Verschlüsselung von Dateien und Ordnern

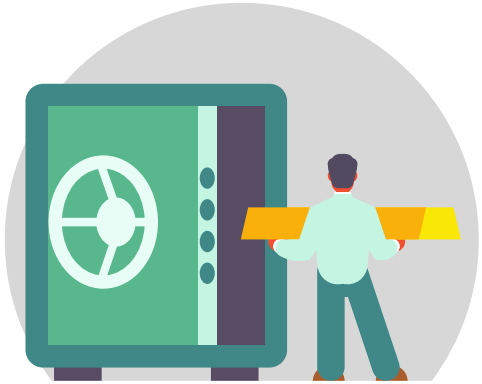
Stefan Kirsch

24. Januar 2024

Worüber will ich heute sprechen?

- Verschlüsseln – worum geht's da?
- Warum und wann will ich das?
- Wie geht das? – Prinzip der vorgestellten Tools
- Strategien – was wird verschlüsselt?
  - Veracrypt
  - Cryptomator
- Abschluss

Verschlüsseln – worum geht’s da?



meine Daten

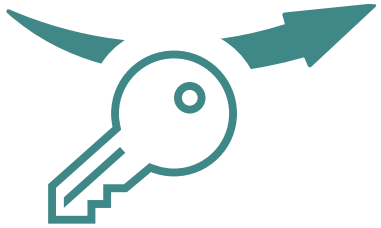
„Klartext“ *

Unlesbar - „Zeichensalat“

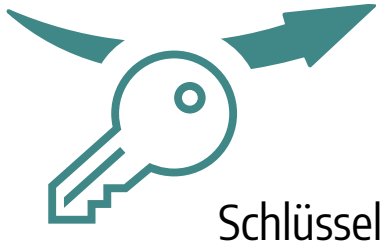
„Geheimtext“ *

meine Daten

„Klartext“ *



Schlüssel
(gut ausgewählt, geheim)

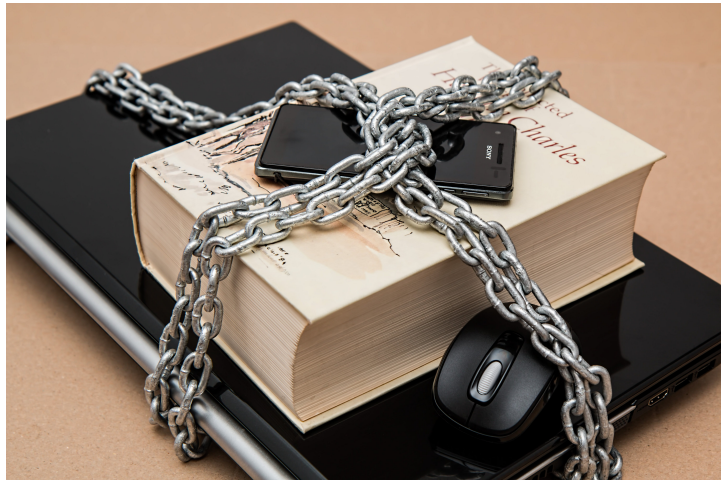


Schlüssel

*) Wikipedia, 2024-01-22
https://de.wikipedia.org/wiki/Verschl%C3%BCsselung#Entschl%C3%BCsseln

Verschlüsseln - warum und wann will ich das?

- Vertraulichkeit, z.B. von
  - Kommunikation
  - personenbezogenen Daten
  - Zugangsdaten
  - z.B. Fotos von Familie oder Kindern



- Integrität von Daten schützen
- Daten auf „nicht-stationären“ Datenträgern schützen (unbefugte Einsicht, Verlust, Diebstahl)
  - USB-Sticks, externe Festplatten/ SSDs
  - Laptop, Smartphone
  - Daten in der Cloud

Wie geht das?

