IT-Sicherheit

IT-Sicherheit: Grundlagen für einen sicheren Arbeitsplatz

- Kurze Einordnung: Schutz von Daten, Systemen und Geräten vor Verlust, Missbrauch und Angriffen. Bedeutung für Unternehmen, Privatnutzer und öffentliche Einrichtungen.

Bedrohungslage

- Malware (Viren, Trojaner, Ransomware)
- Phishing und Social Engineering
- Datenverlust durch Hardwaredefekte
- Unsichere Netzwerke und veraltete Systeme
- Menschliche Fehler als häufigste Ursache Einordnung: Angriffe werden professioneller, automatisierter und häufiger.

Schutzziele der IT-Sicherheit

- **Vertraulichkeit** – Daten dürfen nur Berechtigte sehen
- **Integrität** – Daten müssen unverändert bleiben
- **Verfügbarkeit** – Systeme müssen zuverlässig funktionieren
- **Authentizität** – Identitäten müssen überprüfbar sein
- **Nachvollziehbarkeit** – Aktionen müssen dokumentiert sein

Hardwareaspekte: Physische Sicherheit

- Zugangskontrolle zu Serverräumen und Arbeitsplätzen
- Sichere Aufbewahrung von Notebooks und mobilen Geräten
- BIOS/UEFI-Passwörter und Secure Boot
- Hardware-Verschlüsselung (TPM-Chip, BitLocker-Unterstützung)
- Schutz vor Diebstahl (Kensington-Schloss, Inventarisierung) Hinweis: Physische Sicherheit ist die Basis jeder IT-Sicherheitsstrategie.

Hardwareaspekte: Netzwerke & Infrastruktur

- Firewalls (Hardware-Firewall, Router-Sicherheitsfunktionen)
- Segmentierung von Netzwerken (Gastnetz, Firmennetz)
- Sichere WLAN-Standards (WPA3, starke Passwörter)
- USV-Systeme zum Schutz vor Stromausfällen
- Regelmäßige Wartung und Austausch veralteter Geräte

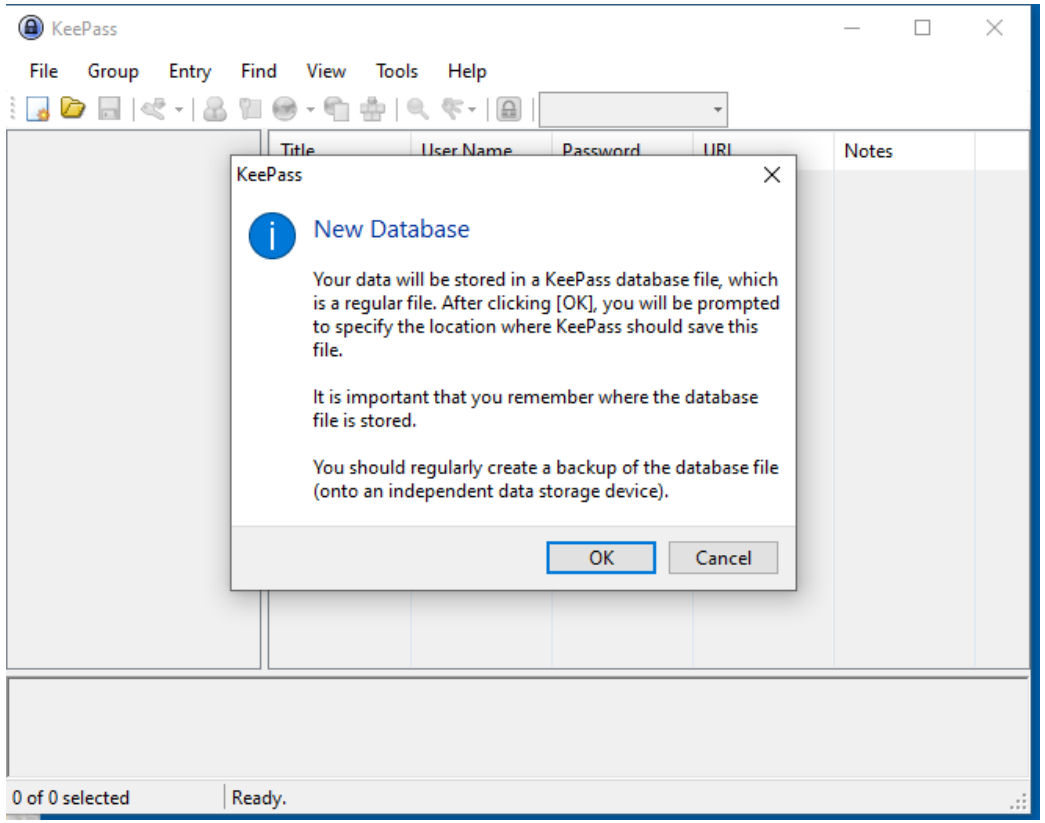
Softwareunterstützung: Betriebssystem & Updates

