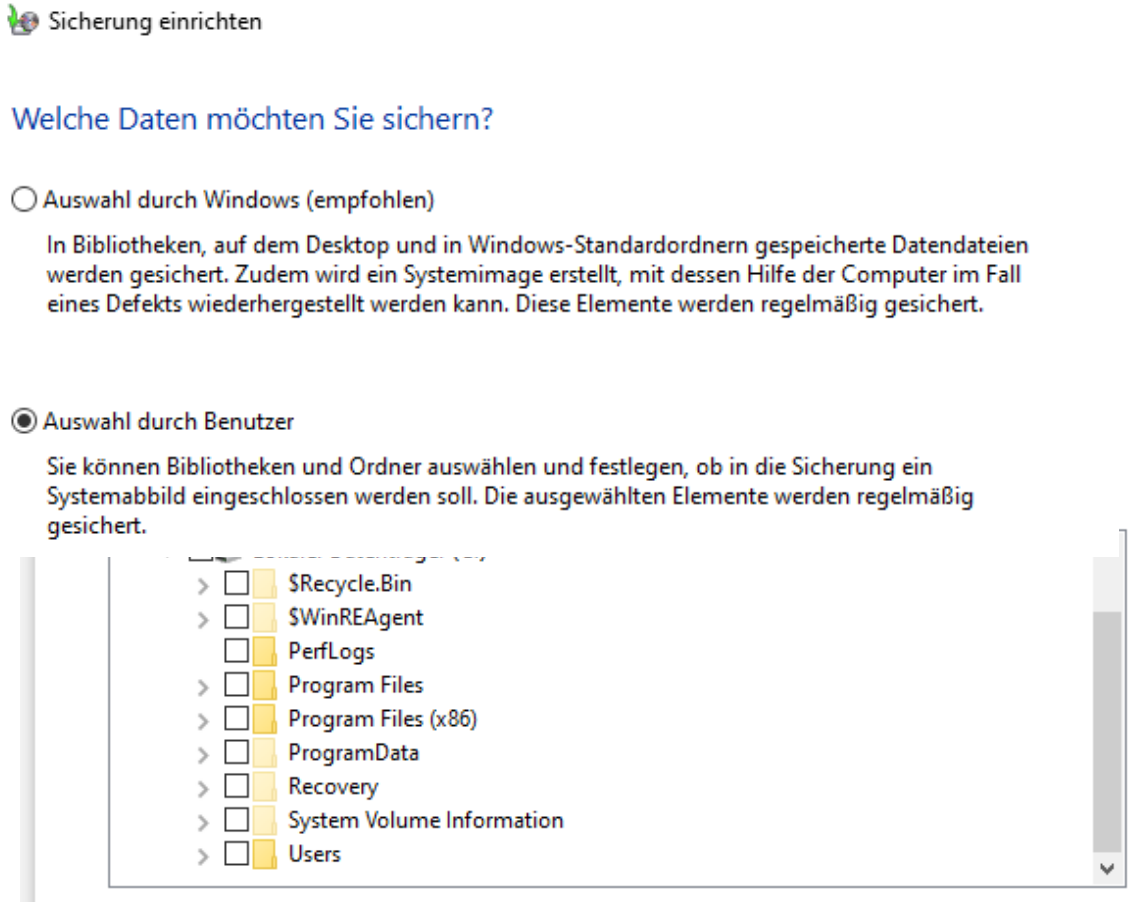
5. Stellen Sie die Dateien und Ordner aus der Sicherung wieder her.

Sicherung von Daten mit Windows-Bordmitteln

Windows 10 bietet verschiedene Möglichkeiten zur Datensicherung. Eine Möglichkeit findet sich in der Systemsteuerung unter *Sichern und Wiederherstellern (Windows 7)*.



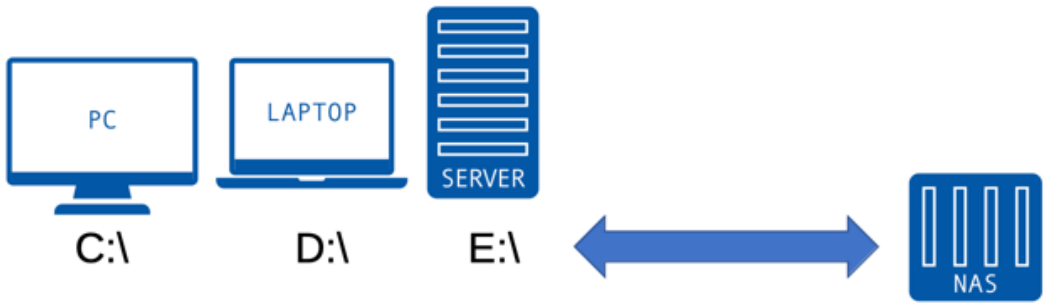
Hier kann ausgewählt werden, ob ein Systemabbild des gesamten Systems erstellt werden oder nur einige Dateien oder Ordner gesichert werden sollen. Es kann zudem ein Zeitplan erstellt werden, wann die Sicherung automatisiert, durchgeführt werden soll.



LABORÜBUNG 08 - 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.



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.

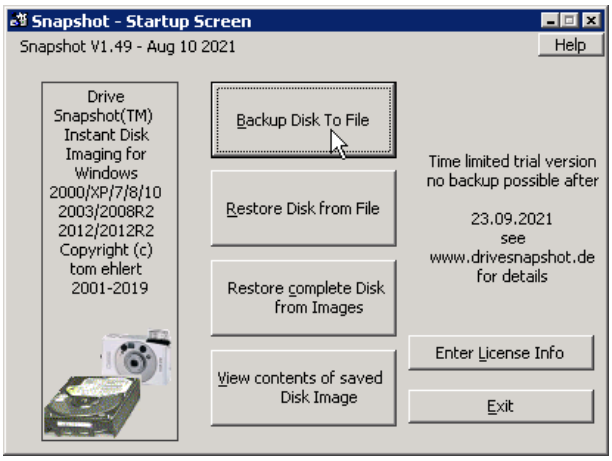
Weiterführende Aufgabe

3. Spielen Sie die Daten- oder Systemsicherung wieder zurück und überschreiben Sie dazu ihr aktuelles System.

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.

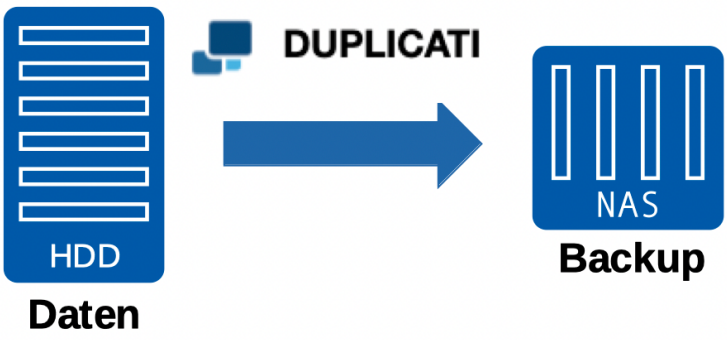
Sollte Windows nicht mehr lauffähig sein oder wurden Einstellungen im Bootmanager verändert, ist es notwendig, Drive Snapshot aus einem Live-System (WinPE) zu starten und ggf. den Bootmanager zu restaurieren.

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

LABORÜBUNG 09 - SICHERUNG VON DATEN EINES WINDOWS-RECHNERS MIT DUPLICATI

Szenario

Auf einem Windows-Rechner liegen im Verzeichnis „Daten“ viele relevanten Daten (z. B. für die Unterrichtsvorbereitung der Lehrkräfte etc.). Das Verzeichnis Daten soll täglich auf ein NAS-System 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 einem NAS-System 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.

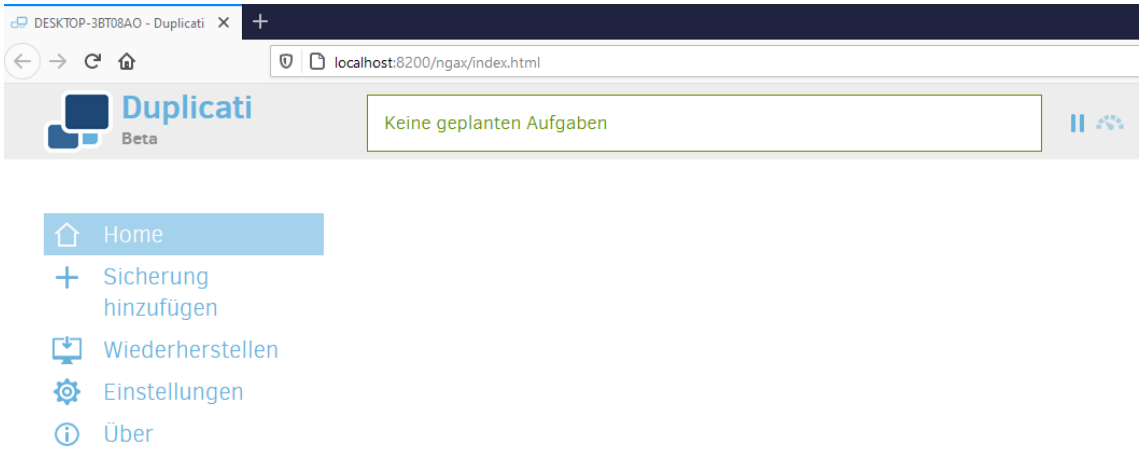
Hinweise

Eigenschaften von Duplicati

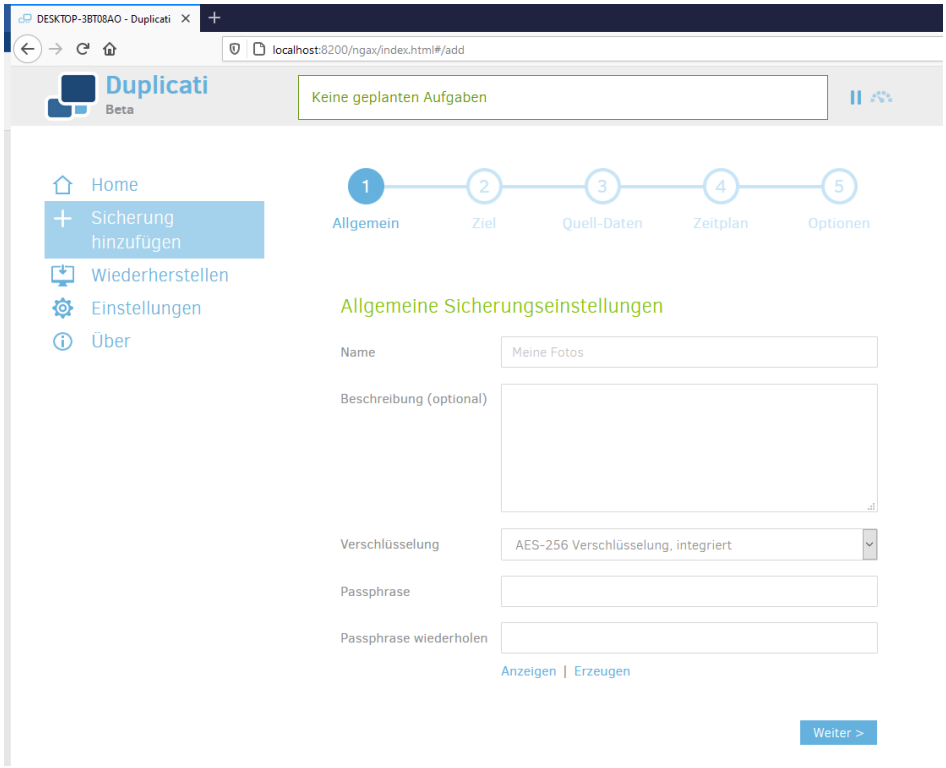
- Duplicati kennt sehr viele mögliche Sicherungsziele (Windows-Systeme, Linux-Systeme, NAS-Systeme, Cloud-Dienste) und Übertragungsprotokolle (z. B. smb, FTP, webdav, ssh).
- Duplicati 2.0 befindet sich noch im Beta-Status, kann aber verwendet werden
- Eine Erfolgskontrolle der Sicherung ist nur durch einen Test oder durch das Sicherungsprotokoll möglich.
- Duplicati kann Dateien mit AES-256 verschlüsseln.
- Duplicati arbeitet inkrementell, d. h. nur Änderungen an Dateien werden gesichert

Datensicherung mit Duplicati 2.0

Duplicati 2.0 läuft als moderne Weboberfläche im Browser. Standardmäßig ist die Konfigurationsseite nur von dem Rechner aus erreichbar, auf dem das Backup-Tool installiert wurde.



Nachdem Sie auf *Sicherung hinzufügen* geklickt haben und *Neue Sicherung konfigurieren* ausgewählt haben, kommen Sie zur Konfigurationsseite



Hier können Sie entscheiden, ob Duplicati die Sicherung direkt mit AES-256 verschlüsseln soll. Wählen Sie eine möglichst komplexe Passphrase, die Sie nicht vergessen.

Wählen Sie im Anschluss das Ziel (z. B. USB-Stick oder NAS) und die zu sicherenden Daten.

Unter Zeitplan kann festgelegt werden, wann die Sicherung durchgeführt werden soll. Verpasst Duplicati den Zeitpunkt der Sicherung, etwa weil es den USB-Stick nicht fand oder keinen Netzzugriff auf das NAS hatte, versucht es, das Backup schnellstmöglich nachzuholen.

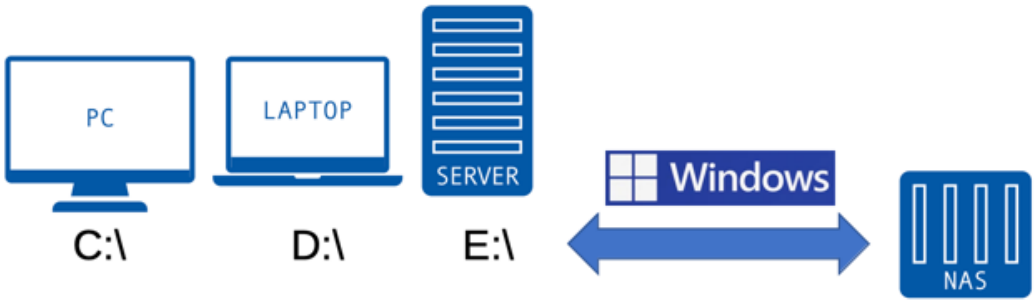
Duplicati speichert die Daten in Volumes ab und komprimiert diese. Voreingestellt sind 50 MB. Die Backup-Software arbeit inkrementell und speichert nach dem ersten Durchlauf nur jene Daten, die sich seit der letzten Sicherung verändert haben.

Ihre Notizen

LABORÜBUNG 10 - BACKUP EINES WINDOWS-PC MIT BOARDMITTELN

Szenario

Auf einem Windows-Computer soll eine Sicherung der Windows-Partition durchgeführt werden. Im Gegensatz zu Wiederherstellungspunkten speichert ein Systemabbild das Betriebssystem mit allen dazugehörigen Einstellungen.



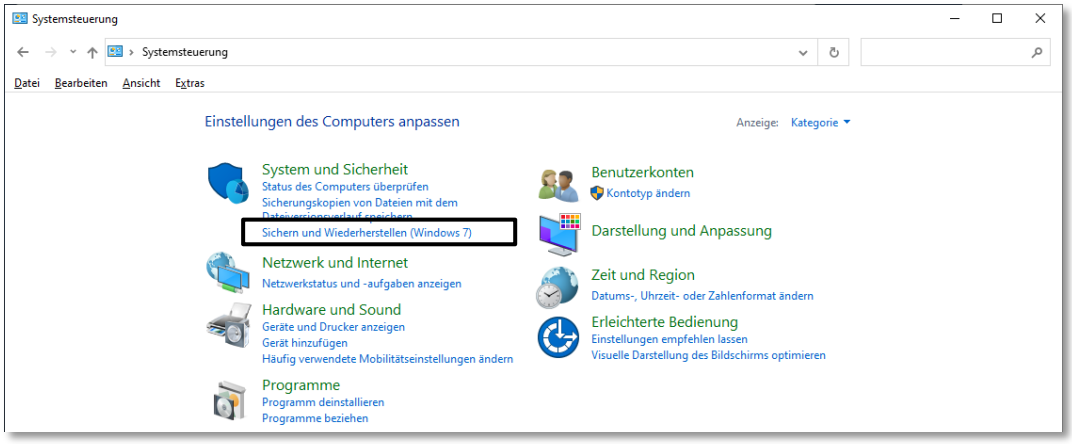
Aufgaben

1. Erstellen Sie ein Systemabbild des Desktop-Rechners auf einem Datenträger Ihrer Wahl. Das Systemabbild kann auf eine (externe) Festplatte, auf ein DVD-Laufwerk oder ein Netzlaufwerk gesichert werden. Wenn Sie eine externe Festplatte verwenden, müssen Sie diese eventuell in das **NTFS-Format** formatieren.
2. Spielen Sie das Systemabbild zurück und überprüfen Sie die Funktionalität.

HINWEISE

Erstellung eines Systemabbilds mit Boardmitteln

1. Öffnen Sie die Systemsteuerung über die Suche im Start-Menü in der Kategorien Ansicht.
2. Wechseln Sie im Bereich Systeme und Sicherheit in Sichern und Wiederherstellen (Windows 7).