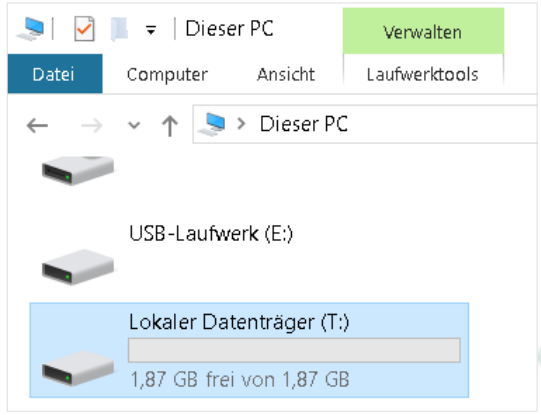
- jede Person oder Maschine, die lesen/ schreiben will, braucht eine entschlüsselte „Ansicht“ – z.B. dasselbe Programm, das die entschlüsselten Daten bereitstellt

  Aber: der Aufwand wird überschätzt

Prinzip der Tools:

sicher **verschlüsselte** Daten
im “Tresor“, „Container“

Software und
(im einfachsten Fall) Passphrase



die **entschüsselten** Daten
über ein virtuelles Laufwerk
erstellen, bearbeiten, …

Strategien

- System vollständig verschlüsseln
  - Bordmittel der Betriebssysteme:
    LUKS, BitLocker, MacOS FileVault
  - mobile OS: Verschlüsselung "hersteller- und versionsabhängig" (BSI)

- Datenträger ganz oder teilweise verschlüsseln
  - z.B. Veracrypt

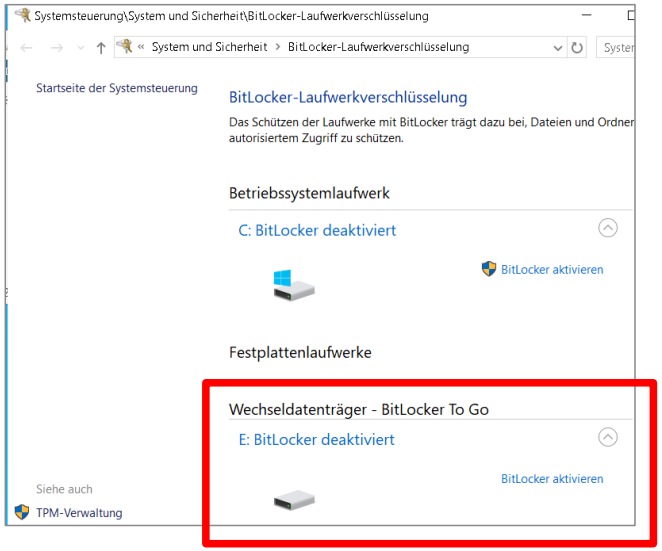
- Dateien und Ordner verschlüsseln
  - z.B. für Synchronisierung in die Cloud
  - Komprimierungswerkzeuge (7zip)
  - Cryptomator

BSI, 2024-01-18
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/Verschluesselung-auf-mobilen-Geraeten/verschluesselung-auf-mobilen-geraeten_node.html

Wechseldatenträger verschlüsseln

z.B. USB-Sticks, externe Festplatten/ SSDs, zzgl. gemeint sind Nicht-Systemdatenträger

- Bordmittel der Betriebssysteme
  - nicht interoperabel
- Veracrypt
  - frei, offen, multilizenziert
  - für Win, MacOS, GNU/Linux
  - CLI-tauglich

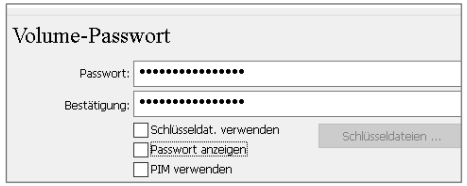


Veracrypt nutzen:

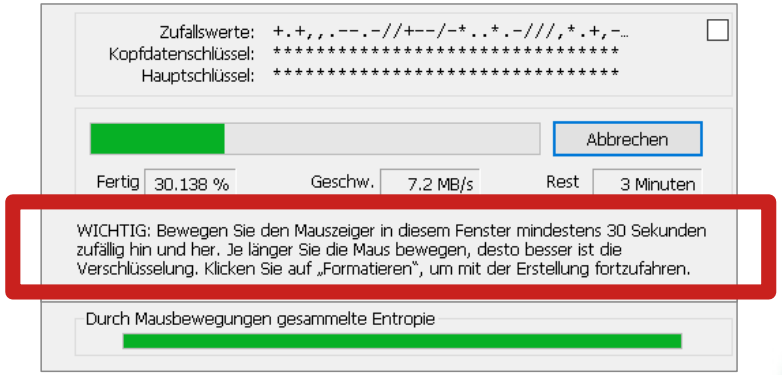
Bereich auf USB-Stick anlegen, auf den nur mit Veracrypt+Passwort zugegriffen werden kann

Auswahldialoge im Assistenten:

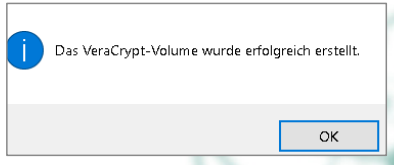
1) Partition/Laufwerk verschlüsseln
2) Typ wählen: Standard-Veracrypt-Volume
3) Speicherort auswählen z.B. USB-Stick
4) Verschlüsseltes Volume erstellen und formatieren
5) Verschlüsselungseinstellungen z.B. AES / SHA-512
6) Volume-Größe, z.B. ganzer USB-Stick
7) Passwort festlegen



8) Volumenformat festlegen z.B. FAT
9) „Zufall“ per Maus erzeugen



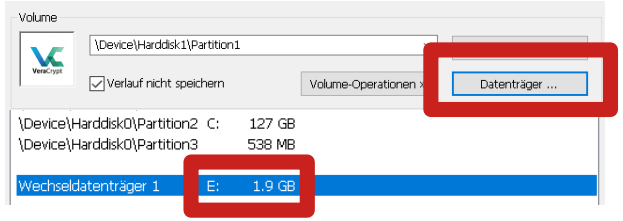
10) Volumen wird erstellt



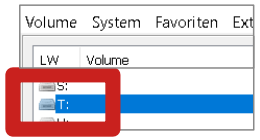
Veracrypt nutzen: Volume einbinden

Verschlüsselten Bereich auf USB-Stick als virtuelles Laufwerk einbinden
(„Laufwerksbuchstaben zuordnen“)

1) **verschlüsselten** Datenträger auswählen



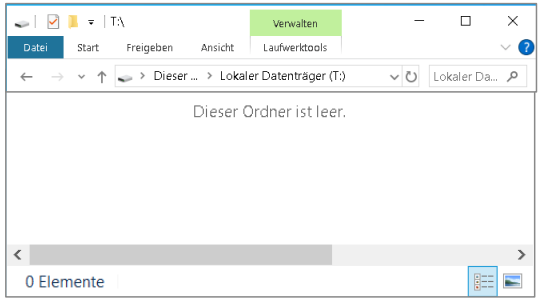
2) Stelle aussuchen, wo **entschlüsselte** Daten zur Verfügung gestellt werden

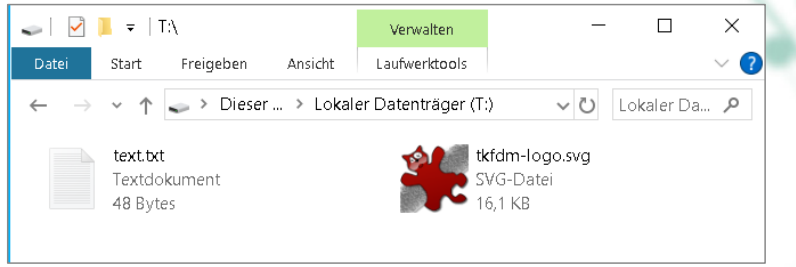


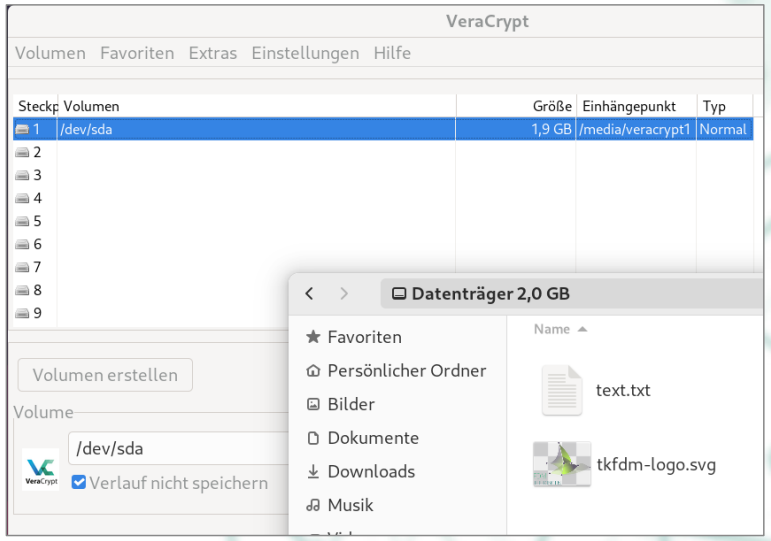
z.B. als Laufwerk T:

3) Passwort eingeben, kurz warten

4) auf Laufwerk T:
wie gewohnt arbeiten







Veracrypt nutzen: Bemerkenswertes

- Verschlüsselung der Systemfestplatte unter Windows möglich
  - unterschiedliche Aussagen zur Eignung, z.B. bzgl. Geschwindigkeit auf SSDs bestimmter Typen
- relativierende Einschätzungen, z.B. betreffend die Wartbarkeit des Codes
  - Audit:

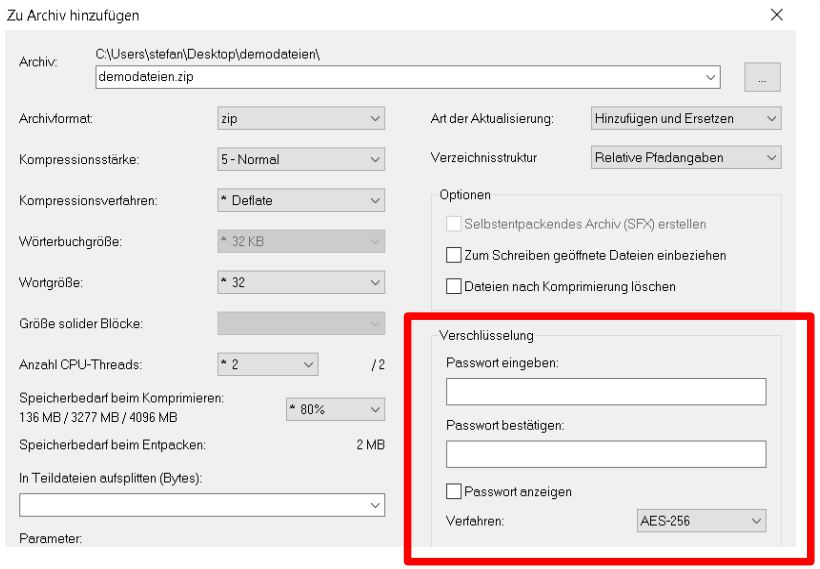
    „VeraCrypt schützt prinzipbedingt nicht vor Angriffen auf ein laufendes System mit geöffnetem Container"

    „VeraCrypt bietet vor allem dann guten Schutz, wenn Daten offline auf verschlüsselten Laufwerken gelagert werden, etwa auf einer Festplatte oder einem USB-Stick" (Fraunhofer SIT/ BSI)*
- für Backups: Tools verschlüsseln die Backups,
  Veracrypt verschlüsselt den Speicherort

*) Fraunhofer SIT/ BSI, 2024-01
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Veracrypt/Veracrypt.pdf?__blob=publicationFile&v=2

Dateien und Ordner verschlüsseln

z.B. für Synchronisierung in die Cloud

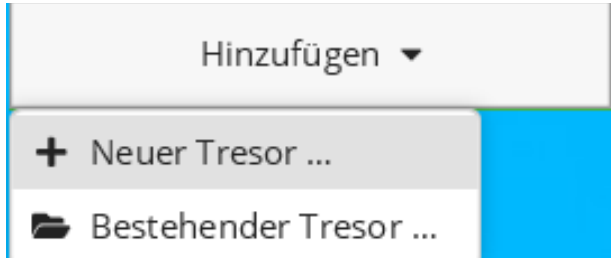


- Software, die Archivdateien (ent-)packen kann
  - unterstützt z.T. Verschlüssellung → z.B. 7zip
- Veracrypt Containerdatei
  - USB-Stick z.T. unverschlüsselt lassen
  - Container ist beweglich (z.B. auf Stick speicherbar)
  - Größe bei Erstellung festzulegen
  - bei Cloudsync: kleine Änderung an den Daten → „Container geändert“
- Cryptomator
  - dual-lizenziert, quelloffen
  - MacOS, Win, GNU/Linux (mobil: iOS, Android (€))
  - Tresor aus verschlüsselten Teilen - nur geänderte Teile werden neu synchronisiert

Cryptomator nutzen: Tresor hinzufügen

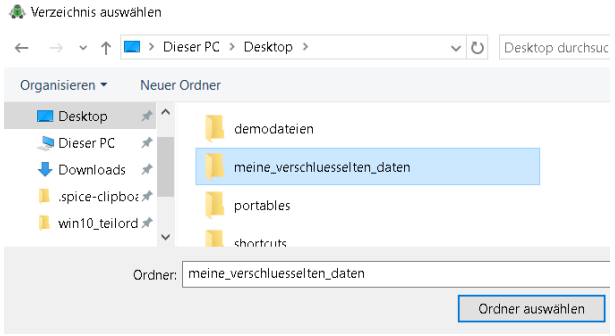
Dateien und Ordner verschlüsseln, z.B. für Synchronisierung in die Cloud