- Regelmäßige Sicherheitsupdates (Windows, macOS, Linux)
- Automatische Update-Funktionen aktivieren
- Entfernen veralteter Software
- Nutzung sicherer Standardkonfigurationen
- Rechteverwaltung: Arbeiten mit Standardbenutzer statt Admin

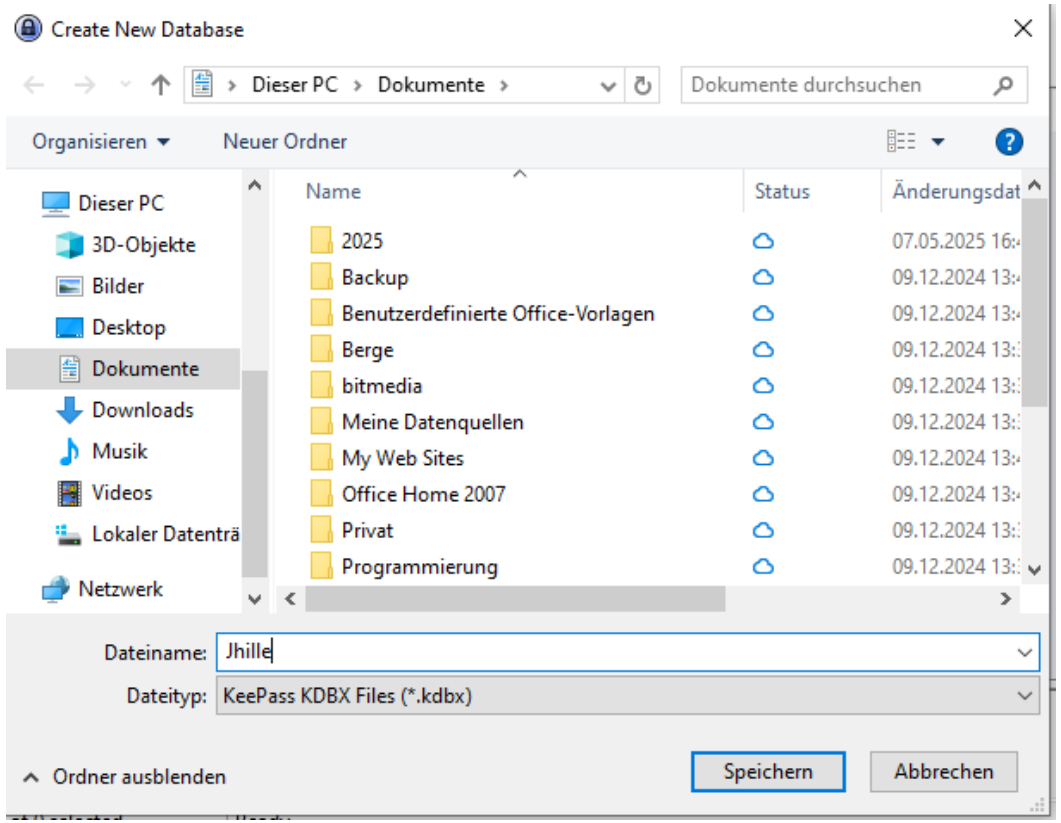
Softwareunterstützung: Schutzprogramme

- Antiviren- und Anti-Malware-Software
- Firewall-Konfiguration (Windows Firewall, Unternehmenslösungen)
- E-Mail-Filter und Spam-Schutz
- Browser-Sicherheitsfunktionen (HTTPS, Tracking-Schutz)
- Passwortmanager zur sicheren Verwaltung von Zugangsdaten