3. Wählen Sie nun „Systemabbild erstellen“ aus und geben Sie anschließend an, wo die Sicherung gespeichert werden soll. Ein externer Datenträger muss für die Sicherung des Systemabbilds im NFTS Format vorliegen!
4. Geben Sie an, welche Laufwerke gesichert werden sollen. Laufwerke, die für die Ausführung von Windows notwendig sind, werden automatisch miteingeschlossen. Führen Sie eine erste Sicherung durch!
5. Prüfen Sie, ob Sie die Sicherung wieder zurückspielen können.

Benutzerauthentifizierung – Möglichkeiten und Risiken

Schulen setzen häufig eine Windows Domänenstruktur mit personalisierten Zugängen ein. Dabei müssen sich die Benutzer einen eindeutigen Benutzernamen und ein (möglichst komplexes) Passwort merken. Diese Anmeldeinformationen (Credentials) werden dann bei jedem Anmeldevorgang abgefragt. Das gleiche Prinzip wird auch bei der Nutzung verschiedener Onlinedienste angewendet. Die verschiedenen Credentials werden bei jedem Dienst zentral in einer Datenbank gespeichert.

Die geforderte Komplexität der Passwörter soll die Sicherheit der Credentials erhöhen. Leider erreicht man dadurch oft das Gegenteil: Das Passwort wird z. B. auf einem Notizzettel unter der Tastatur aufbewahrt oder persönliche Daten (z. B. Vornamen + Geburtsjahr) werden mit einem Sonderzeichen kombiniert, um die geforderte Komplexität des Passworts zu erreichen. Diese Credentials weisen Schwachstellen auf (Social Engineering).

Allerdings muss es nicht zwangsläufig am Benutzer liegen, dass die Credentials Unbefugten zugänglich sind. So kommt es immer wieder zu sog. Data Breaches (Datendiebstahl oder Missbrauch), bei dem die zentralen Benutzerdatenbanken bei den Dienstanbietern kompromittiert werden. Sind Passwörter bei diesen im Klartext gespeichert, kann der Datendieb die Credentials bei vielen Onlinedienste automatisiert ausprobieren. Näheres finden Sie in den Selbstlernkursen *Sicherheit durch Passwörter* und *Datensicherheit durch Verschlüsselung*.

Passwort Safes (oder Manager) bieten die Möglichkeit zur sicheren Verwahrung von Passwörtern. Dabei werden die Credentials verschlüsselt in eine zentrale (lokale) Datenbank geschrieben, die mit einem Masterpasswort gesichert ist. Der Benutzer muss sich dann nur noch dieses merken. Dieses Passwort sollte dann aber die notwendige Komplexität aufweisen.

2-Faktor-Authentifizierung (ZFA) und Multi-Faktor-Authentisierung (MFA)

Rein passwortbasierte Identitätsnachweise beruhen auf der Kenntnis des Benutzernamens und des Passworts. Idealerweise kann hier eine zweite Sicherheitsstufe integriert werden, wenn ein Konto mehr als die Kenntnis des Passworts verlangt. Zusätzlich möglich sind Kombinationen aus folgenden Faktoren:

- Identitätsnachweis mittels Sein (Biometrie) (z. B. Fingerabdruck)
- Identitätsnachweis mittels Besitzes (z. B. physischer Sicherheitsschlüssel)
- Identitätsnachweis mittels Wissens (z. B. Passwort)

Bei einer MFA werden mehrere unterschiedliche Faktoren, bei einer ZFA werden zwei beliebige Faktoren kombiniert.

Verwendet man für die Authentisierung zwei Faktoren, spricht man von einer Zwei-Faktor-Authentisierung (ZFA).

MFA und ZFA sollten unbedingt bei wichtigen Zugängen verwendet werden (Onlinebanking). Die meisten Anbieter ermöglichen es ihren Kunden mittlerweile verschiedene Möglichkeiten.

Identitätsnachweis mittels Sein (Biometrischer Faktor)

Zur Ermittlung der Identität einer Person werden hierbei biometrische Merkmale herangezogen (Fingerabdruck sein oder eine Gesichtserkennung). Für das IT-Sicherheitsziel der Authentizität werden biometrische Systeme als am geeignetsten angesehen. Für die biometrische Überprüfung ist eine spezielle Hardware (z. B. Fingerabdrucksensor oder IR Webcam) notwendig.

Die biometrischen Merkmale werden dabei nur lokal auf dem Gerät gespeichert.

Identitätsnachweis mittels Besitzes

Die Authentisierung kann hier auf einem zweiten Gerät des Anwenders erfolgen, z. B. durch eine Authenticator-App auf dem eigenen Smartphone geschehen. Dort muss dann die Anmeldung zusätzlich genehmigt werden (z.B. PIN-Nummer Übertragung, One Time Password).

Unter der FIDO-Allianz (FIDO = Fast Identity Online) haben sich u. a. Google, Amazon, Microsoft, Apple und PayPal zusammengeschlossen, um einen neuen passwortlosen Identitätsnachweis im Internet zu etablieren (FIDO 2). Hier wird ein Authenticator (App oder physischer Sicherheitsschlüssel) verwendet, in dem durch asymmetrische Kryptografie die Anmeldedaten gespeichert werden.

Identitätsnachweis mittels Wissens

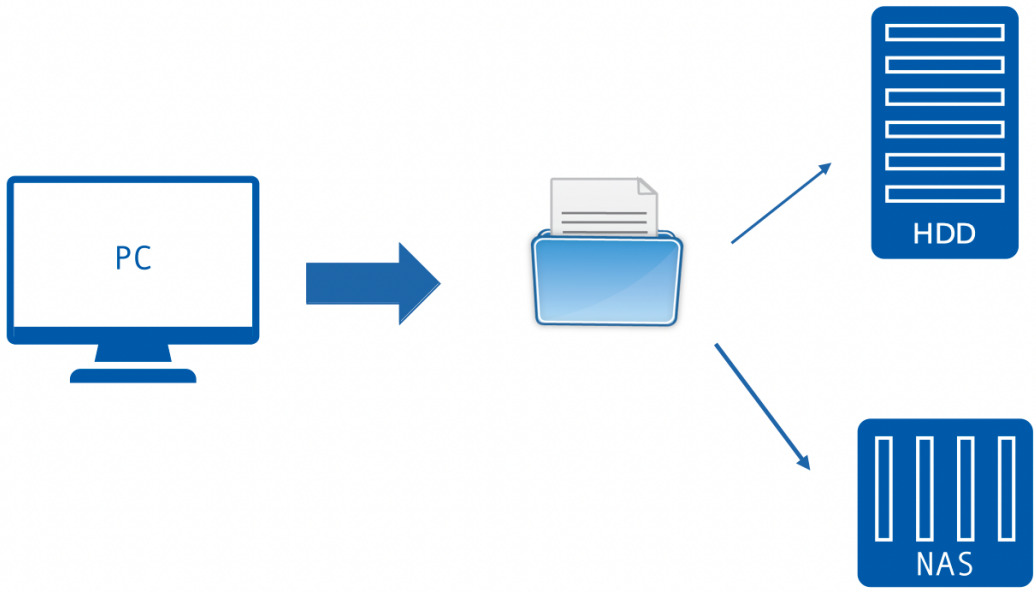
Diese Art der Authentisierung ist die am weitesten verbreitete. Dabei wird die Identität mittels Benutzername und Passwort oder Sicherheitsabfrage nachgewiesen.

Weitere Informationen können unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/Zwei-Faktor-Authentisierung-Datensicherheit/zwei-faktor-authentisierung-datensicherheit_node.html nachgelesen werden.

LABORÜBUNG 11 - 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 mobilen USB-Festplatten bzw. NAS-Speichern sichern, die er abwechselnd benutzt.



Aufgaben

1. Überlegen Sie sich eine Möglichkeit, wie die Daten abwechselnd auf einem NAS-System und einer mobilen Festplatte gesichert werden können. Wie könnte man die Sicherung automatisieren bzw. eine mehrstufige Sicherung einrichten?
2. Testen Sie das Kommandozeilenwerkzeug robocopy zur Datensicherung. Erstellen Sie ein Skript, das die Datensicherung „auf Knopfdruck“ ausführt.

HINWEISE

Kopieren von Daten 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). Sie ist in der Handhabung eher schwerfällig und nur bedingt zu empfehlen.

```
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.

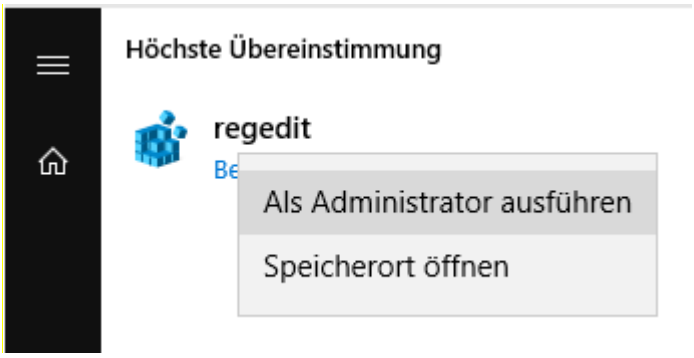
```
@ECHO OFF