1) Neuen Tresor hinzufügen

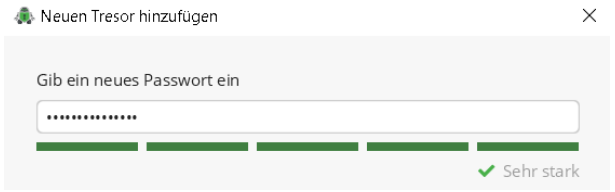


2) Tresornamen vergeben

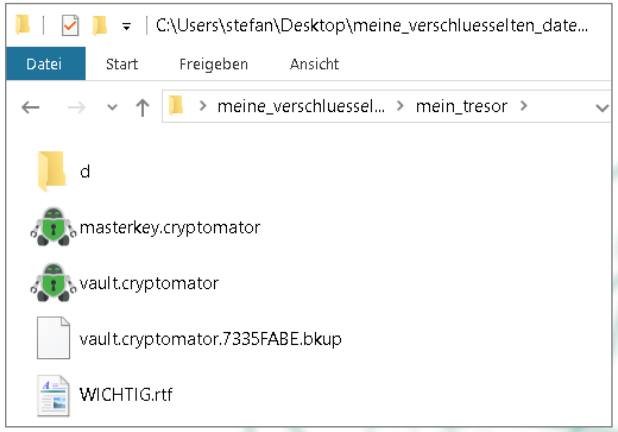
3) Tresorspeicherort festlegen



4) Passwort vergeben



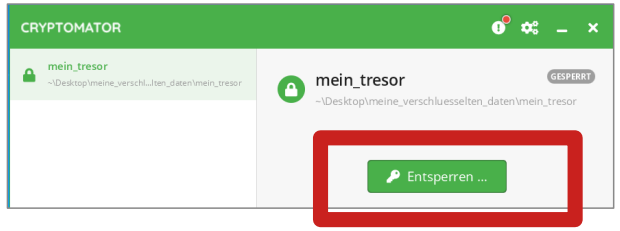
5) Fertig hinzugefügt



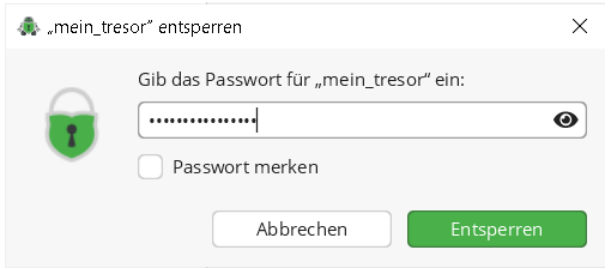
Cryptomator nutzen: Tresor einhängen

Dateien und Ordner verschlüsseln, z.B. für Synchronisierung in die Cloud

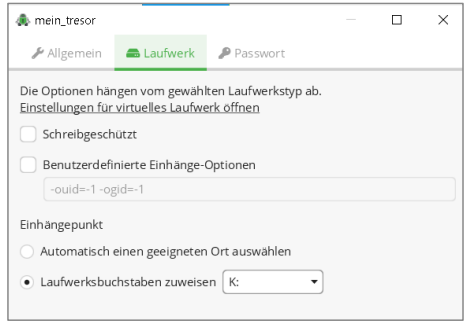
1) Tresor wählen > entsperren



2) Passwort eingeben

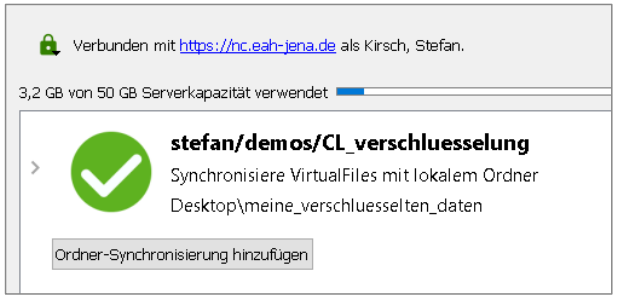


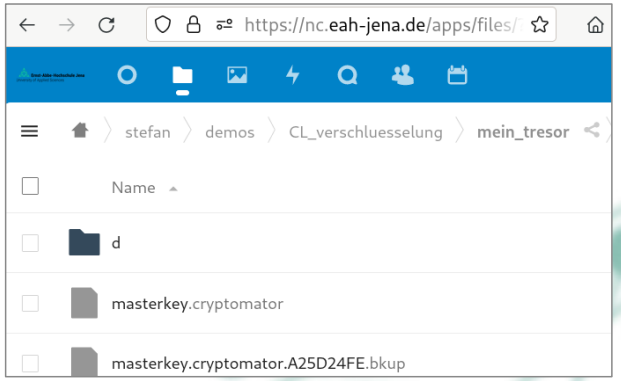
3) Tresoroptionen: Laufwerk K:



4) Fertig entsperrt und eingehängt

- Synchronisation in die Nextcloud

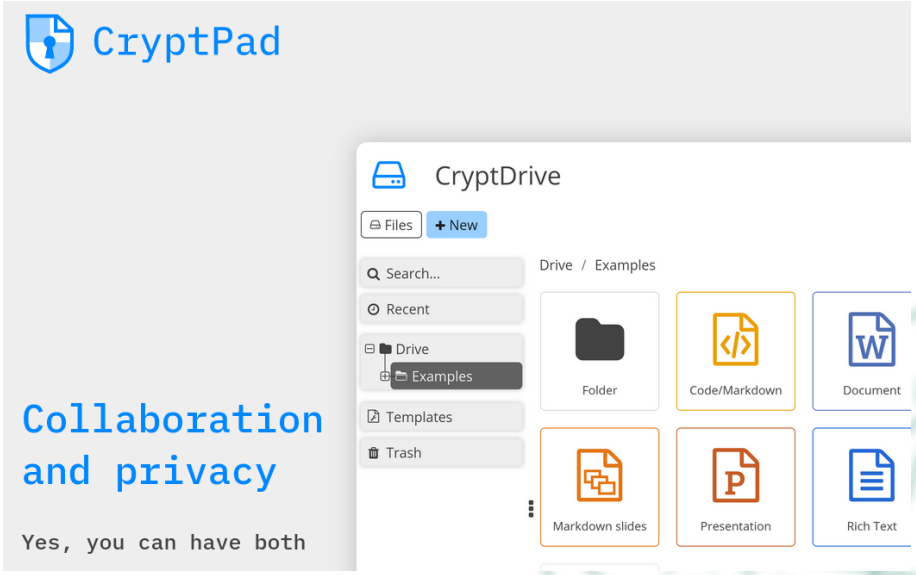




Cryptomator: Bemerkenswertes

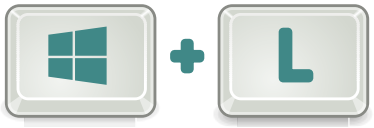
- „Bequemlichkeitseinstellungen“
  - beim Systemstart laden, Tresor automatisch entsperren, Passwort merken
  - Verknüpfung zum Einhängepunkt des Tresors erstellen (z.B. K:)