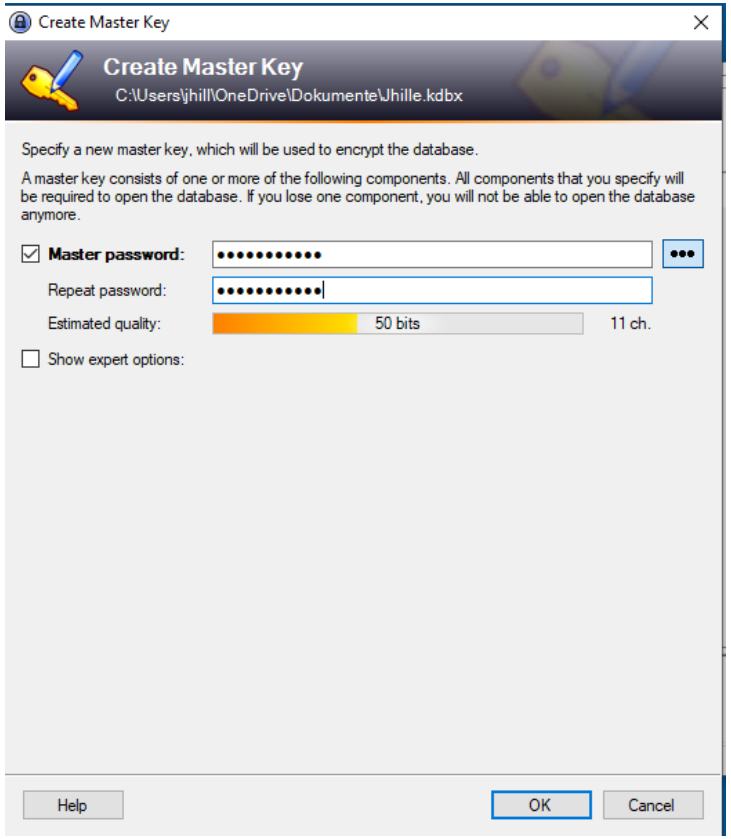
Passwordmanager Keepas



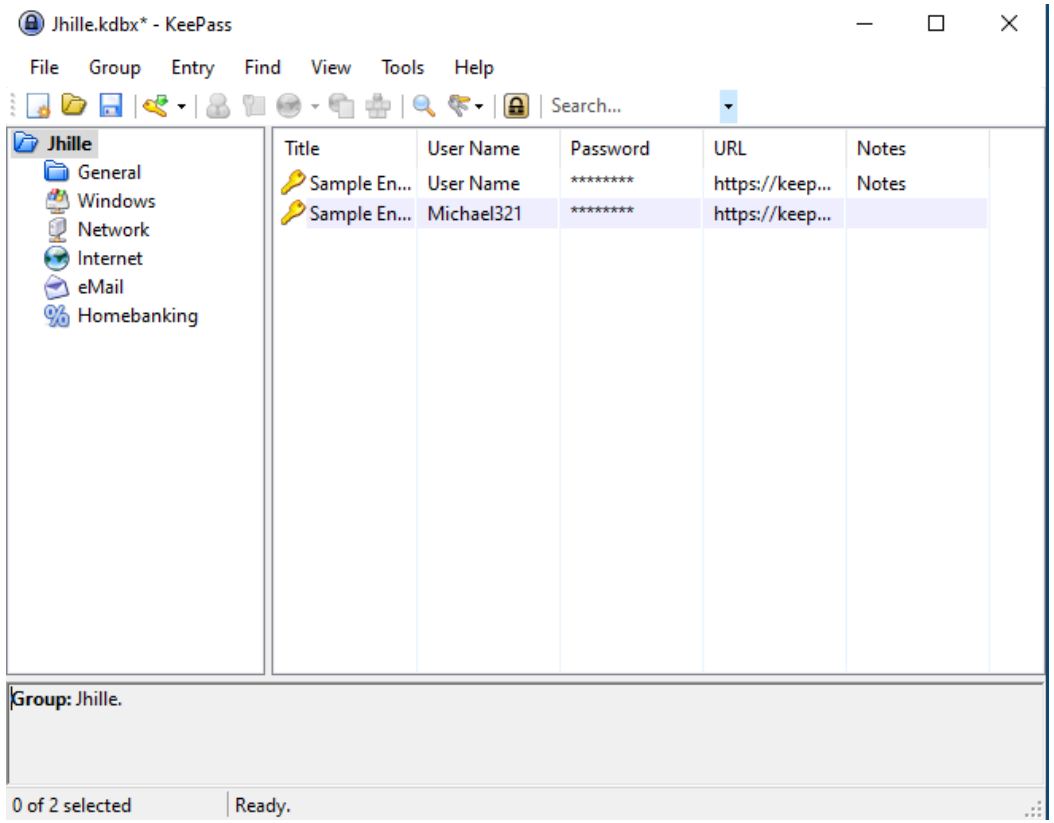
Passwordmanager Keepas



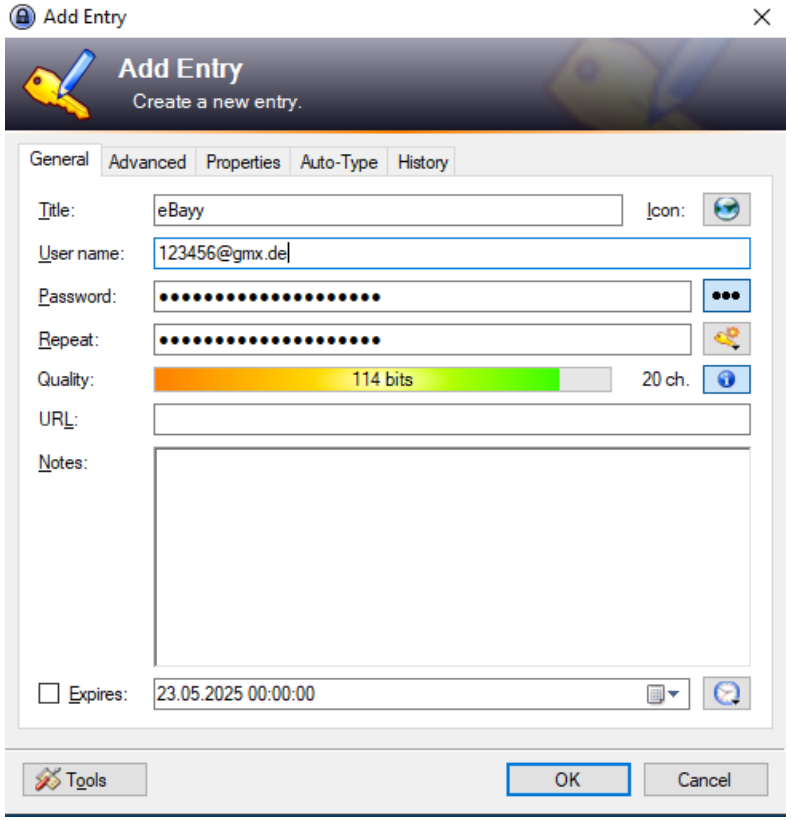