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
```


Mit Hilfe solcher Skripten ist eine Automatisierung von Backups einfach möglich. So ist es beispielsweise möglich, wichtige Daten einer Windows10-Arbeitsstation nach dem Systemstart in ein Backupverzeichnis zu sichern. Das Sicherungsverzeichnis kann

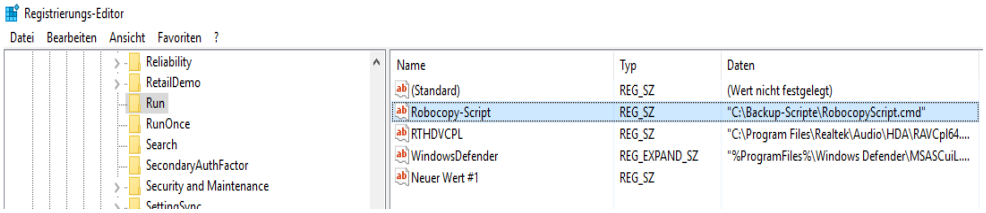
- auf einer lokalen Platte
- auf einem Wechselmedium (z.B. USB-Platte)
- auf einem Netzlaufwerk

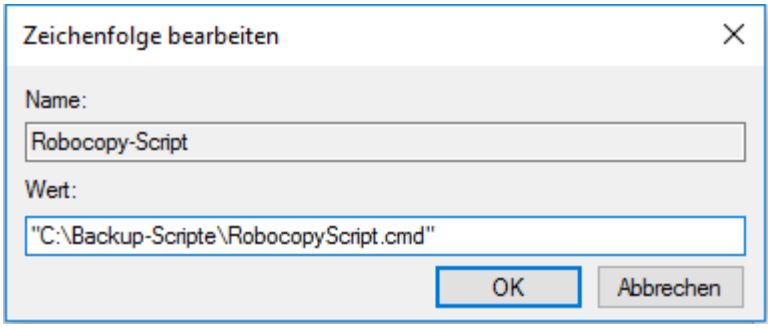
liegen. Dazu gibt es beispielsweise die Möglichkeit, das Backup-Script über einen **Run-Schlüssel in der Registry** zu starten:

(1) Ausführen von regedit als Administrator

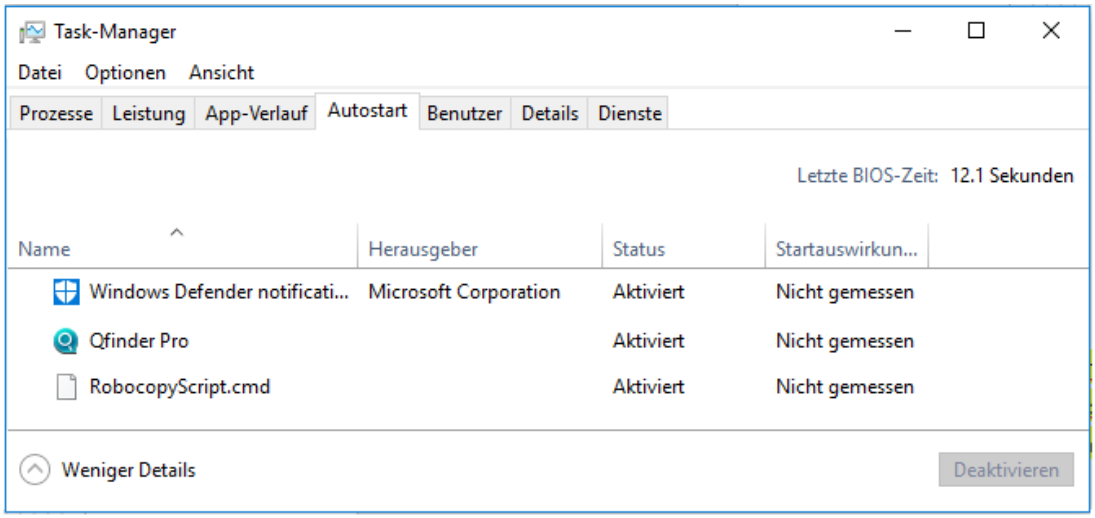


Anlegen einer Zeichenfolge mit einem beliebigen Namen (z.B. „Robocopy-Script“). Als Wert wird eingetragen, wo das beim Systemstart auszuführende Skript liegt (hier z.B. "C:\Backup-Scripte\RobocopyScript.cmd").





Mit msconfig kann die Einstellung überprüft werden:



Es ist auch möglich, die Autostart-Funktion von Windows10 zu nutzen, um das Skript beim Hochfahren jedes Mal aufzuführen. Dazu legen Sie am besten eine Verknüpfung zu dem Skript an, die sie in den Ordner

„C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\StartUp“

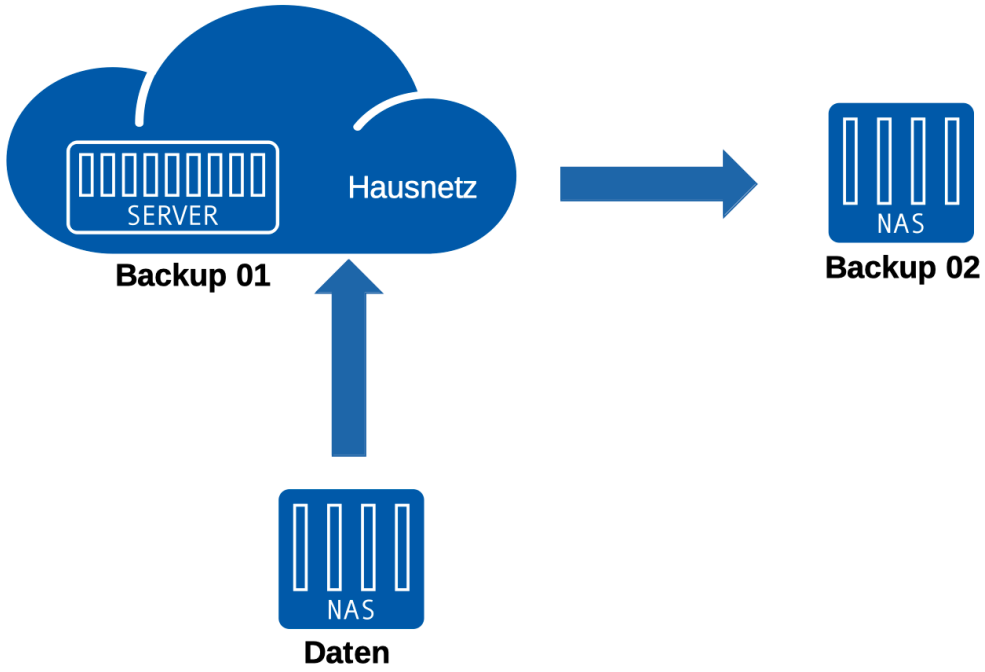
kopieren.

LABORÜBUNG 12 - SICHERUNG VON DATEN EINER NAS AUF EINE BACKUP-NAS

Viele NAS-Systeme unterstützen eine komfortable Backup-Funktion (NAS to NAS) zwischen NAS-Systemen 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. Zusätzlich soll in regelmäßigen Abständen eine zweite Sicherung auf ein NAS an einem anderen Standort eingerichtet werden.

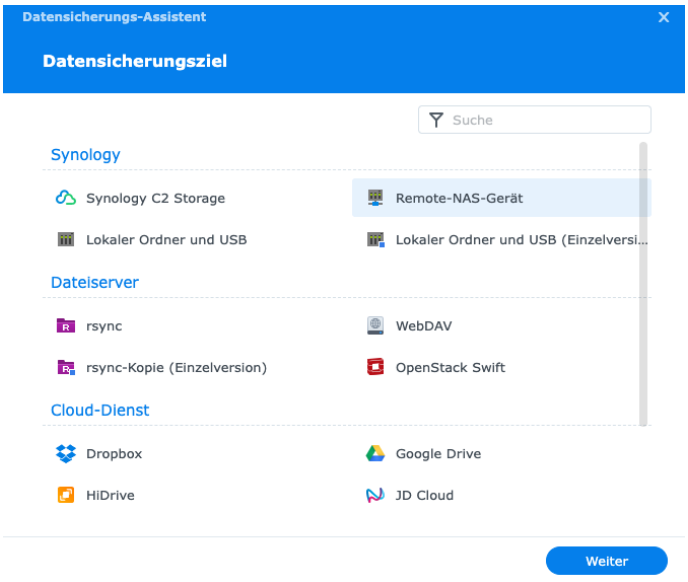


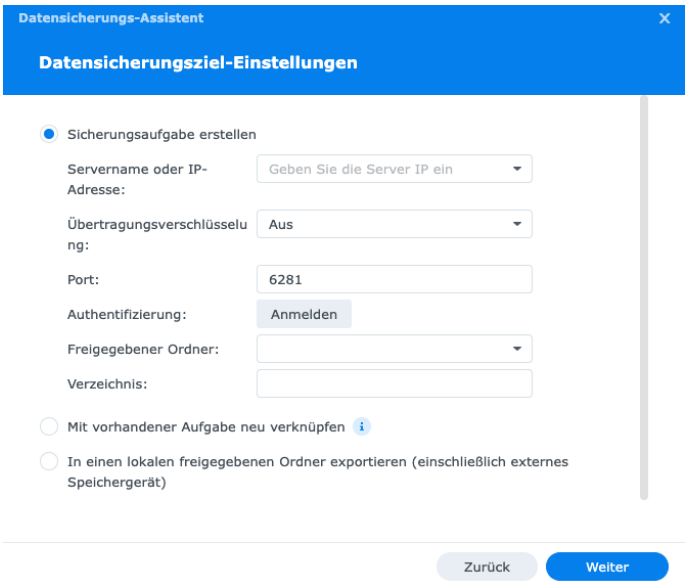
Aufgaben

1. Richten Sie auf einem NAS die Freigabe Lehrer und auf dem Backup-NAS die Freigabe Backup und das Unterverzeichnis Lehrer ein.
2. Richten Sie auf dem NAS-System 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.
3. Konfigurieren Sie die Sicherungshäufigkeit und die Optionen (nur Dateien kopieren, die sich unterscheiden; Zusatzdateien löschen). Zum Testen kann man den Auftrag sofort ausführen.

4. Einige Sicherungen sollen archiviert werden. Benennen Sie zur Datenarchivierung den Zielordner Backup/Lehrer um (z.B. in Backup\Lehrer_2022_03_04) Überprüfen Sie, ob bei der nächsten Sicherung der Ordner Backup\Lehrer erneut angelegt wird.
5. Konfigurieren Sie eine entsprechende Sicherung vom Backup-NAS auf ein drittes NAS-System für alle archivierten Sicherungen! Wie lässt sich dieses NAS-System vor Malwarebefall schützen?

HINWEISE





LABORÜBUNG 13 - VERWENDUNG EINES PASSWORT-MANAGERS

Passwort-Manager bieten eine einfache Möglichkeit, die verschiedenen Benutzerpasswörter sicher und bequem zu speichern.

Szenario

Richten Sie auf Ihrem privaten Endgerät einen Passwort-Manager ein.

Aufgaben

1. Laden Sie den Passwortmanager Bitwarden oder KeePass herunter und installieren Sie ihn auf einem Endgerät.
2. Erstellen Sie eine Passwort-Datenbank.
3. Vergeben Sie einen komplexen Hauptschlüssel (Masterschlüssel) und überlegen Sie sich ein Konzept, wie Sie diesen sicher aufbewahren können!
4. Tragen Sie einige Passwort-Einträge in die Datenbank ein.
5. Nutzen Sie, sofern vorhanden, den Passwortgenerator und probieren Sie die verschiedenen Komplexitätsmöglichkeiten aus!
6. Richten Sie eine Synchronisierung der Datenbank für ihre Geräte ein.

Weiterführende Aufgaben

7. Installieren Sie eine Browserweiterung zur Nutzung des Passwort-Managers im Browser.
8. Richten Sie Windows-Hello als Alternative zum Entsperren mit einem Masterpasswort ein!

HINWEISE

Passwort-Manager speichern Passwörter in einer verschlüsselten Datenbank auf einem Rechner oder einem Netzwerkspeicher. Teilweise können auch weitere sensible Daten (z. B. Kreditkarten) sicher digital in ihnen gespeichert werden. Die Sicherheit des Masterpassworts bestimmt die Sicherheit der gespeicherten Passwörter maßgeblich.

Zusätzliche Funktionen sind Hilfestellungen wie Warnungen vor kompromittierten Passwörter, das Finden von mehrfach verwendeten Passwörtern oder zusätzliche Speichermöglichkeiten für Notizen, Seriennummern.

KeePass (https://keepass.info)

Kostenlose Open-Source Lösung.

Verschiedene Ableger von KeePass sind für alle Betriebssystemversionen verfügbar, allerdings gibt es keine automatische Synchronisierung der Datenbank zwischen mehreren Geräten. Nicht alle Plug-Ins funktionieren unter allen Versionen

Bitwarden (https://www.bitwarden.com)

Die grundsätzlich kostenlose Open-Source-Lösung Bitwarden verfügt über Desktop-Apps für alle verbreiteten Desktop-Betriebssysteme und kann auch lokal, z.B. auf einer NAS, installiert werden. Zudem werden für alle Browser entsprechende Erweiterungen angeboten. In den kostenpflichtigen Versionen sind weitere Features integriert.

1Password (https://1password.com)

Kostenpflichtiger Passwort-Manager, der für alle Betriebssysteme und zahlreiche Browser erhältlich ist mit automatischer Synchronisierung der Datenbank zwischen verschiedenen Geräten, auch mit unterschiedlichen Betriebssystemen.

Browserbasierte Lösungen

In modernen Browsern sind inzwischen auch Passwort-Manager integriert. Eine Synchronisierung über Geräte hinweg geschieht hier mit Hilfe eines Kontos, das beim entsprechenden Browserhersteller eingerichtet wird. Bei der Verwendung muss sichergestellt werden, dass der Browserhersteller keinen Zugriff auf die gespeicherten Passwörter hat. Das kann durch eine Ende-zu-Ende-Verschlüsselung erreicht werden.

In Betriebssystemen integrierte Passwortverwaltungen

Alle Betriebssysteme bieten eine Verwaltung für Passwörter an, die meistens nicht alle Komfortfunktionen der vorgestellten Passwortmanager bietet, für grundlegende, zentrale Passwortverwaltung jedoch ausreichen.

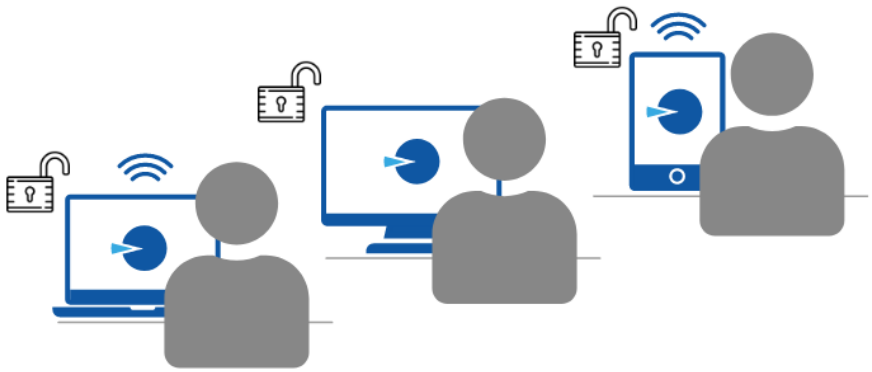
LABORÜBUNG 14 - EINRICHTUNG EINER PASSWORTLOSEN ANMELDUNG FÜR BENUTZER

Viele Betriebssysteme bieten alternative Anmeldemethoden zur Benutzerauthentifizierung. Außerdem gibt es geführte Zugriffsmöglichkeiten (z. B. Kiosk oder Gastmodus)

Szenario

Benutzer sollen alle mobilen Geräte der Schule ohne Anmeldung verwenden können.

Auf Ihren eigenen Geräten sollen alternative Anmeldemetzhoden verwendet werden.



Aufgaben

1. Richten Sie auf Ihrem Endgerät den Zugriff über ein Gastkonto ein!
2. Richten Sie auf einem Mobilgerät einen geführten Zugriff ein!
3. Konfigurieren Sie alternative Zugriffsmöglichkeiten wie Windows HELLO und eine automatische Anmeldung!
4. Erstellen Sie ein Kiosk System, bei dem ein Browser als einzige Anwendung automatisch startet.

HINWEISE

Alle Betriebssysteme verfügen über die Möglichkeit des Zugriffs über ein Gastkonto mit eingeschränkten Rechten.

Mobilgeräte können mit Dummy Accounts betrieben werden und wesentliche Sicherheitsfunktionen (Anmelden nach Leerlauf nötig) außer Kraft gesetzt werden.

Es gibt vereinfachte Anmeldeverfahren wie Windows HELLO oder Touch ID. Auch USB-Sticks als Anmeldetoken werden unterstützt.

Automatisches Anmelden unter Windows

WIN + R – *netplwiz* (Muss als Administrator ausgeführt werden)

Registry Einstellung für netplwiz

HKEY_LOCAL_MACHINE – Software – Microsoft - Windows NT – CurrentVer-sion – PasswordLess – Device - DevicePasswordLessBuildVersion muss den Wert 0 haben.

Die automatische Anmeldung erfordert eventuell weitere Einstellungen wie das Deaktivieren von Windows HELLO.

Es gibt mehrere Tools für die automatische Anmeldung, z.B. Systernals Autologon.

Kiosk Modus

https://docs.microsoft.com/de-de/windows/configuration/kiosk-single-app

VERSCHLÜSSELUNG VON VERTRAULICHEN DOKUMENTEN UND DATENTRÄGERN

Grundsätzlich können einzelne Dateien, Ordner und Archive oder ganze Datenträger verschlüsselt werden. Je nach Anwendungsszenario kommen unterschiedliche Programme in Frage.

Verschlüsselung von Daten kann notwendig werden, wenn

- vertrauliche Daten bei externen Anbietern in der Cloud gespeichert werden
- zur Datenübertragung nicht abgesicherte Transportwege benutzt werden,
- Onlinedienste mit wenig vertrauenswürdigen Herstellern benutzt werden.

Hardwareverschlüsselung