- Cloud-Sync ja, aber kein synchrones Bearbeiten von mehreren Geräten aus

  → keine zeitgleiche Zusammenarbeit auf Tresoren
  - Cryptomator Hub (€)
  - für Dokumentenzusammenarbeit: Cryptpad
    - cryptpad.org



Zum Mit-nach-Hause nehmen

- keine absolute Sicherheit: → Aufwand für unerwünschten Zugriff lässt sich durch Verschlüsselung erhöhen
- Gute Verschlüsselung: → sorgt für unverhältnismäßig hohen Aufwand
  → Passwortverlust – Daten weg
- Keine Entbindung von: → Betriebssystem- und Programmupdates
  → System sperren bei Abwesenheit



- einfache Umsetzung: → wenn ein Tool fertig eingerichtet ist: „normales Arbeiten“
- Verschlüsselungstools kombinieren
  Externes Laufwerk: → Veracrypt
  Daten für die Cloud: → Cryptomator (7zip)

Das Thüringer Kompetenznetzwerk
Forschungsdatenmanagement präsentiert...

FDM THÜRINGEN

Forschungsdatenmanagement

Online Coffee Lectures 23/24

21.02.2024

SQLite als Schweizer Taschenmesser für die Auswertung von tabellarischen Daten

Philipp Mathias Schäfer (zedif, Uni Jena)