Passwordmanager Keepas



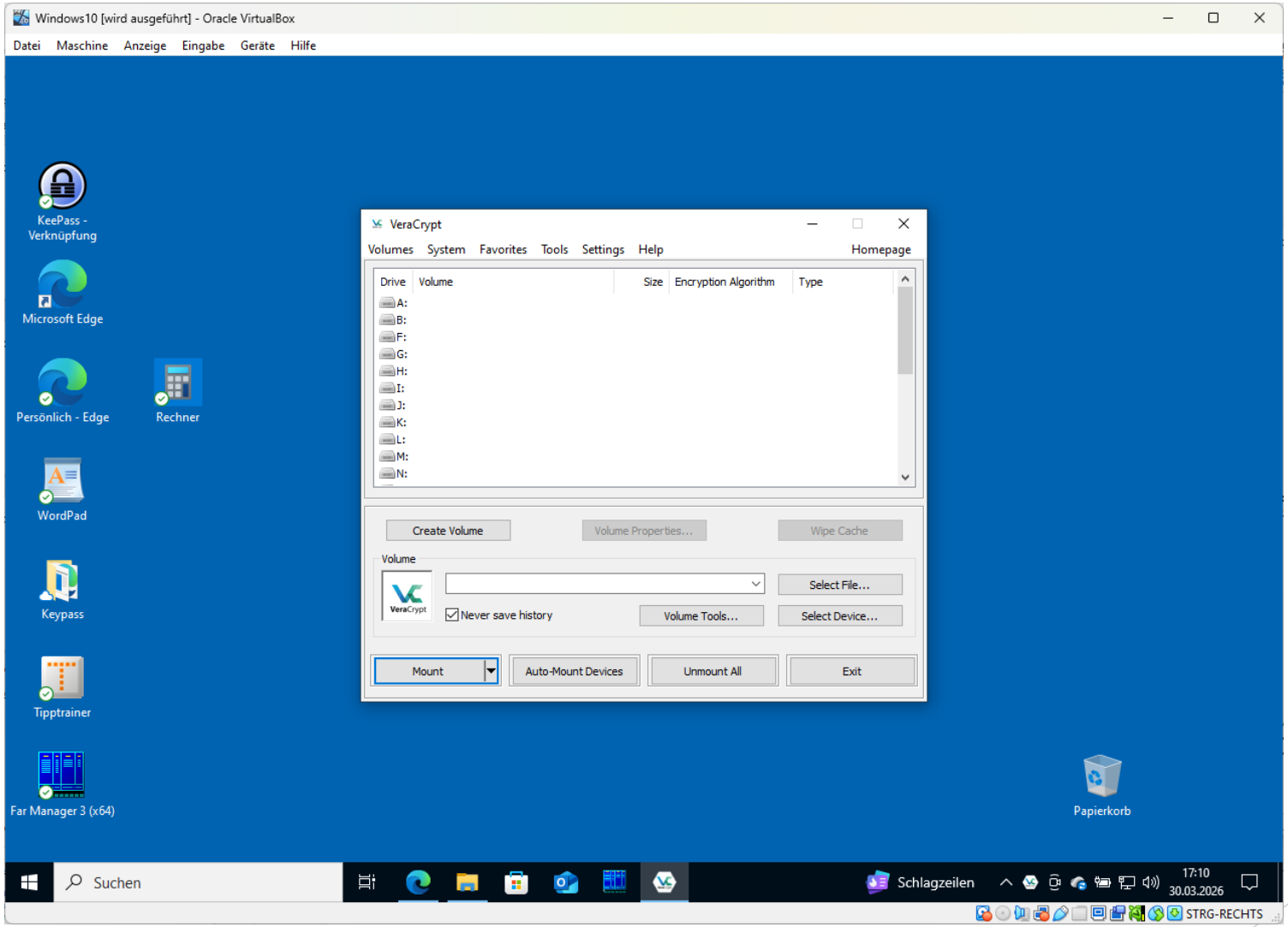
Passwordmanager Keepas



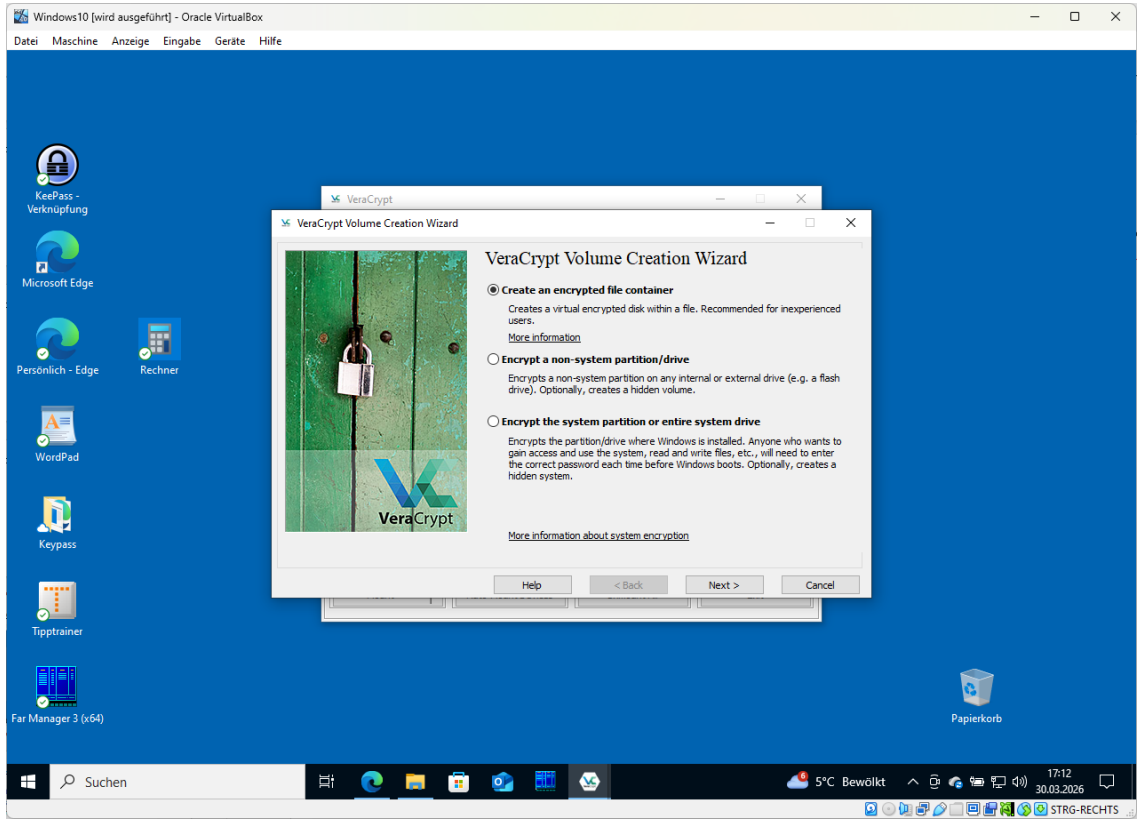
Passwordmanager Keepas