Dabei können Daten per Software verschlüsselt werden oder man benutzt Speichermedien (z. B. Krypto-USB-Sticks), die eine Verschlüsselung in Hardware implementiert haben. Verschlüsselnde USB-Datenspeicher mit eigener Tastatur sind praktisch, weil sie ohne Zusatzsoftware an vielen unterschiedlichen Geräten funktionieren. Selbst Angreifer mit einfachen IT-Kenntnissen hebeln schlecht gemachte Sicherheitsfunktionen jedoch aus. Weil es keine Pflicht für externe Prüfungen gibt, kann jeder Hersteller einfach behaupten, sein Produkt sei „sicher“ – bis jemand das Gegenteil beweist. Allerdings sind Daten auf einem standardmäßig verschlüsselten USB-Stick besser geschützt als auf einem normalen USB-Stick.

Softwareverschlüsselung

Moderne Betriebssysteme bieten Möglichkeiten (z. B. BitLocker, FileVault) zur Verschlüsselung von Festplatten oder externe Speichergeräte. Alternativ gibt es hierzu auch diverse kostenlose oder kommerzielle Verschlüsselungssoftware (z. B. Veracrypt, Boxcryptor). Bei der Verschlüsselung von Datenträgern sollte darauf geachtet werden, dass der gesamte Datenträger verschlüsselt wird. Dadurch kann verhindert werden, dass versehentlich unverschlüsselte Dateien auf dem Datenträger abgelegt werden.

Bei der Verschlüsselung muss ein entsprechendes Passwort gewählt werden, welches für die Verschlüsselung genutzt werden. Dabei hängt die Sicherheit der Verschlüsselung auch von der gewählten Komplexität und Sicherheit des gewählten Passworts ab. Es empfiehlt sich ein Passwort oder Passphrase mit ausreichend Länge (mind. 15 Zeichen) und Komplexität (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen) zu verwenden.

Aktuelle Empfehlung für Passwörter:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

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 Alternativen zu einer Verschlüsselung:

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

Ihre Notizen

Programme zur Verschlüsselung von einzelnen Dateien und Ordnern

Office-Programme

Office-Programme (z. B. Microsoft Office, Libre Office, Open Office) bieten die Option „Passwortschutz“. Dabei wird der Zugriff auf das Office-Dokument mit einem Passwort geschützt und der Inhalt des Dokuments verschlüsselt. Bisher ist bei aktuellen Office-Versionen kein Verfahren bekannt, wie man ohne dieses Passwort den Inhalt lesen kann. Office-Dokumente, die als PDF gespeichert werden, können auch mit einem Passwortschutz versehen werden und so verschlüsselt gespeichert werden.

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

7-Zip

7-Zip ist ein Open Source Programm, das für alle Betriebssysteme erhältlich ist zur Komprimierung von Dateien oder Ordnern mit optionaler Verschlüsselung (z.B. zum Transport oder als E-Mail-Anhang). Mit 7-Zip verschlüsselte Archive können auch mit Alternativen (z. B. WinRar, Winzip) entpackt werden, solange sie mit dem AES-Algorithmus umgehen können.

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. Inzwischen kann das Tool in kommerzielle Kollaborationstools (z. B. MS Teams) als App eingebunden werden und direkt dort Dateien und Nachrichten verschlüsseln. Zudem kann es mit allen gängigen Cloud-Anbietern direkt zusammenarbeiten.

Cryptomator

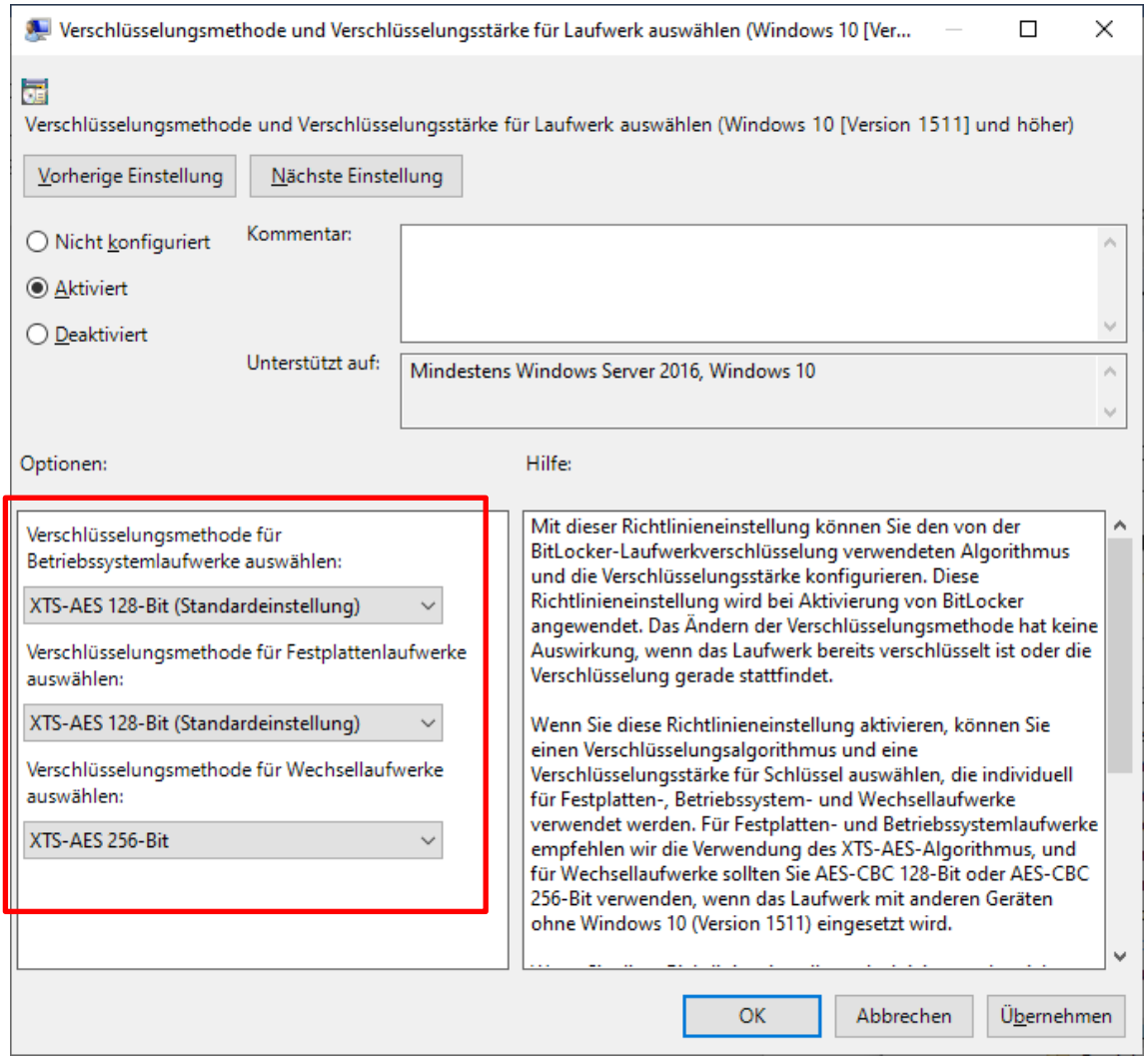
Cryptomator verschlüsselt Dateien einzeln und ermöglicht die Synchronisierung mit Cloud-Speichern. Die Software stellt den verschlüsselten Ordner entschlüsselt als virtuelles Laufwerk zur Verfügung. Die Version für Windows, Mac, Linux und Android ist kostenlos nutzbar. Die IOS-Version ist kostenpflichtig.

Programme zur Verschlüsselung von Datenträgern

BitLocker

BitLocker ist ein Windows-Feature, das Datenträger (Partitionen oder Volumes) sicher verschlüsselt. Es eignet sich sehr gut zur Verschlüsselung von mobilen Datenträgern und Festplatten mobiler Endgeräte. Zur erstmaligen Einrichtung der Verschlüsselung ist eine Education, Professional oder Enterprise -Versionen von Windows nötig, die anschließende Nutzung ist mit beliebigen Windows-Versionen möglich. Ein Benutzer muss Bitlocker nicht manuell aktuell halten (Windows Update). Bitlocker verschlüsselt auch virtuelle Festplatten.

Standardmäßig verschlüsselt BitLocker mit dem AES-Verfahren mit 128-Bit langem Schlüssel. Das geht auch sicherer, denn BitLocker kann auch 256 Bit lange Schlüssel verwenden. Es muss nur über Gruppenrichtlinien aktiviert werden. Dazu öffnet man den Gruppenrichtlinienordner (gpedit.msc), hangelt sich in den Ordner *„Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerksverschlüsselung“*.



FileVault

MacOS bietet mit FileVault eine zu BitLocker vergleichbare Verschlüsselungsfunktion an. Die Verschlüsselung kann entweder in den Systemeinstellungen (Modul Sicherheit) oder über das Kommando `sudo fdesetup enable` aktiviert werden. Für die Verschlüsselung ist kein eigenes Passwort vorgesehen. Bei aktuellen Macs wird zur Verschlüsselung der integrierte T2-Chip verwendet. Auf Geräten ohne diesen Secure-Chip wird die Verschlüsselung mit dem Login-Passwort verknüpft.

Beim Einrichten von FileVault gibt das Betriebssystem die Möglichkeit, den Schlüssel in iCloud oder in einer lokalen Datei zu speichern. Die Schlüsseldatei bietet im Notfall eine Möglichkeit zum Datenzugriff ohne das Login-Passwort.

VeraCrypt

VeraCrypt ist das Nachfolgeprogramm von TrueCrypt und ist in der Bedienung und Anwendung nahezu identisch. Es ist für alle gängigen Betriebssysteme im Desktopbereich erhältlich. 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. Zusätzlich werden die Container bei der inkrementellen Datensicherung oft ignoriert, da am Container nicht erkennbar ist, wann dieser zuletzt aktualisiert wurde. Für mobile Endgeräte gibt es keine VeraCrypt App.

LABORÜBUNG 15 - PASSWORTSCHUTZ UND VERSCHLÜSSELUNG VON OFFICE-DOKUMENTEN

Szenario

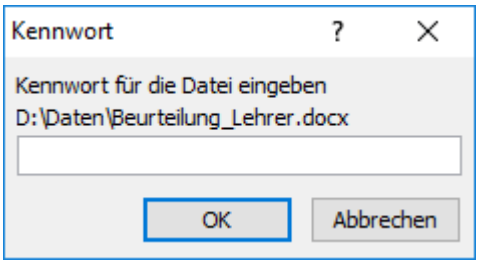
Ein vertrauliches Office-Dokument soll mit einem Passwort geschützt werden.

Aufgaben

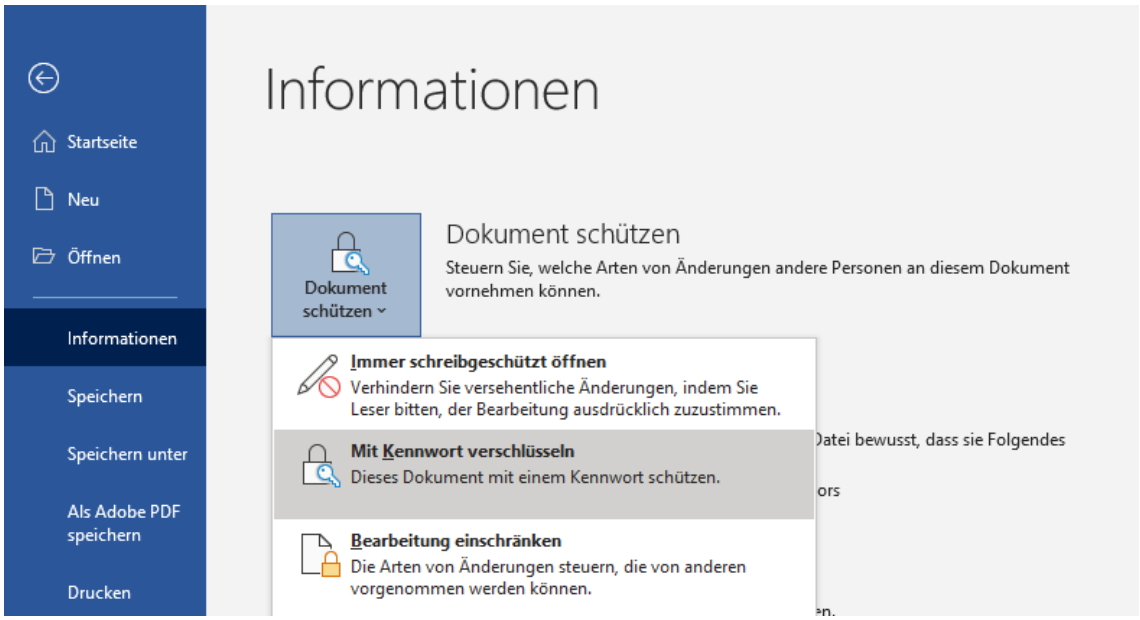
1. Erstellen Sie ein Office-Dokument (z. B. mit Microsoft-Office oder Libre-Office) und versehen Sie das Dokument mit einem Passwort.
2. Zeigen Sie, dass ohne dieses Passwort das Office-Dokument nicht geöffnet werden kann und auch mit einem anderen Programm der Inhalt nicht gelesen werden kann.
3. Speichern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

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. Bei Libre-Office gibt es die Möglichkeit, dass zudem ein Rechte-Passwort vergeben wird.



Sollte ein Microsoft Office Dokument an jemanden weitergeben werden, der kein MS Office besitzt, aber ein Programm hat, das Office- Dateien lesen kann (z. B. Libre Office, Softmaker Office) stellt das kein Problem dar. Die Programme können die verschlüsselte Office Datei öffnen und mit dem Kennwort entschlüsseln.

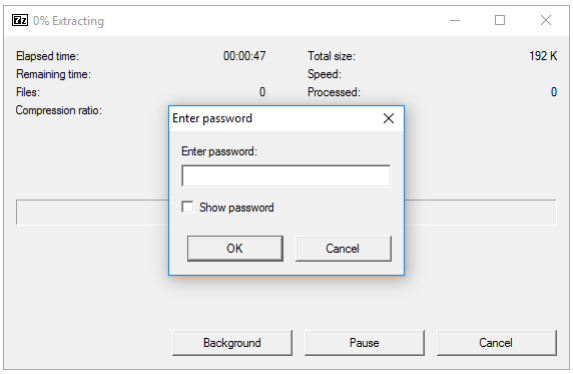


Ihre Notizen

LABORÜBUNG 16 - 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 oder bereits im Vorfeld vereinbart.

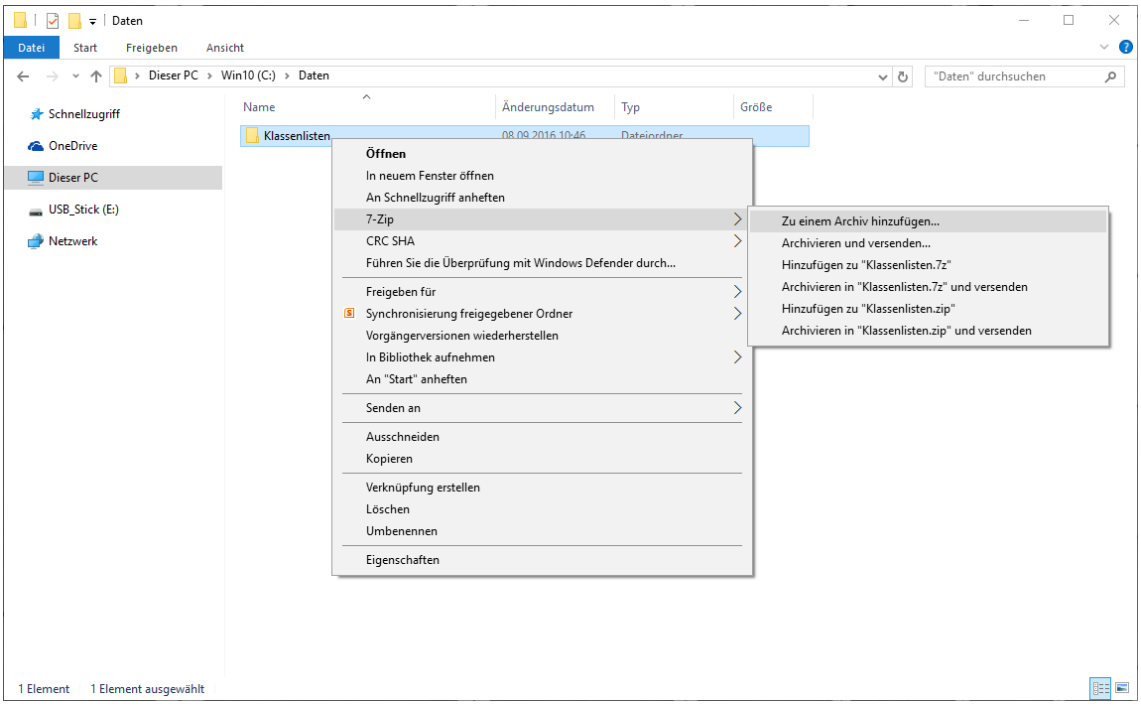


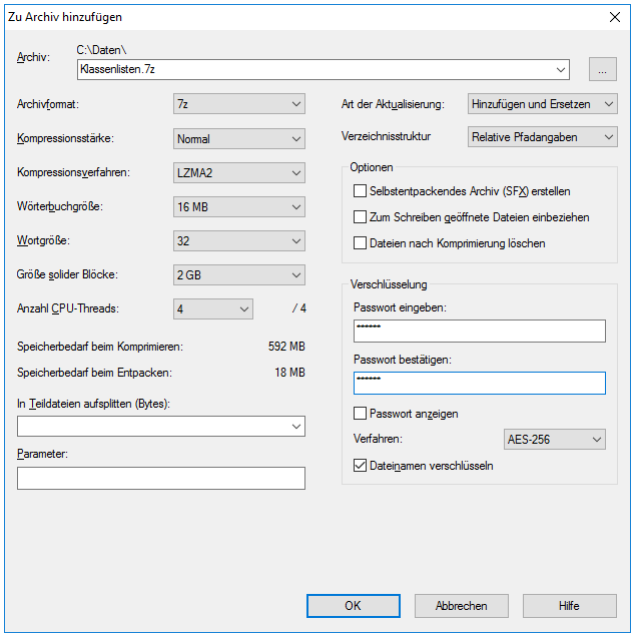
Aufgaben

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 Standardinstallation im Kontextmenü von Dateien und Ordnern zugänglich.





LABORÜBUNG 17 - VERSCHLÜSSELUNG VON USB-STICKS MIT BITLOCKER

Szenario

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

Die pädagogische Systembetreuung 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. Es soll die sichere Verschlüsselung mit 256 Bit zum Einsatz kommen.

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).

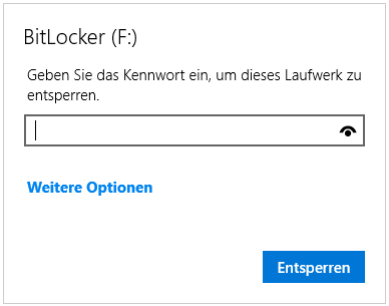
Weiterführende Aufgaben

4. Entschlüsseln Sie den USB-Stick an einem anderen Endgerät.
5. Erstellen Sie mit Hilfe von Veracrypt einen verschlüsselten Container und testen Sie die Funktionsfähigkeit!
6. Vergleichen Sie den Funktionsumfang von Veracrypt, Cryptomator und Bitlocker und treffen Sie eine Entscheidung für Ihren schulischen Einsatz!

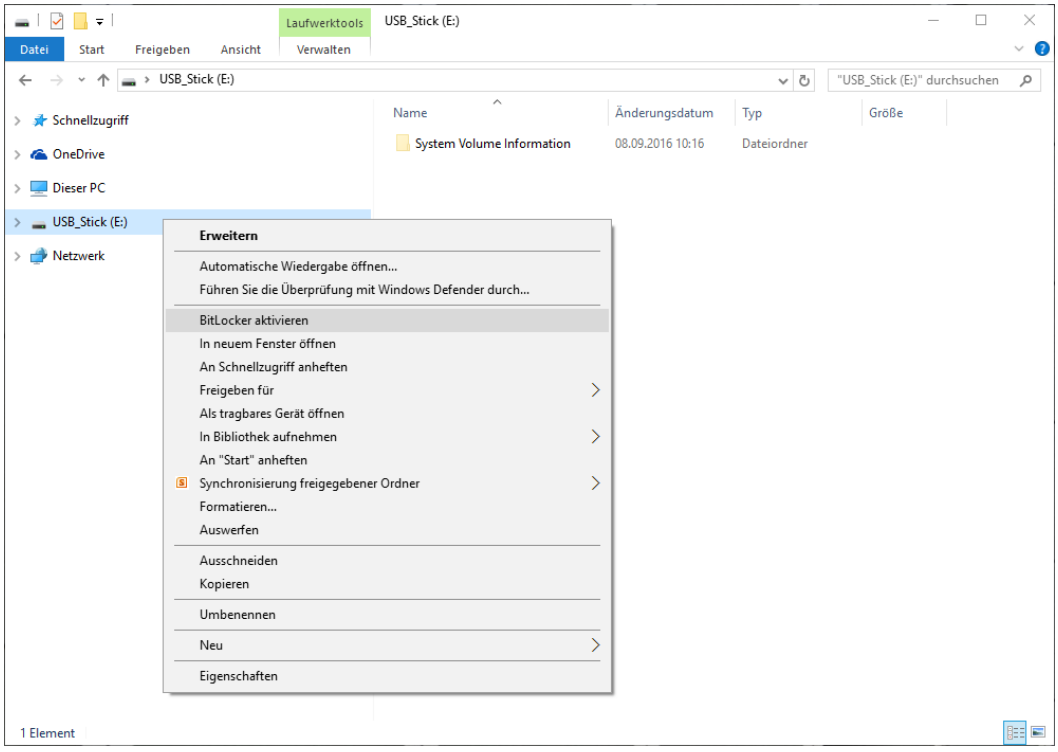
Hinweise

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

Während des Verschlüsselungsvorgangs kann normal weitergearbeitet werden.



Die BitLocker-Verwaltung ist im Kontextmenü eines Laufwerks zugänglich.



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

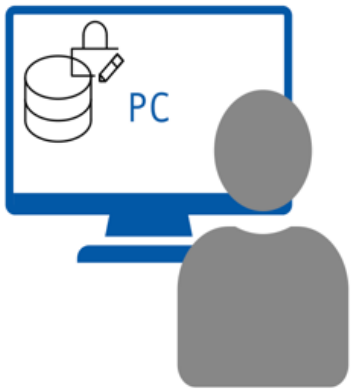
Prüfung des Verschlüsselungsfortschritts per PowerShell oder administrativer Eingabeaufforderung

