Dateien und Datenträger verschlüsseln

digitalcourage
Hochschulgruppe

Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - bei Verlust/Diebstahl des Laptops oder USB-Stick
  - alle, die personenbezogene Daten speichern
- Weil Ihr ein Grundrecht auf digitale Privat- und Intimsphäre habt!
  - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ – sogenanntes IT-Grundrecht
    - Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

Sinnbild: Tresor mit Kombination

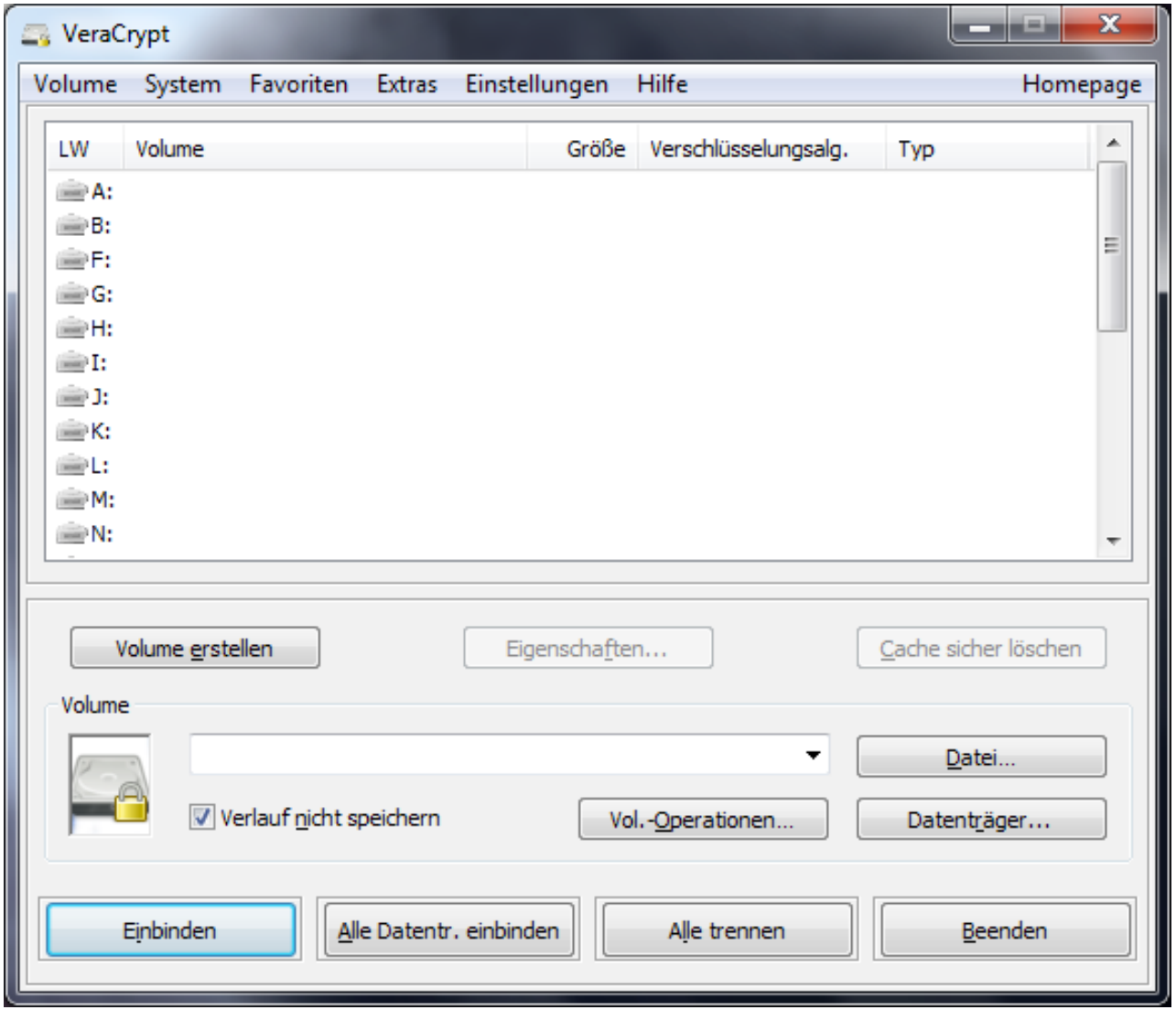
Software-Auswahl: VeraCrypt

- Software zur Dateiverschlüsselung
- quelloffen und auf allen gängigen Plattformen verfügbar
- Freie Software

Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
- Datenträger:
  - Festplatten/SSDs
  - CDs, DVDs, … (Container)
  - USB-Sticks
- Systempartition

Screenshot VeraCrypt



VeraCrypt: Vorteile und Nachteile

Vorteile

- quelloffen, freie Software
- nachvollziehbare Änderungen am Code
- plattformübergreifend
- auf USB-Stick transportierbar
- unabhängiger Audit

Nachteile

- Komfortverlust
- Passwortverlust = Datenverlust

Umgang mit VeraCrypt

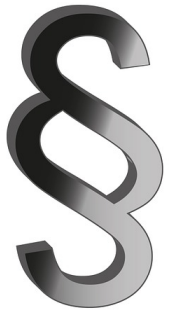
- Was will ich verschlüsseln?
- Starkes Passwort wählen
- Adminrechte notwendig
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen
- Größtes Sicherheitsrisiko ist fast immer der Nutzer!

Alternativen zu VeraCrypt

- **dm-crypt** (Teil des Linux-Kernels ab Version 2.6)
  - z.B. Ubuntu und Mint erlauben Systemverschlüsselung bei Installation
- **7-Zip**: freie Software, unterstützt AES256-Verschlüsselung
- Nicht vertrauenswürdig, da nicht quelloffen:
  - Windows: **BitLocker** (ab Vista, nur bei teuren Windows-Versionen)
  - MacOS: **FileVault**
  - zahllose weitere kommerzielle Produkte

Rechtliches

- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
  - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
  - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch



Weiterführende Literatur

- Mike Kuketz, VeraCrypt: Daten auf USB-Stick sicher verschlüsseln
  https://www.kuketz-blog.de/veracrypt-daten-auf-usb-stick-sicher-verschluesseln/
- Wikipedia über Festplattenverschlüsselung:
  https://de.wikipedia.org/wiki/Festplattenverschlüsselung

Bild- und Linknachweise

- soweit nicht anders angegeben, sind alle Grafiken gemeinfrei
- alle Links wurden zuletzt am 22. Juni 2020 überprüft

– Ende Datei-/Datenträgerverschlüsselung –