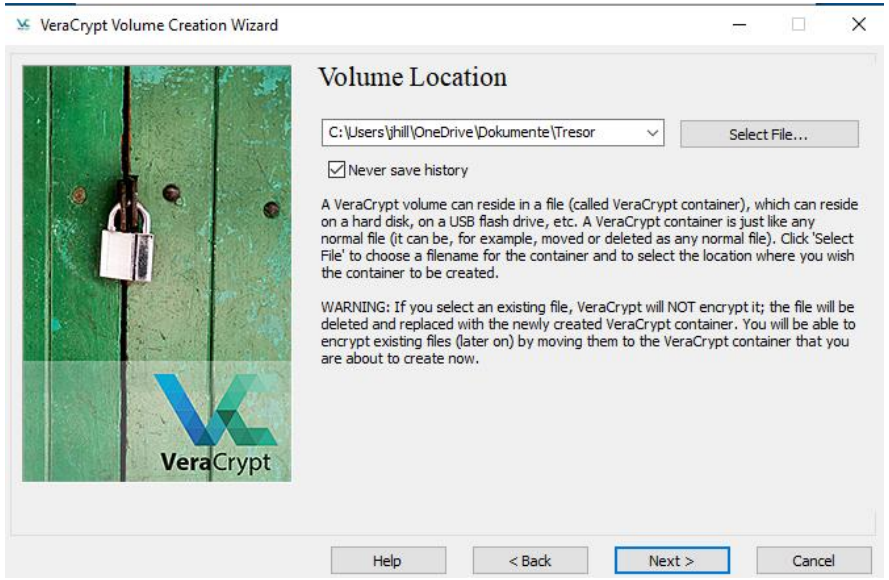


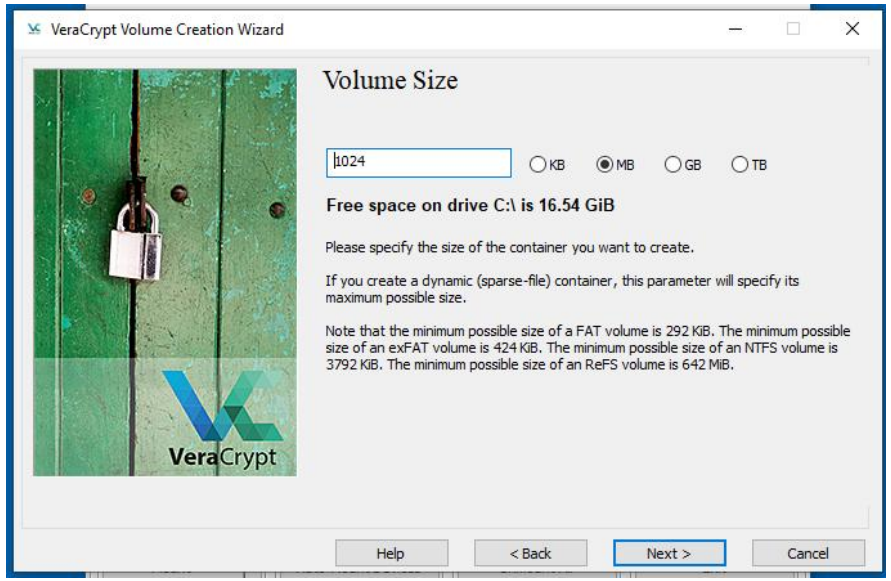
Verschlüsselungssoftware VeraCrypt

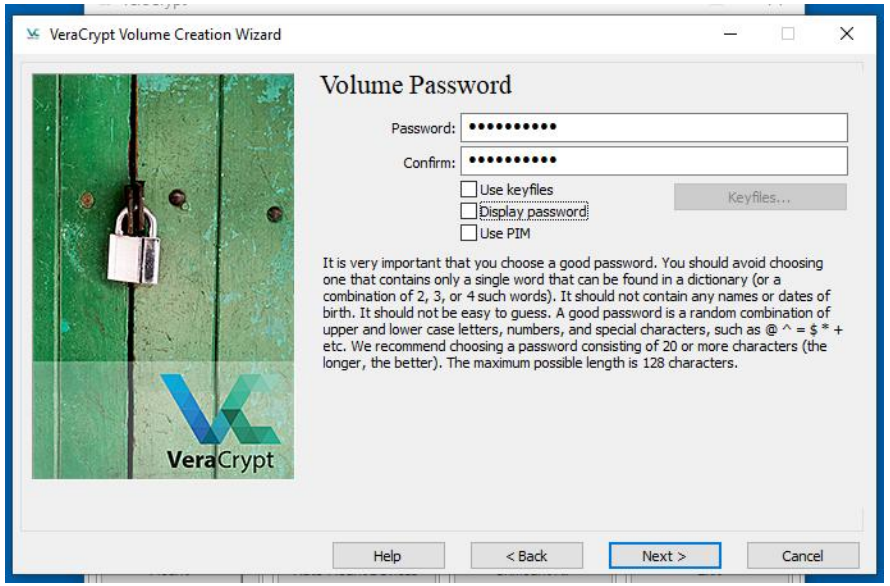


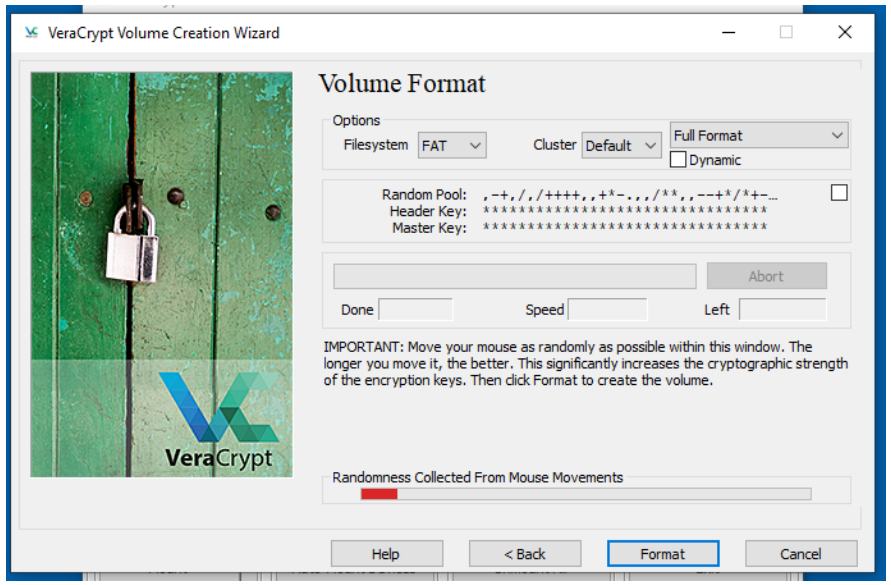