```
manage-bde -status Laufwerksbuchstabe
```

LABORÜBUNG 18 - FESTPLATTENVERSCHLÜSSELUNG MIT BITLOCKER

Szenario

Auf Ihrem Dienstrechner soll die Festplatte mit BitLocker verschlüsselt werden.



Aufgaben

1. Stellen Sie fest, ob bei Ihrem Gerät UEFI Secure Boot aktiviert ist und ob ihr Gerät über ein TPM verfügt.
2. Kontrollieren Sie, ob BitLocker bereits aktiv ist.
3. Verschlüsseln Sie an Ihrem Desktop-PC die Festplatte mit BitLocker. Notieren Sie sich das Kennwort und drucken Sie den Wiederherstellungsschlüssel aus.
4. Testen Sie die Festplattenverschlüsselung.

Weiterführende Aufgaben

5. Verschlüsseln Sie die Festplatte mit Veracrypt und testen Sie die Funktionsfähigkeit!

Hinweise

UEFI Secure Boot

Secure Boot stellt sicher, dass während des Startprozesses nur solche Programme, die mit einem dem Mainboard bekannten Schlüssel signiert sind, gestartet werden.

Trusted Platform Module (TPM)

Dabei handelt es sich um einen Chip, der grundlegende Verschlüsselungsfunktionen zur Verfügung stellt, das Gerät mit einem Key eindeutig identifiziert und einen Speicher zur sicheren Verwahrung der Schlüssel zur Verfügung stellt.

Bitlocker speichert im TPM-Chip den Verschlüsselungs-Key. Solange Windows direkt vom Gerät gestartet wird, gelingt der direkte Zugriff auf das BitLocker-Dateisystem ohne Passworteingabe.

Alternativen zu BitLocker

Veracrypt

Die Open-Source Software steht für alle gängigen Desktopbetriebssystem zum Download bereit. Mit ihr können sowohl externe Speichergeräte als auch interne Speicher vollständig verschlüsselt werden. Zudem können versteckte Container erstellt werden. Eine ausführliche Beschreibung findet sich unter https://schulnetz.alp.dillingen.de/materialien/Veracrypt.pdf.

Cryptomator

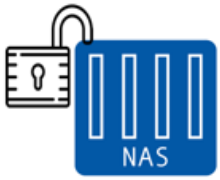
Es handelt sich hierbei um ein Dateiverschlüsselungstool für die Speicherung von Dateien in der Cloud. Für Windows, MacOS und Linux ist die Software kostenlos erhältlich. Cryptomator verwendet Vaults (Tresore) zur verschlüsselten Ablage von Dateien und Verzeichnisse. Die Verbindung zur Cloud entsteht, indem man das Verzeichnis für die Vault-Datei vor der Speicherung mit einem Cloud-Anbieter verbindet. Das entsprechende virtuelle Laufwerk kann bei OneDrive und iCloud mit den im jeweiligen Betriebssystem integrierten Clients direkt gestartet werden.

Eine Verschlüsselung von ganzen Festplatten ist nicht möglich.

LABORÜBUNG 19 - VERSCHLÜSSELN VON DATEN AUF EINEM NAS-SYSTEM

Szenario

Um die Daten auf einem NAS-System bei einem eventuellen Diebstahl des NAS-Systems zu schützen, sollen diese in einer verschlüsselten Freigabe auf dem NAS-System abgelegt werden. Bei einem Neustart des NAS-Systems bzw. beim Zugriff auf die Freigabe muss erst ein Passwort eingegeben werden, damit auf die verschlüsselten Daten zugegriffen werden kann.



Aufgaben

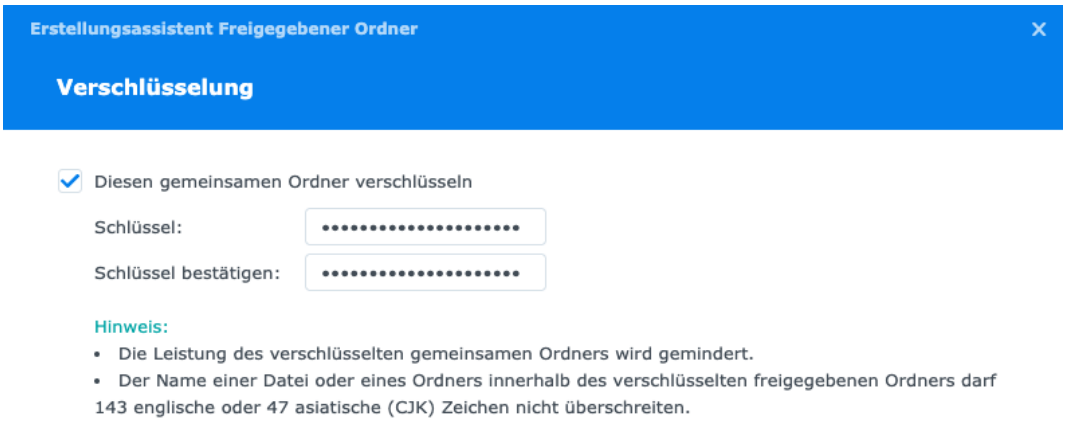
1. Erstellen Sie auf dem NAS-System eine neue verschlüsselte Freigabe. Der Verschlüsselungsschlüssel soll bei der Erstellung nicht auf dem NAS-System gespeichert werden.
2. Passen Sie die Rechte für den Zugriff auf die Freigabe so an, dass nur berechtigte Personen Zugriff haben.
3. Greifen Sie von einem PC auf die Freigabe zu und speichern Sie einige Testdaten darauf.

Hinweise

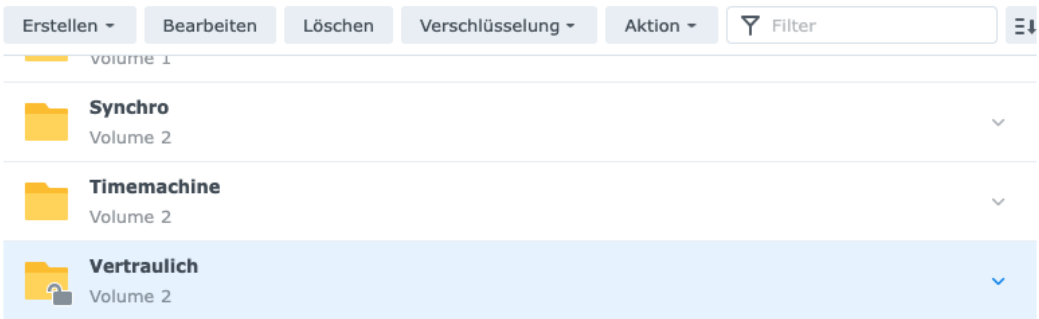
Synology-NAS mit Verschlüsselung

Bei der Erstellung von Freigaben oder später in deren Eigenschaften steht der Menüpunkt Verschlüsselung zur Verfügung. Synology-NAS-Systeme verschlüsseln nicht die komplette Festplatte, sondern beim Erstellen von neuen Freigaben kann festgelegt werden, dass das System einzelne Freigaben verschlüsseln soll. Die Verschlüsselung freigegebener Verzeichnisse kann bei der Erstellung vorgenommen werden, aber auch jederzeit nachträglich.

Sind die Schlüssel für ein verschlüsseltes Objekt nicht mehr bekannt, kann niemand mehr auf die Daten zugreifen: Ohne den Schlüssel ist kein Zugriff auf die Daten mehr möglich. Für die Verschlüsselung von Synology-NAS-Systemen wird auf dem NAS der **Schlüsselmanager** von Synology benötigt. Hier kann zum Beispiel ein externer USB-Stick angebunden werden. Auf diesem lassen sich die Schlüssel zur Verschlüsselung sichern. Der Zugriff auf die Daten im Schlüsselmanager wird ebenfalls über ein Kennwort verschlüsselt.



Verschlüsseltes und freigegebenes Verzeichnis: Für den Zugriff auf das Verzeichnis benötigt man sowohl Zugriffsberechtigung (Credentials für die Freigabe) als auch den Verschlüsselungsschlüssel.



MEDIENEINSATZ

Um digitale Medien im Unterricht einsetzen zu können, benötigen Lehrkräfte grundlegende eigene Kompetenzen im Umgang mit diesen Medien und darüber hinaus Handlungskompetenzen, um den Unterricht mit digitalen Medien realisieren zu können.

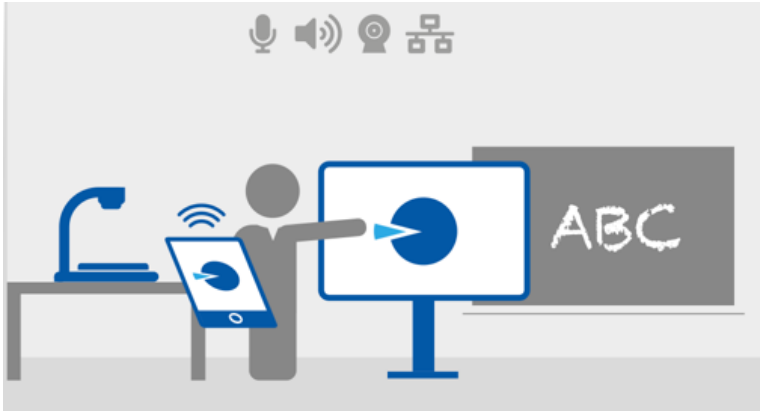
Dazu gehören z. B.

- der routinierte Umgang mit unterrichtsspezifischen digitalen Medien (derzeit z. B. Umgang mit Dokumentenkamera, Tablet, interaktives Whiteboard)
- unterrichtsspezifische Handlungskompetenzen im Umgang mit digitalen Medien (derzeit z. B. Begleitung des Unterrichts mit Lernplattformen, Einsatz ggf. Erstellung von Erklär-Videos, Austausch von digitalen Materialien mit allen Schülern, Umgang mit Cloud-Diensten)
- Handlungskompetenzen beim fachspezifischen Einsatz digitaler Medien (derzeit z. B. Computer-Algebra-Systeme im Mathematikunterricht, Grafikprogramme im Kunstunterricht, Audio-Programme im Fremdsprachenunterricht, Simulationsprogramme im naturwissenschaftlichen Unterricht)

LABORÜBUNG 20 - DRAHTLOSE BILDÜBERTRAGUNG AUF EINEN BEAMER

Szenario

Der Bildschirminhalt und der Ton eines Tablets oder Smartphones soll auf eine Großbilddarstellung drahtlos übertragen werden.



Aufgaben

1. Informieren Sie sich über die verschiedenen Möglichkeiten zur Bildschirmspiegelung (Hardware vs. Software) und deren technische Anforderungen an das mobile Endgerät.
2. Stellen Sie den Bildschirminhalt Ihres Notebooks, Tablet oder Smartphone am Beamer bzw. der zur Verfügung stehenden Großbilddarstellung dar.
3. Öffnen Sie mit Ihrem Mobilgerät gleichzeitig eine WLAN-Verbindung ins Hausnetz bzw. ins Internet.
4. Übertragen Sie ein Video, das Sie live über das Internet beziehen, mit Bild und Ton auf den Beamer.
5. Entwerfen Sie für Ihre Schule ein Konzept zur Sicherstellung der mobilen Bildschirmübertragung in allen Klassenzimmern.
    - Welche Lösung soll bevorzugt werden? (Hardware oder Softwarelösung)
    - Erfüllen alle eingesetzten Geräte die entsprechenden Voraussetzungen? (z. B. WiFi-Schnittstelle?)
    - Abschätzung der finanziellen Kosten und des personellen Aufwands bei der Einrichtung
    - Wer könnte bei der Einrichtung unterstützen? (Medienteams, Medientutoren ...)
    - Erstellung eines Konzepts zur Schulung des Kollegiums

HINWEISE

Der Optimalfall wäre eine möglichst einfach zu bedienende und komfortable Lösung mit Unterstützung aller gängigen Übertragungstechnologien (AirPlay, Miracast und Chromecast). Dadurch können auch schülereigene und lehrereigene Geräte ohne Probleme in den Unterricht eingebunden werden.

Bevor man sich für eine zentrale Lösung entscheidet, sollte an der Schule ein ausgiebiger Test der angestrebten Lösung mit verschiedenen Lehrkräften stattfinden.

Die drahtlose Bildschirmübertragung kann über Hardware-Lösungen und Software-Lösungen realisiert werden. In jedem Fall ist eine WiFi-Schnittstelle am mobilen Endgerät notwendige Voraussetzung.

Soll auch an stationären PCs die Möglichkeit zur drahtlosen Bildschirmübertragung eingerichtet werden, muss ggf. ein WLAN-Stick beschafft werden, sofern keine integrierte Schnittstelle vorhanden ist.

Wichtige Auflösungen für die Schule:

4k UHD	4k Ultra High Definition - Bildschirmauflösung 3840 x 2160 Pixel, Seitenverhältnis 16:9, 2160p
WQHD	Wide Quad High Definition - Bildschirmauflösung 2560 x 1440 Pixel, Seitenverhältnis 16:9, 1440p
Full HD	Full High Definition - Bildschirmauflösung 1920 × 1080 Pixel, Seitenverhältnis 16:9, 1080p
HD	High Definition - Bildschirmauflösung 1280 x 720 Pixel, Seitenverhältnis 16:9, 720p

VORHERSCHENDE ANSCHLÜSSE ZUR BILDÜBERTRAGUNG

An den verschiedenen Präsentationsmedien muss ein Hardware-Adapter vorhanden sein oder installiert werden. Bei kabelgestützten Verbindungen müssen Herstellerangaben berücksichtigt werden, da meist nicht alle Möglichkeiten der Übertragungsstandards vollständig implementiert werden.

Video Graphics Array (VGA)

Mit einem VGA-Anschluss sind Auflösungen bis 1920 x 1080 Pixel (Full-HD) möglich. Jedoch kann kein Bild übertragen werden. Zudem ist das analoge Videosignal störanfällig.

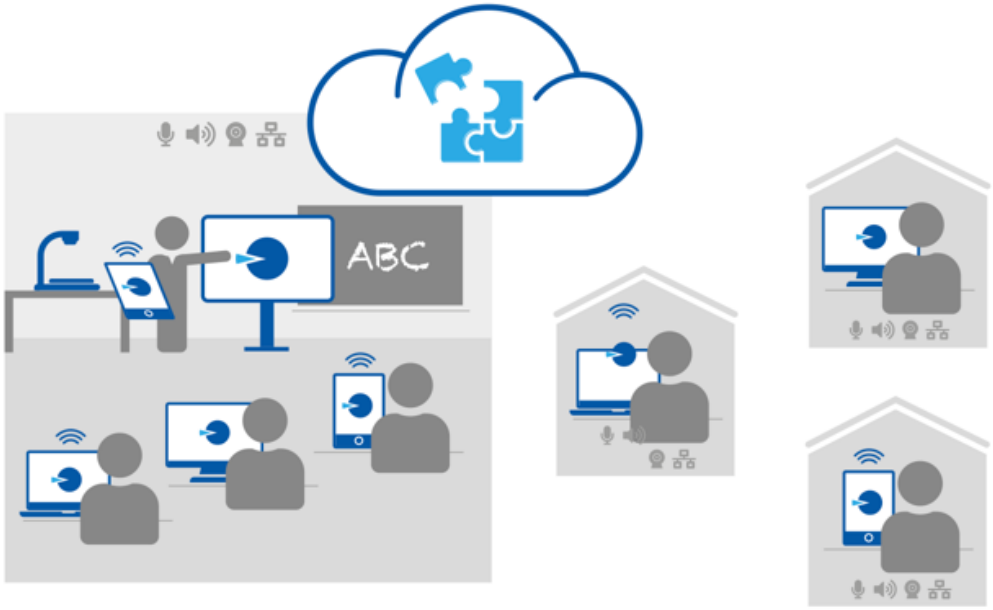
High-Definition Multimedia Interface (HDMI)

Es handelt sich im Gegensatz zu VGA um eine digitale Schnittstelle. HDMI kann Bild und Ton übertragen und ist bis 8k (7680 x 4320 Pixel) spezifiziert. Durch die gleichzeitige Übertragung von Bild und Ton, kann das Ausgabegerät als Sound-Hub dienen und das Signal an angeschlossene Boxen weiterreichen.

LABORÜBUNG 21 - EINBINDUNG VON MOBILEN ENDGERÄTEN IN VIDEOKONFERNZLÖSUNGEN

Szenario

Im Distanzunterricht wollen Sie den Bildschirm Ihres mobilen Endgeräts freigeben. Schüler im Distanz - und Präsenzunterricht sollen teilnehmen.



Aufgaben

1. Starten Sie eine Videokonferenz mit dem Tool Ihrer Wahl!
2. Stellen Sie den Bildschirminhalt Ihres Notebooks, Tablets oder Smartphone innerhalb einer Videokonferenz dar, die sie über den Webbrowser erstellt haben.

HINWEISE

Alle Videokonferenzlösungen bieten die Möglichkeit über den Browser per Link beizutreten. Einige Anbieter ermöglichen zusätzlich die Möglichkeit des Beitritts über eine App, die weitere Funktionalität bietet und dem Browserbeitritt vorgezogen werden sollte.

EINBINDUNG VON TABLETS (IPAD ODER ANDROID) PER BROWSER

Tritt man einer Videokonferenz über den Browser bei und möchte seinen Bildschirm freigeben, ist man darauf angewiesen, dass der Hardwarehersteller den Zugriff auf den Bildschirm über das WebRTC-Protokoll zulässt. Das ist bei Apple oder Android-Tablets nicht der Fall, weswegen eine Bildschirmfreigabe per Browser hier nicht ohne weiteres möglich ist. Auf einem Tablet bietet eine App mehr Möglichkeiten als die browsergestützte Verbindung.

Kabelgebundenes Spiegeln eines iPad-Bildschirms auf einen Mac

Um den Bildschirm eines iPad für Videokonferenzen per Browser freizugeben, müssen Sie das Tablet zunächst physisch mit dem Hauptrechner verbinden. Am Mac brauchen Sie dafür einen USB auf Lightning Adapter oder direkt ein USB-C-Kabel zur Verbindung des Macs und des iPads. Spiegeln Sie den Bildschirminhalt des iPad über die Funktion *Sidecar* auf den Mac-Desktop. Ältere iPads verfügen nicht über diese Funktion. Hier kann das iPad anders eingebunden werden, indem Sie im QuickTime-Player im Ablage-Menü „Neue Filmaufnahme“ auswählen und aktivieren dort über das kleine Dreieck neben dem Aufnahme-Button statt der Kamera das iPad.

Kabelgebundenes Spiegeln eines iPad-Bildschirms auf einen Windows-PC

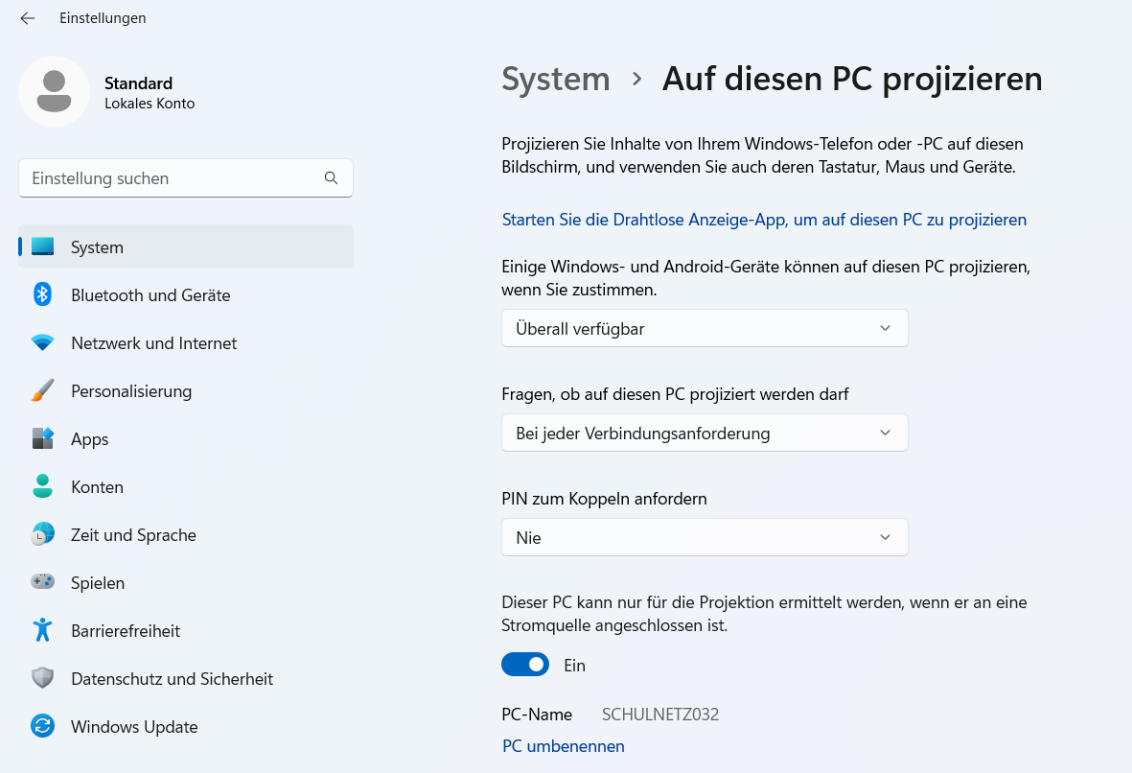
Am Windows-PC können Sie über einen HDMI-Grabber und ein USB-C auf HDMI-Kabel das Bild des iPads auf den Windows-PC einspeisen und über die Kamera-App in den Videostream einbinden.

Softwaregebundenes Spiegeln eines Tablet-Bildschirms

Alternativ kann auch eine Software-Lösung zur Bildschirmspiegelung, wie AirServer, eingesetzt werden, um das Gerät auf einen weiteren Rechner zu spiegeln. Beide Geräte müssen dazu im WLAN sein.

Drahtloses Projizieren auf einen Windows-Rechner

Windows 10/11 bietet die Möglichkeit, dass das Gerät als digitales Wiedergabegerät verwendet werden. Dazu muss das optionale Feature *Drahtlose Anzeige* installiert werden. Anschließend kann der Windows-Gerät zum Spiegeln von Windows- und Android-Geräten verwendet werden.

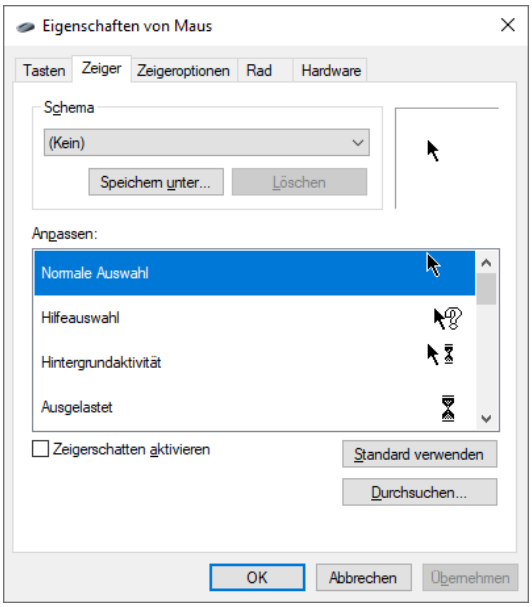


WEITERE TIPPS FÜR VIDEOKONFERENZEN

Microsoft bietet seit einiger Zeit *Power Toys* für Windows 10 an. Ein enthaltenes Tool ist Video Conference Mute, mit dem per Hotkey Videokamera und Mikrofon gesteuert werden können. Immer mehr Videokonferenzlösungen bieten in ihren Apps ebenfalls ähnliche Funktionalitäten. Video Conference Mute verhindert aber den Ausfall der Kamera im Problemfall (Absturz einer Anwendung oder eines Einstellungsdialogs) bis zum Reset.

Für eine bessere Soundqualität bieten sich Headsets oder USB-Mikrofone an. Eine externe Webcam bietet eine höhere Auflösung (i. d. R. mind. Full HD) im Vergleich zu integrierten Webcams (i. d. R. HD).

Der Mauszeiger kann nach den eigenen Bedürfnissen verändert werden, damit dieser besser sichtbar ist. Unter http://www.rw-designer.com/ können verschiedene, benutzerdefinierte Mauszeiger ausgewählt und anschließend unter *Mauseinstellungen* verändert werden.



Visavid

Kostenlose browserbasierte Videokonferenzlösung des Staatsministeriums für Unterricht und Kultus. weitere Informationen über die Funktionen der Software findet sich unter https://visavid.de/downloads/. Inzwischen gibt es für mobile Endgeräte entsprechende Apps, die genutzt werden können und bspw. eine Bildschirmfreigabe ermöglichen

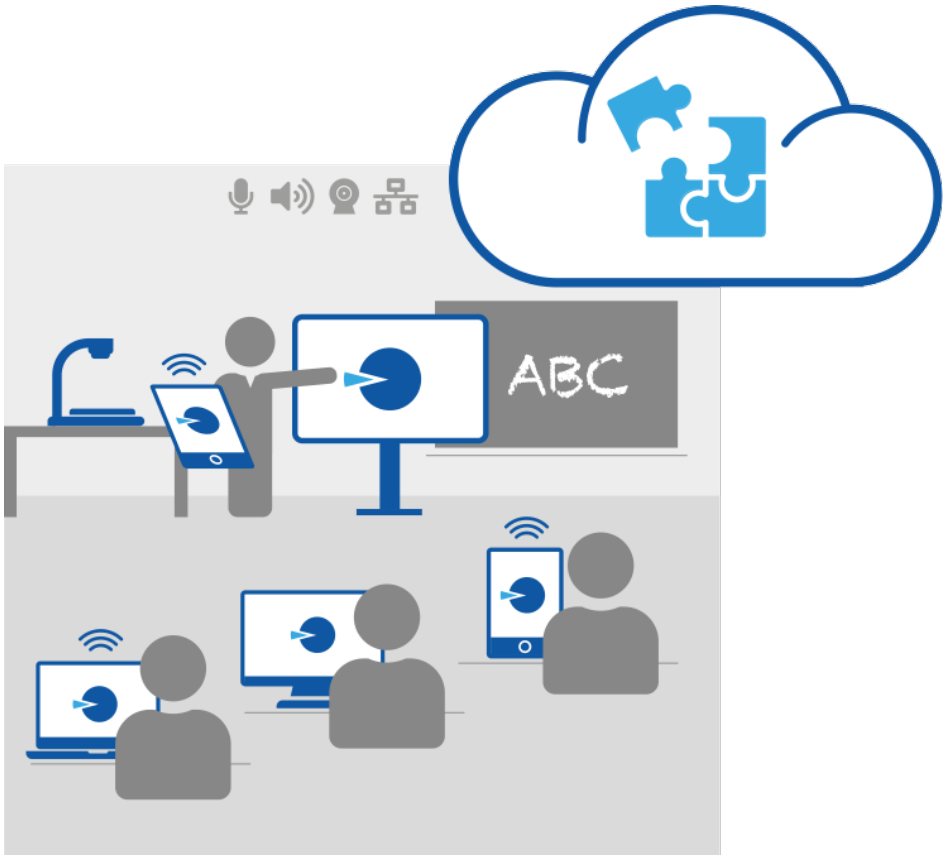
MS-Teams

Video- und Kollaborationslösung von Microsoft. Hier können sowohl im Browser als auch per App Videokonferenzen durchgeführt werden. Es können auch Besprechungen über den Kalender geplant werden. Eine Bildschirmfreigabe in der App ist mit dem iPad möglich.

LABORÜBUNG 22 - ARBEITEN MIT ONLINE-WERKZEUGEN FÜR DEN UNTERRICHT

Szenario

Im „Digitalen Klassenzimmer“ steht allen Schülern und ein Tablet oder Smartphone zur Verfügung, das über WLAN in das Unterrichtsnetz eingebunden ist.



Aufgaben

1. Testen Sie verschiedene Online-Werkzeuge hinsichtlich eines möglichen Unterrichtseinsatzes.
2. Informieren Sie sich – soweit möglich – über jeweilige Nutzungs- und Lizenzbedingungen. Reflektieren Sie jeweils die Eignung für den Schuleinsatz unter anderem auch aus rechtlicher Sicht (z. B. Werbeverbot, Datenschutz, Vertragsbeziehungen).

Beispiele für interaktive Online-Werkzeuge

LearningApps

https://www.learningapps.org
Kleine webbasierte interaktive Lernbausteine, die ohne Registrierung genutzt werden können. Das Erstellen, Speichern und Verwalten eigener Lernbausteine benötigt eine Registrierung.

Geogebra

https://www.geogebra.org

Interaktive Lernumgebung aus dem Bereich der Mathematik.

Kahoot

https://kahoot.com -> Einstieg für Lehrer, Registrierung ist erforderlich.

https://kahoot.it -> Einstieg für Schüler, ohne Registrierung.

Spielebasierte Lernplattform, auch für Umfragen geeignet.

Schlaukopf

https://www.schlaukopf.de

Eine Lernplattform für alle Schularten und viele Fächer, welche Quizze zu den verschiedensten Themen anbietet. Die Plattform ist kostenlos und kann ohne Registrierung genutzt werden.

Anton

http://www.anton.app

Interaktive Übungen zu Deutsch, Mathematik, Sachunterricht, Musik und DaZ.

Aufgabenfuchs

https://www.aufgabenfuchs.de

Interaktive Übungen zu Erdkunde, Geschichte und Mathematik.

Worksheet Go

https://worksheetcrafter.com

Worksheet Go! ist die interaktive Ergänzung zum Worksheet Crafter (im App-Store erhältlich).

Coollama

https://coollama.de

Interaktive Übungen in Mathematik im Grundschulbereich.

Klötzchen

https://dlgs.uni-potsdam.de

Mit der Klötzchen-App können verschiedene Darstellungen (realistische Abbildung, Bauplan, Zweitafelbild, isometrische Darstellung, Schrägbild) nebeneinander betrachtet werden.

Onilo

https://www.onilo.de/

Mit Onilo wird der Leseprozess durch sukzessiv eingeblendeten Text und sparsame, aber fokussierende Animationen, die das Text-, Lese- und Hörverständnis unterstützen, zielführend begleitet. (Grundschule, kostenpflichtig)

Geoboard

https://www.mathlearningcenter.org/apps

Online-Übungen für geometrische Formen (Grundschulbereich)