Anlegen eines Containers

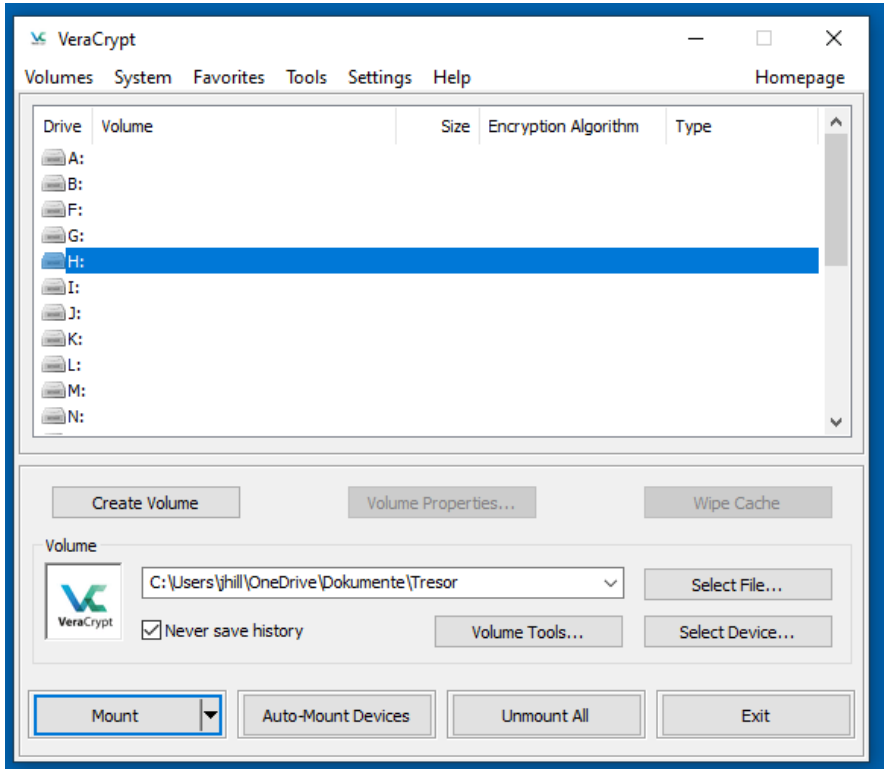


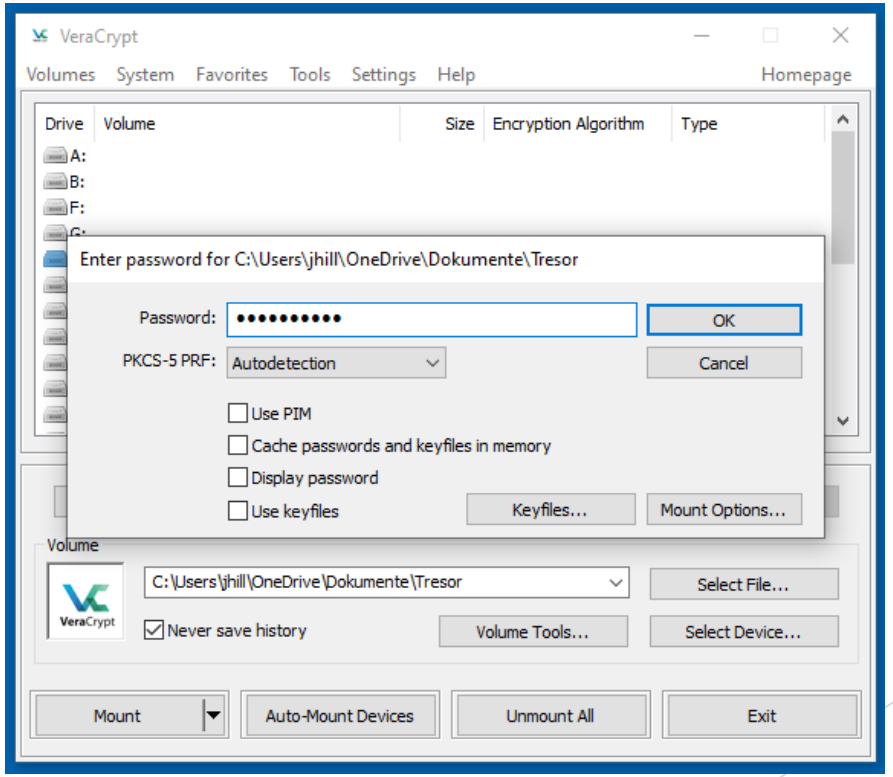

VeraCrypt Volume Creation Wizard
Volume Location
C:\Users\jhill\OneDrive\Dokumente\Tresor
Select File...
Never save history
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.
VeraCrypt
Help
< Back
Next >
Cancel