Beispiele für Kollaborationswerkzeuge

Padlet

https://de.padlet.com

Digitale Pinnwand, welche die Zusammenarbeit über das Internet ermöglicht. Für die Erstellung von Padlets ist eine Registrierung der Lehrkraft notwendig. Eine etwas eingeschränkte Grundfunktion gibt es kostenlos, jedoch mit Werbung.

TaskCards

https://www.taskcards.de/

Digitale Pinnwand, die wie Padlet funktioniert. Um die digitale Pinnwand nutzen zu können, muss eine Lizenz durch die Lehrkraft beantragt werden. Die Nutzung ist im aktuellen Beta-Status kostenlos.

Answergarden

http://www.answergarden.ch

Ein Tool zum gemeinsamen Erstellen einer Ideensammlung.

Plickers

https://www.plickers.com

Ein Umfragetool, bei dem nur der Lehrer ein digitales Endgerät benötigt. Zum Erstellen einer Umfrage ist eine Registrierung notwendig.

Etherpad

https://etherpad.alp.dillingen.de -> Etherpad sofort nutzbar

https://etherpad.org -> Etherpad zum herunterladen

Etherpad ist ein webbasierter Editor zur gemeinsamen Bearbeitung von Texten. Es kann eine fertige Version im Netz verwendet werden oder auf einem eigenen Server installiert werden.

Twine

http://twinery.org

Interaktive Geschichten, Tutorials, Spiele oder Gedichte schreiben.

Digiboard

https://digiboard.app/

Browserbasiertes Whiteboard für interaktives Arbeiten (auf der Seite https://ladigitale.dev/ werden noch weitere Tools angeboten)

Newstest

https://der-newstest.de/

In einem digitalen Selbsttest können die Fähigkeiten im Umgang mit Nachrichten im Internet getestet werden.

Kits

https://kits.blog/

Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung

Kostenfreie browserbasierte Tools für kollaboratives Arbeiten im Unterricht

HINWEISE

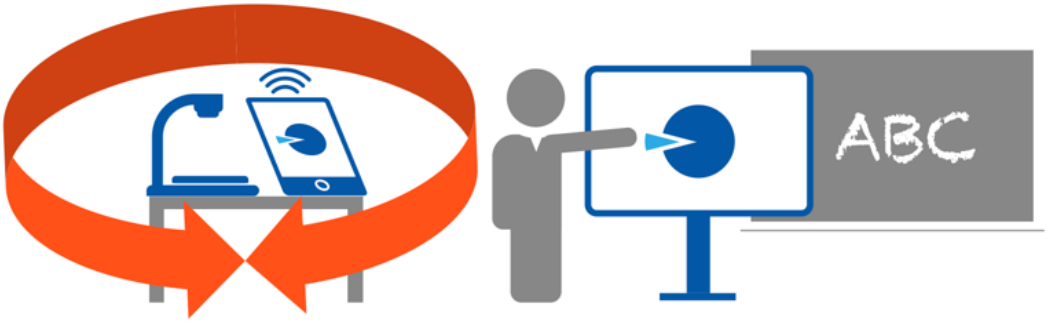
Bei dem Einsatz von Apps im Unterricht ist darauf zu achten, dass die geltenden Datenschutzbestimmungen eingehalten werden. Es ist zu prüfen, inwieweit Daten an Drittanbieter weitergegeben werden und ob eine vertragliche Verpflichtungen seitens der Schüler eingegangen wird. Im Rahmen der Fortbildungsoffensive wurde im Modul Digitalisierung, Schule und Recht eine Checkliste zum Einsatz von Apps im Unterricht veröffentlicht.

https://fortbildungsoffensive.alp.dillingen.de/downloads/digitalisierung_recht/pdf/praxis_apps.pdf

LABORÜBUNG 23 - DIE DOKUMENTENKAMERA UND DAS TABLET ALS OHP-ERSATZ

Szenario

Die im Unterricht mit Schülern unter der Dokumentenkamera erarbeiteten Ergebnisse sollen digital gespeichert werden, um sie den Schülern zur Verfügung zu stellen. In Schulen wird zunehmend das Tablet als Ersatz für die Dokumentenkamera eingesetzt. Es gibt inzwischen spezielle Vorrichtungen, in die das Tablet gelegt werden kann und so als Ersatz für die Dokumentenkamera dienen.



Aufgaben

Übung an der Dokumentenkamera:

1. Identifizieren Sie die Schnittstellen und Bedienmöglichkeiten der Dokumentenkamera. Untersuchen Sie, ob die Dokumentenkamera auch ohne PC genutzt werden kann.
2. Präsentieren Sie unterschiedliche Vorlagen mit der Dokumentenkamera am Beamer oder am Großbildmonitor (z. B. Textvorlagen mit unterschiedlicher Schriftgröße, räumliche Gegenstände, Tablet oder Smartphone). Experimentieren Sie mit dem Zoom und der externen Beleuchtung.
3. Schließen Sie ein Speichermedium (USB-Stick im Format **FAT32**) an der Dokumentenkamera an. Nehmen Sie mit der Fototaste ein Foto auf und betrachten Sie dieses anschließend am PC.
4. Installieren Sie die passende Software zur Dokumentenkamera und schließen Sie die Dokumentenkamera am PC an. Welche zusätzlichen Möglichkeiten bietet die Software?
5. Nehmen Sie mit der Dokumentenkamera ein kurzes Video auf und spielen Sie es über den Beamer ab.

Übung am Tablet:

1. Öffnen Sie eine Whiteboard-Software Ihrer Wahl auf dem Tablet und entwerfen Sie ein Tafelbild. Stellen Sie die Tafelbilder allen Schülern zur Verfügung, z. B. über die Lernplattform mebis, NAS-System oder Cloud-Lösung.
2. Vergleichen Sie die Möglichkeiten der Dokumentenkamera mit den Möglichkeiten eines Tablets als Dokumentenkameraersatz.

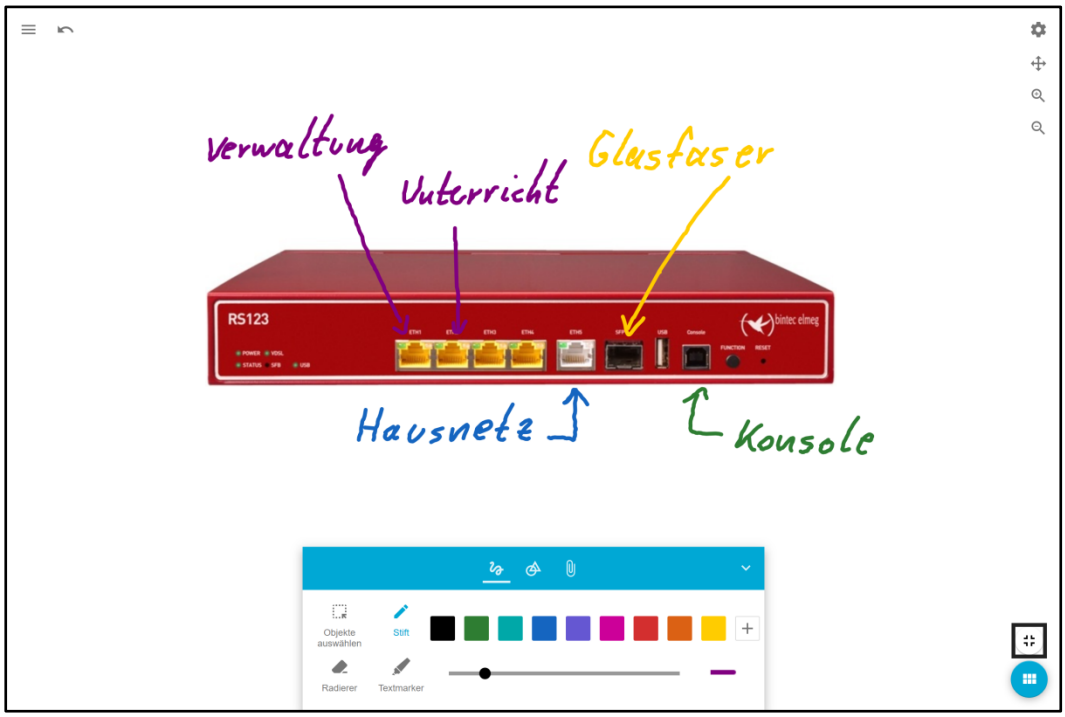
mebis-Tafel

Innerhalb von mebis wird mit der mebis-Tafel ein Werkzeug bereitgestellt, das als browserbasierte Tafelsoftware mit jedem Endgerät mit einem aktuellen Browser verwendet werden kann:

https://tafel.mebis.bayern.de

Um die mebis Tafelsoftware auch ohne Internetverbindung nutzen zu können, stehen für Windows und MacOS Installationsdateien zur Verfügung.

Weitere Informationen zur Verwendung der mebis Tafel findet man im mebis Infoportal unter https://www.mebis.bayern.de/infoportal/kategorie/tafel/

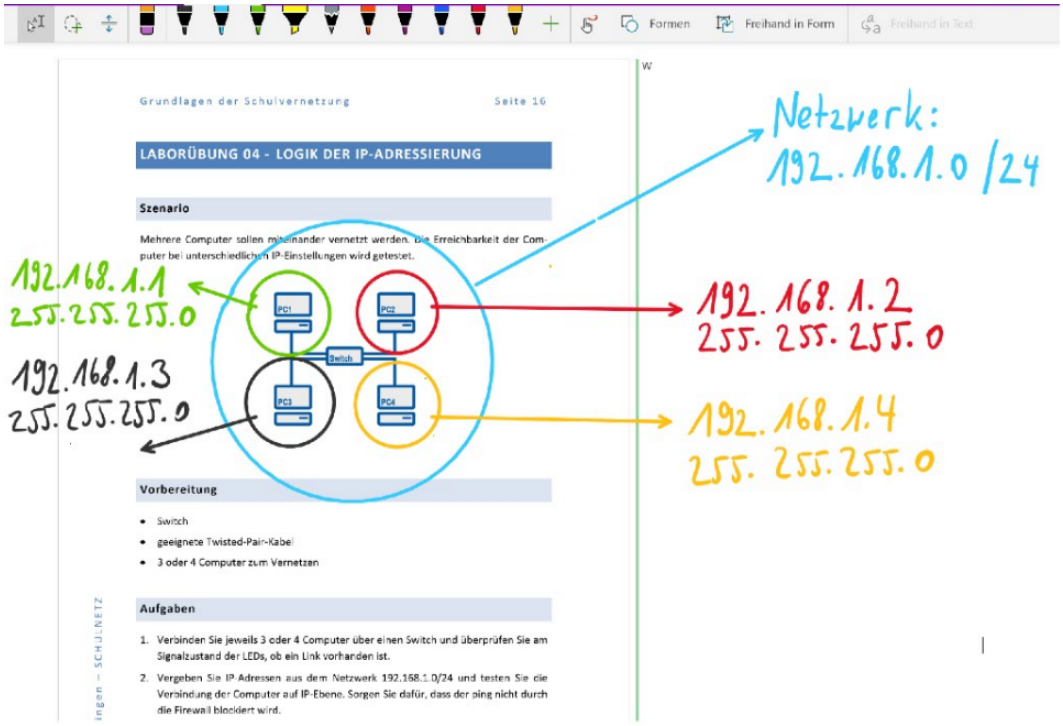


OneNote

Microsoft stellt das Produkt OneNote in folgenden Varianten zur Verfügung:

- OneNote Desktop-App (enthalten in Office 2016)
- OneNote Store-App (im Umfang von Windows 10/11 enthalten)
- OneNote Online-Version
- App für mobile Endgeräte

One-Note wird häufig in Verbindung mit OneDrive verwendet. Dazu ist ein Microsoft-Konto erforderlich.



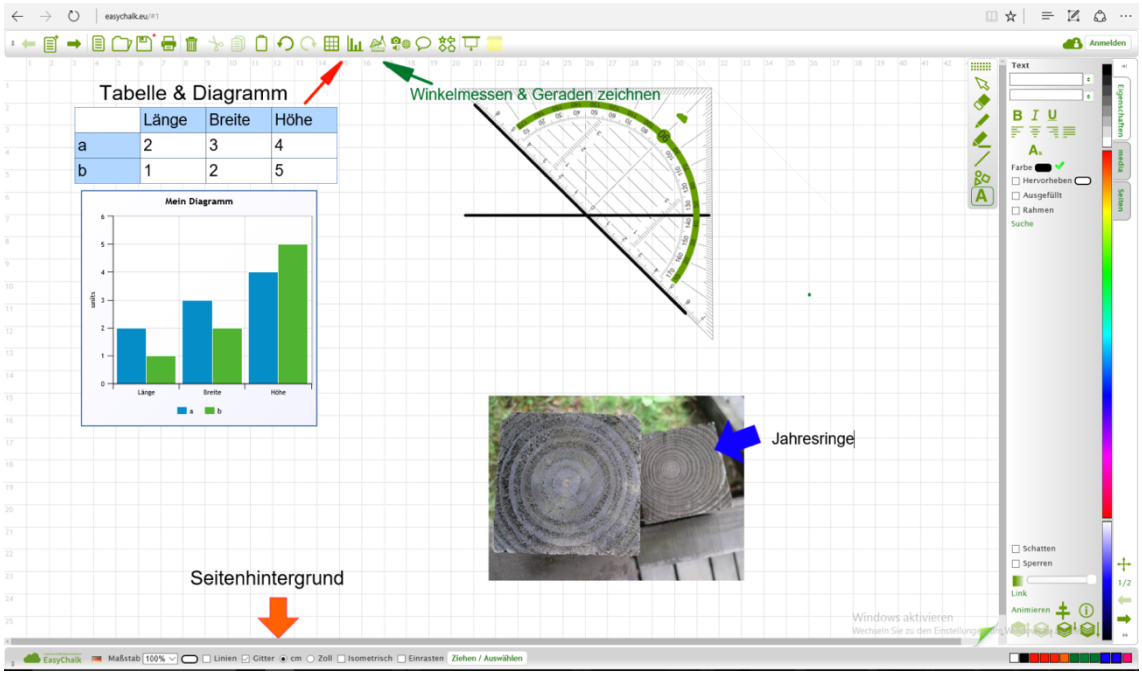
Microsoft Whiteboard

Das Microsoft Whiteboard ist Teil von Office 365 und kann standardmäßig bereits im A1 Plan genutzt werden.

EasyChalk

https://www.easychalk.eu

EasyChalk ist eine Online-Whiteboard-Software, die im Browser läuft. Bei der Nutzung fallen jährliche Lizenzgebühren an. In der kostenlosen Demo-Version können keine Tafelbilder gespeichert werden, eine Registrierung ist erforderlich.



Whiteboard Chat

https://www.whiteboard.chat/

Es handelt sich hierbei auch um ein Whiteboard, das im Browser läuft. Möchte man das Whiteboard sichern, ist eine Registrierung erforderlich.

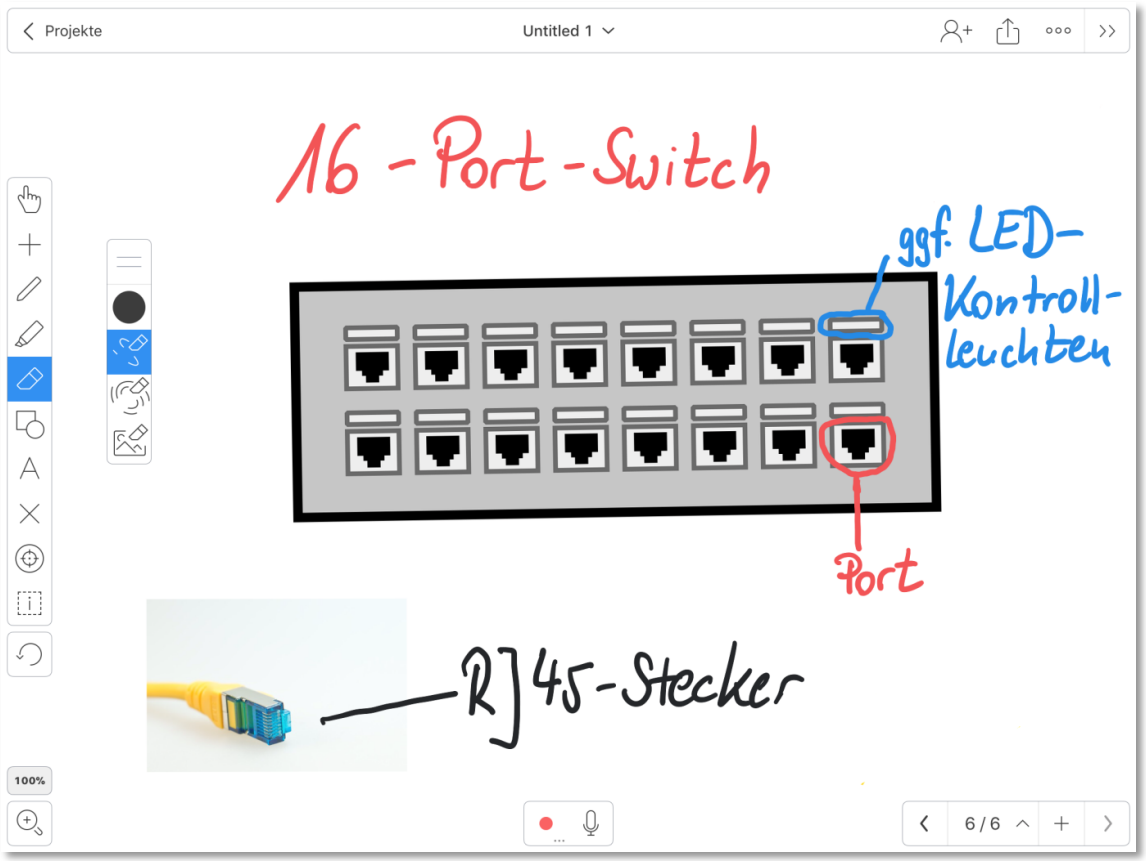
Explain-Everything

Explain Everything gibt es als App für iOS und mit einem etwas eingeschränkten Funktionsumfang auch für Android und Windows 10/11. Unter iOS ist es z. B. möglich, gemeinsam an einem Projekt zu arbeiten.

Ein Formeleditor ermöglicht den Einsatz in Mathematik oder Physik. Explain-Everything unterstützt auch das Schreiben mit Stift und Handballenerkennung.

Videos können je nach Gerät beim Abspielen beschriftet und erklärt werden, auch in einer Unterbrechungspause. Das Video kann beim Abspielen vergrößert, verkleinert oder auch gedreht werden. Ebenso kann man Webseiten so weit vorbereiten, dass Inhalte im Unterricht direkt genutzt werden können.

Bei der Nutzung fallen jährliche Lizenzgebühren an. Für Schulen gibt es die Möglichkeit eine EDU-Lizenz zu erwerben, bei der nur einmalige Kosten anfallen.

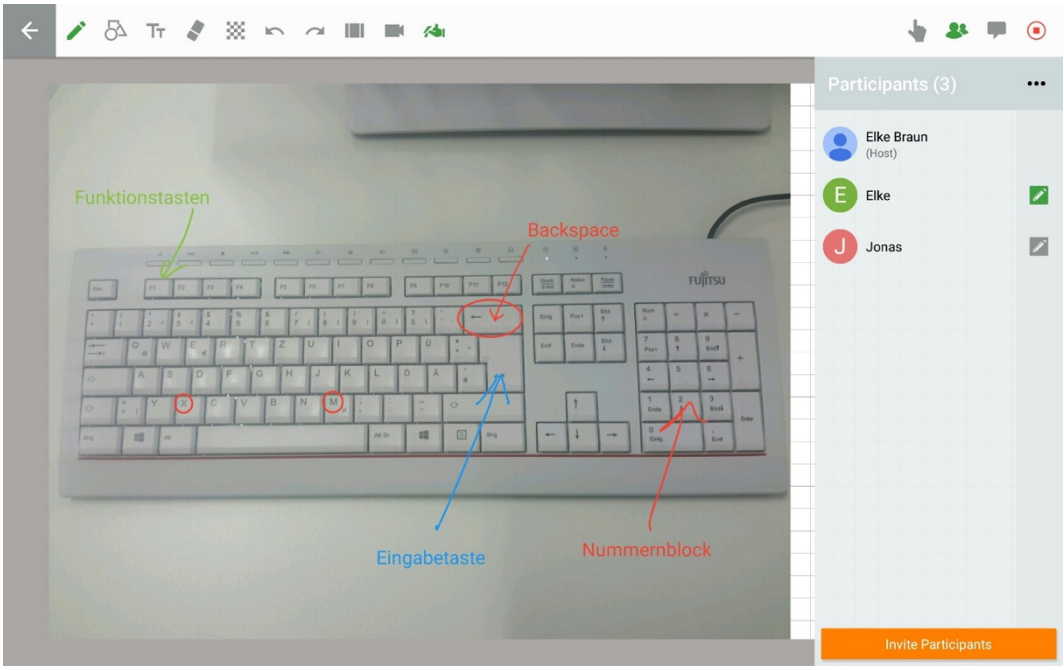


Live Board

Die kostenlose App LiveBoard gibt es für Android, iOS und Windows.

https://liveboard.online.

Sie ermöglicht es mehrere User einzuladen, um an einer digitalen Tafel gemeinsam ein Tafelbild zu erstellen. Dabei werden die Veränderungen, die an einem Gerät durchgeführt werden, zeitgleich auf allen anderen eingeladenen Geräten angezeigt. Der Ersteller kann dabei entscheiden, ob die Teilnehmer bearbeiten können oder nur zusehen dürfen. Der Verlauf der Unterrichtseinheit kann mitgeschnitten und als mp4-Datei gespeichert werden. Die Handauflage beim Schreiben wird erkannt.



Es ist möglich nebenbei in einem Chat Fragen zu stellen oder mit einem virtuellen Finger etwas an der Tafel zu zeigen.

Classroomscreen

https://classroomscreen.com

Dieses Tool ist einfach zu bedienen. Neben vielen bekannten Funktionen (Zeichnungen, Text) sticht der schnelle QR-Code-Generator hervor. Einfach die gewünschte Adresse eingeben und ein QR-Code wird erstellt, den die Schüler oder die Teilnehmer einer Fortbildung nutzen können. Daneben gibt es weitere hilfreiche Tools wie Timer, Arbeitssymbole, aber auch die Möglichkeit die Lautstärke zu messen und ein kurzes Feedback schnell abzufragen.

Die Classroomscreen Funktionen findet man nach dem Öffnen der Seite unten aufgereiht.

LABORÜBUNG 24 - SUCHMASCHINEN FÜR DEN UNTERRICHTSEINSATZ

Szenario

In Ihrem Kollegium werden verstärkt Internetrecherchen durchgeführt. Dabei soll aber auf den Datenschutz und auf angemessene Suchergebnisse wert gelegt werden.

Aufgaben

1. Informieren Sie sich über die verschiedenen Suchmaschinen, die zur Verfügung stehen.
2. Untersuchen Sie die Suchmaschinen hinsichtlich Datenschutzes, Auswahl der Suchergebnisse und Jugendschutzfilter.
3. Entwerfen Sie eine SchiLF für Ihr Kollegium, in dem Sie die ausgewählte Suchmaschine vorstellen.

HINWEISE

Google Search hat sich als Standard unter den Suchmaschinen etabliert. Problematisch ist hier jedoch das Tracking der Benutzereingaben und die bevorzugte Anzeige von bezahlten Inhalten als Treffer einer Suche. Jedoch gibt es verschiedene Alternativen, die teilweise bessere Ergebnisse liefern als Google Search.

Google Search

Technisch gesehen funktioniert die Google Suche hervorragend, schnell und liefert passende Ergebnisse, bietet viel Komfort und praktische Zusatzfunktionen. Google sammelt aus vielen Quellen Nutzerdaten, um sie für personalisierte Werbung einzusetzen. Unter den Suchergebnissen finden sich ganz oben Werbeanzeigen.

Die Google Suche bietet die Möglichkeit anstößige Ergebnisse mit Hilfe von SafeSearch auszublenden. Zudem können die Ergebnisse nach Nutzungsrechten gefiltert werden, um das Urheberrecht zu wahren.

DuckDuckGo

DuckDuckGo punktet vor allem damit, dass die Daten nicht gespeichert oder an Dritte weiterverkauft werden. Der Datenschutz steht an erster Stelle. Jedoch zeigt die Suchmaschine zu den Suchanfragen abgestimmte Werbung an. Das Design ist an Google Search angelehnt. Die Suchanfragen vermengen Suchergebnissen von Yahoo!, Wikipedia und dem eigenen Webcrawler DuckDuckBot.

Ähnlich wie Google Search bietet DuckDuckGo die Möglichkeit einer Sicheren Suche. Es gibt für die verschiedenen Browser jeweils Erweiterungen, die installiert werden können.

StartPage

Das Design von StartPage ist sehr simpel. Die Suchergebnisse beschränken sich auf die Kategorien Web, Bilder und Videos. Die eigenen Suchanfragen werden an die Google-Suchmaschine weitergeleitet, aber vorher anonymisiert. Es werden keine personalisierten Daten wie z. B. IP-Adressen gesammelt. 2008 gewann StartPage das europäische Datenschutz-Siegel.

Die Suchmaschine wird über nicht-personalisierte Werbung finanziert, weswegen über den Suchergebnissen Werbeanzeigen geschaltet werden. StartPage verzichtet im Gegensatz zu Google auf eine Auswertung von Nutzerdaten.

FragFinn

Es handelt sich hierbei um eine Suchmaschine speziell für Kinder im Alter von 6 bis 12 Jahren. In der Suchmaschine erscheinen nur Webseiten, die explizit durch einen Mitarbeiter von FragFinn freigegeben wurden.

Für mobile Endgeräte gibt es auch Apps zum Herunterladen, um die Suchmaschine problemlos am mobilen Endgerät nutzen zu können.

WolframAlpha

Die Suchmaschine WolframAlpha ist vornehmlich für wissenschaftliche Suchanfragen geeignet, kann aber auch für schulische Zwecke z. B. zur eigenen Recherche als Lehrkraft genutzt werden. Die Google-Alternative ist ausschließlich in Englisch und Chinesisch verfügbar. Sie bietet in den abgedeckten Bereichen hochwertige Suchergebnisse an.

Bei WolframAlpha handelt es sich eher um eine Antwortmaschine als eine Suchmaschine. Es kann nicht nur nach einzelnen Worten gesucht werden, sondern WolframAlpha beantwortet auch (getippte) Fragen.

Qwant

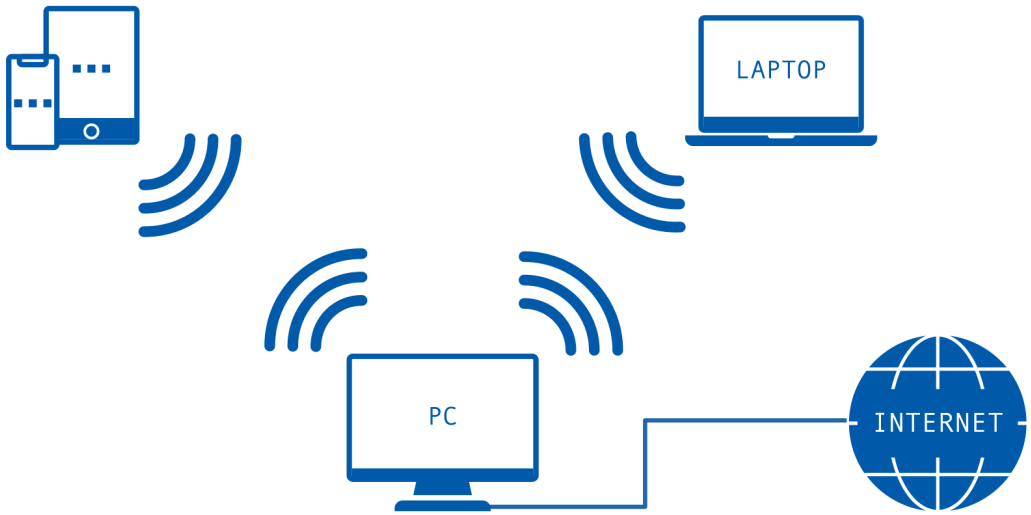
Das Besondere an dieser Suchmaschine ist ihre bunte und auffällige Optik. Zudem verspricht sie, die eigene Privatsphäre sehr ernst zu nehmen. Eigene Suchanfragen werden nicht aufgezeichnet und die eigenen Nutzungsdaten nicht für personalisierte Werbung verwendet.

Qwant bietet auch eine App für Android und iOS an.

LABORÜBUNG 25 - WINDOWS PC ALS WLAN-HOTSPOT EINRICHTEN

Szenario

In Ihrem Klassenzimmer gibt es noch keinen Access-Point. Sie wollen den Schülern WLAN für eine Internetrecherche zur Verfügung stellen.



Aufgaben

Verbinden Sie Ihr Endgerät mit dem schulinternen Netzwerk und prüfen Sie die Internetverbindung.

Vergewissern Sie sich, dass Ihr Gerät über eine aktivierte WLAN-Schnittstelle verfügt.

Öffnen Sie die *Einstellungen* und klicken Sie auf die Gruppe *Netzwerk und Internet* und wechseln Sie im Menü auf mobilem Hotspot.

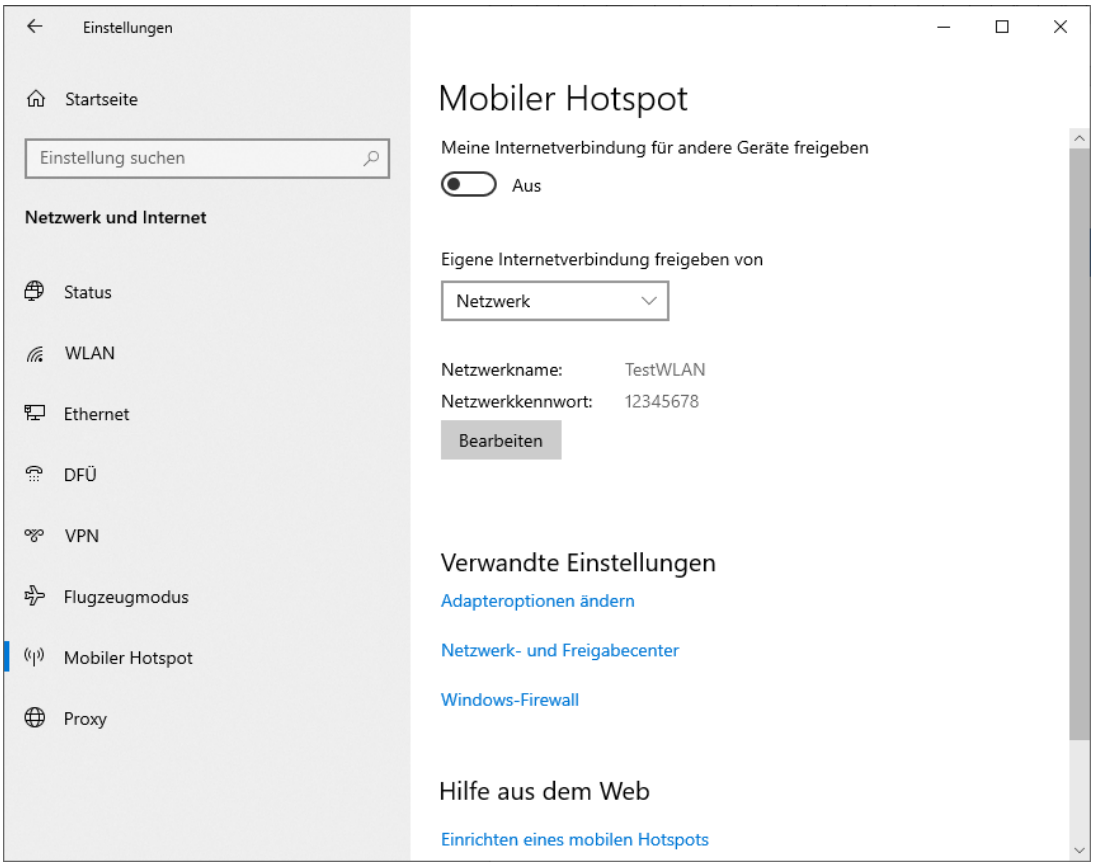
Erstellen Sie einen mobilen Hotspot mit einem eindeutigen Netzwerknamen, mindestens 8-stelligem Passwort. Wählen Sie, sofern verfügbar, bei Frequenzbereich *Alle verfügbaren* aus. Aktivieren Sie anschließend den Hotspot.

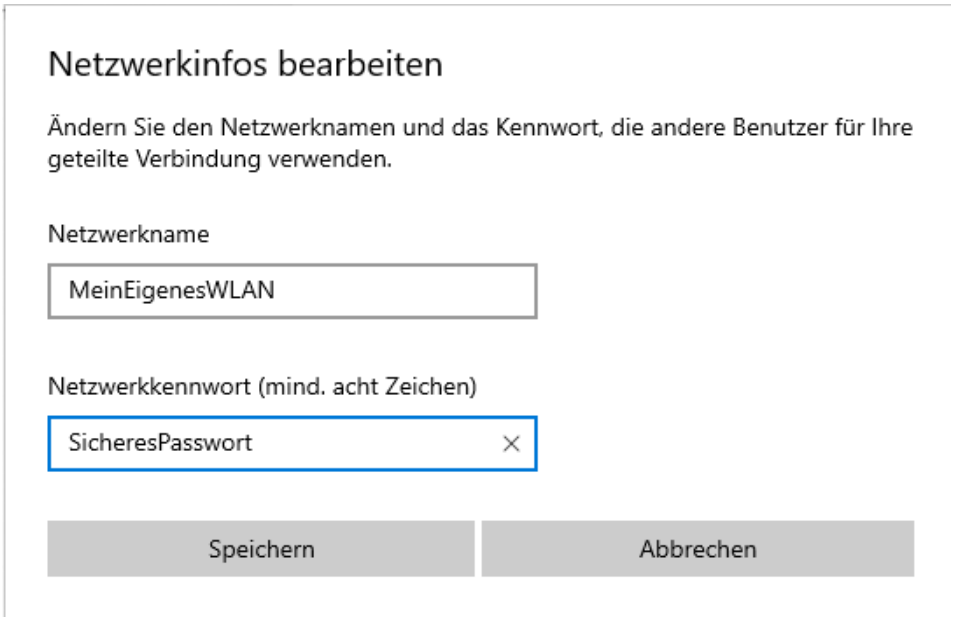
Testen Sie den Internetzugriff Ihrer Schüler.

Alternativ können Sie den Hotspot auch auf einem Mobilgerät aktivieren (iPad, iPhone)!

HINWEISE

Der Hotspot ist für maximal acht Teilnehmer ausgelegt. Technisch fungiert der Laptop wie ein Access Point und teilt die verfügbare Bandbreite des Access Points auf die Teilnehmer auf. Verbundene Geräte werden mit ihrer IP-Adresse und ihrer MAC-Adresse angezeigt.





LABORÜBUNG 26 - GEFÜHRTEN ZUGRIFF BEI APPLE EINRICHTEN

Szenario

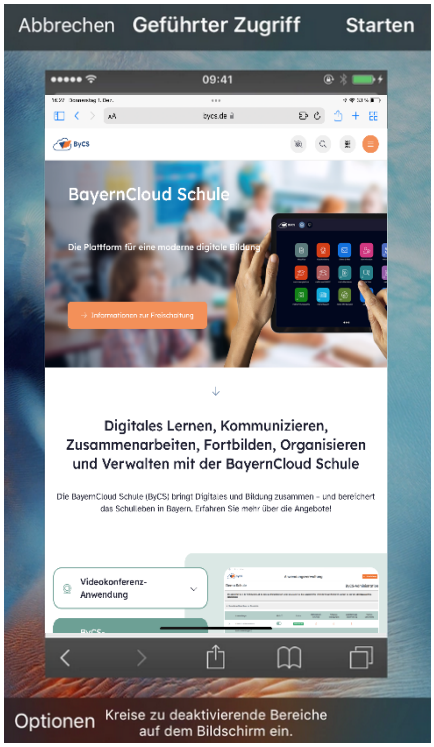
In Ihrem Unterricht möchten Sie einem Schüler ein iPad überlassen, bei dem er ausschließlich Zugriff auf die ByCS hat, ohne dass er sich in der classroom-App befindet.

Aufgaben

1. Suchen Sie in den Einstellungen die Menüpunkt „Geführter Zugriff“
2. Geben Sie einen Code für den geführten Zugriff ein.
3. Überlegen Sie, ob bestimmte Bildschirmabschnitte vor Zugriff geschützt werden sollen und markieren Sie diese.
4. Testen Sie den geführten Zugriff.

HINWEISE

Der geführte Zugriff ist in den Einstellungen unter dem Menüpunkt Bedienungshilfen zu finden. Bei der Aktivierung wird angezeigt, mit welchen Tasten durch dreimaliges Drücken der Modus gestartet und beendet wird.



LABORÜBUNG 27 - EINEN WINDOWS-RECHNER IN DEN KIOSK-MODUS BRINGEN

Szenario

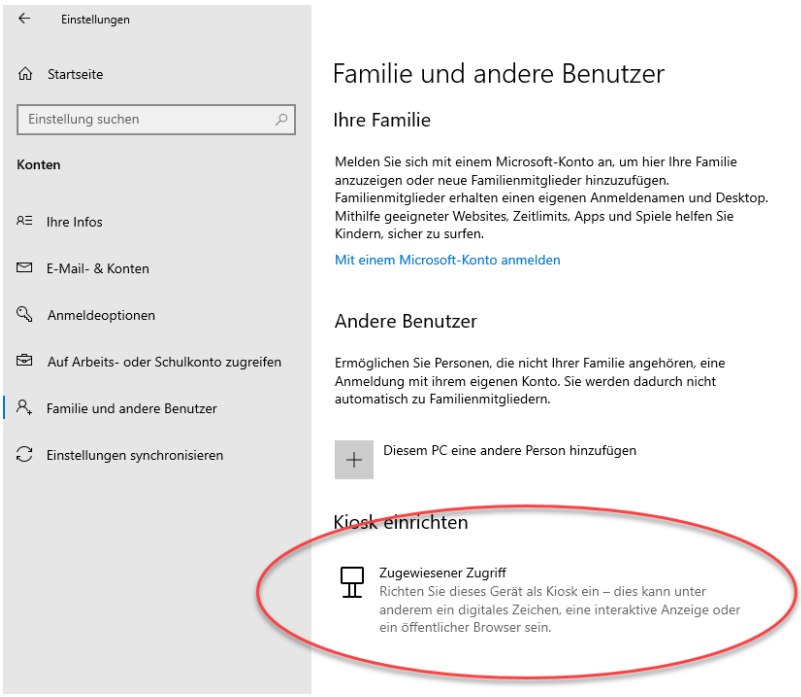
In Ihrer Schule soll in der Aula ein Display mit Informationen zum Schulhaus aufgestellt werden. Die Besucher sollen keine Möglichkeit haben andere Programme/Webseiten auf diesem Gerät aufzurufen.

Aufgaben

1. Richten Sie über die Benutzerkontenverwaltung unter Windows ein Benutzerkonto mit zugewiesenem Zugriff (Kiosk) ein
2. Wählen Sie die gewünschte App/das gewünschte Programm zur Anzeige aus.
3. Wählen Sie bei der ersten Einrichtung „Als digitale Signatur oder interaktive Anzeige“ für die Nutzung aus.
4. Testen Sie den zugewiesenen Zugriff.
5. Ändern Sie das Benutzerkonto im zweiten Schritt ab: Nutzung des Kioskes als öffentlicher Browser. Testen Sie die Änderung.

HINWEISE

Bei dem zugewiesenen Zugriff unter Windows handelt es sich um ein stark beschränktes Benutzerkonto, welches nur eine App ausführt und dem Nutzer sonst keine Möglichkeiten wie beispielsweise den Zugriff auf den Desktop oder Einstellungen von Windows bietet. Nur die von Microsoft zertifizierten Apps (UWP)im Store können für diesen Modus verwendet werden.



Sollen im Kiosk-Modus mehrere Apps angeboten werden, muss dies über ein Profil in einem MDM angelegt werden.

ABSCHLIESSENDE AUFGABE

LABORÜBUNG 28 - ERSTELLEN EINER SCHILF

Szenario

Sie wollen in Ihrer Schule zu bestimmten Teilbereichen des Medienkonzepts schulinterne Fortbildungen anbieten.

Themen:

- Der Umgang mit der Dokumentenkamera
- Der Einsatz von Online-Werkzeugen im Unterricht
- Verschlüsselung von Daten für Lehrkräfte
- Sicherung von in der Schule benutzten Daten
- Tablets als interaktive Tafel
- Zugriff auf den NAS Speicher der Schule, auch von zuhause
- ...

Aufgaben

1. Finden Sie sich in Kleingruppen zusammen und entscheiden Sie sich für eines der o. g. Themen.
2. Überlegen Sie sich eine Zielgruppe, einen Zeitrahmen und welche Ausstattung benötigt wird.
3. Erstellen Sie nun zu dem von Ihnen gewählten Thema eine SchiLF (ggf. mit Handreichungen) für Ihre Kollegen.
4. Stellen Sie Ihr Ergebnis dem Plenum vor.