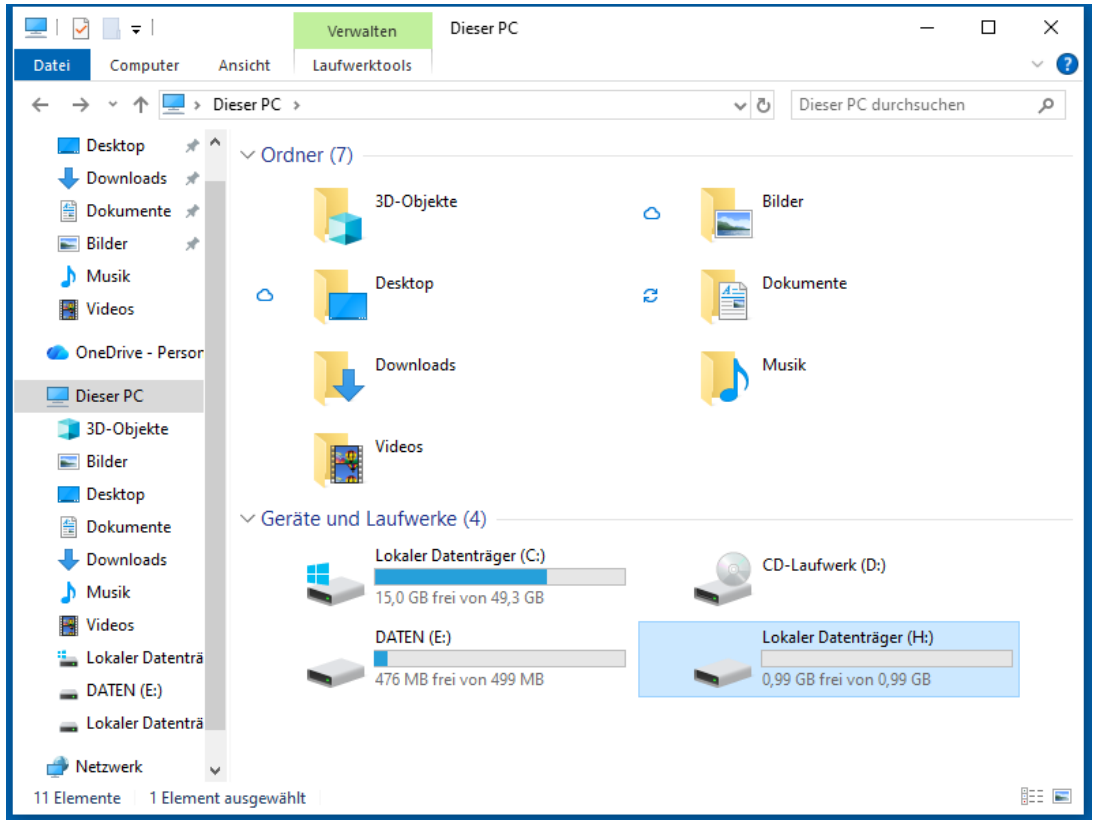

VeraCrypt Volume Creation Wizard
Volume Size
1024
KB
MB
GB
TB
Free space on drive C:\ is 16.54 GiB
Please specify the size of the container you want to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.
Note that the minimum possible size of a FAT volume is 292 KiB. The minimum possible size of an exFAT volume is 424 KiB. The minimum possible size of an NTFS volume is 3792 KiB. The minimum possible size of an ReFS volume is 642 MiB.
VeraCrypt
Help
< Back
Next >
Cancel


VeraCrypt Volume Creation Wizard
Volume Password
Password:
Confirm:
Use keyfiles
Display password
Use PIM
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.
VeraCrypt
Help
< Back
Next >
Cancel


VeraCrypt Volume Creation Wizard
Volume Format
Options
Filesystem
FAT
Cluster
Default
Full Format
Dynamic
Random Pool:
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Randomness Collected From Mouse Movements
VeraCrypt
Help
< Back
Format
Cancel


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\jhill\OneDrive\Dokumente\Tresor
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Unmount All
Exit


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
Enter password for C:\Users\jhill\OneDrive\Dokumente\Tresor
Password:
OK
PKCS-5 PRF:
Autodetection
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
C:\Users\jhill\OneDrive\Dokumente\Tresor
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Unmount All
Exit


Verwalten
Dieser PC
Datei
Computer
Ansicht
Laufwerktools
Dieser PC
Dieser PC durchsuchen
Desktop
Downloads
Dokumente
Bilder
Musik
Videos
OneDrive - Persor
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Netzwerk
Ordner (7)
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Geräte und Laufwerke (4)
Lokaler Datenträger (C:)
15,0 GB frei von 49,3 GB
CD-Laufwerk (D:)
DATEN (E:)
476 MB frei von 499 MB
Lokaler Datenträger (H:)
0,99 GB frei von 0,99 GB
11 Elemente
1 Element ausgewählt

Daten- & Zugriffsschutz

- Verschlüsselung von Festplatten und mobilen Datenträgern
- Sichere Passwörter und Multi-Faktor-Authentifizierung
- Rollenbasierte Zugriffsrechte (Least Privilege)
- Backup-Strategien (3-2-1-Regel, Cloud-Backups, Offline-Backups)
- Schutz sensibler Daten (DSGVO-Konformität)

Menschlicher Faktor

- Schulungen zu Phishing und Social Engineering
- Sensibilisierung für sichere Passwörter
- Umgang mit verdächtigen E-Mails und Anhängen
- Klare Meldewege bei Sicherheitsvorfällen
- Sicherheitskultur im Unternehmen fördern

Zusammenfassung & Ausblick

- IT-Sicherheit ist ein Zusammenspiel aus Hardware, Software und Verhalten
- Regelmäßige Updates, Backups und Zugriffsregeln sind unverzichtbar
- Moderne Angriffe erfordern kontinuierliche Anpassung
- Sicherheit ist kein Zustand, sondern ein fortlaufender Prozess