

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

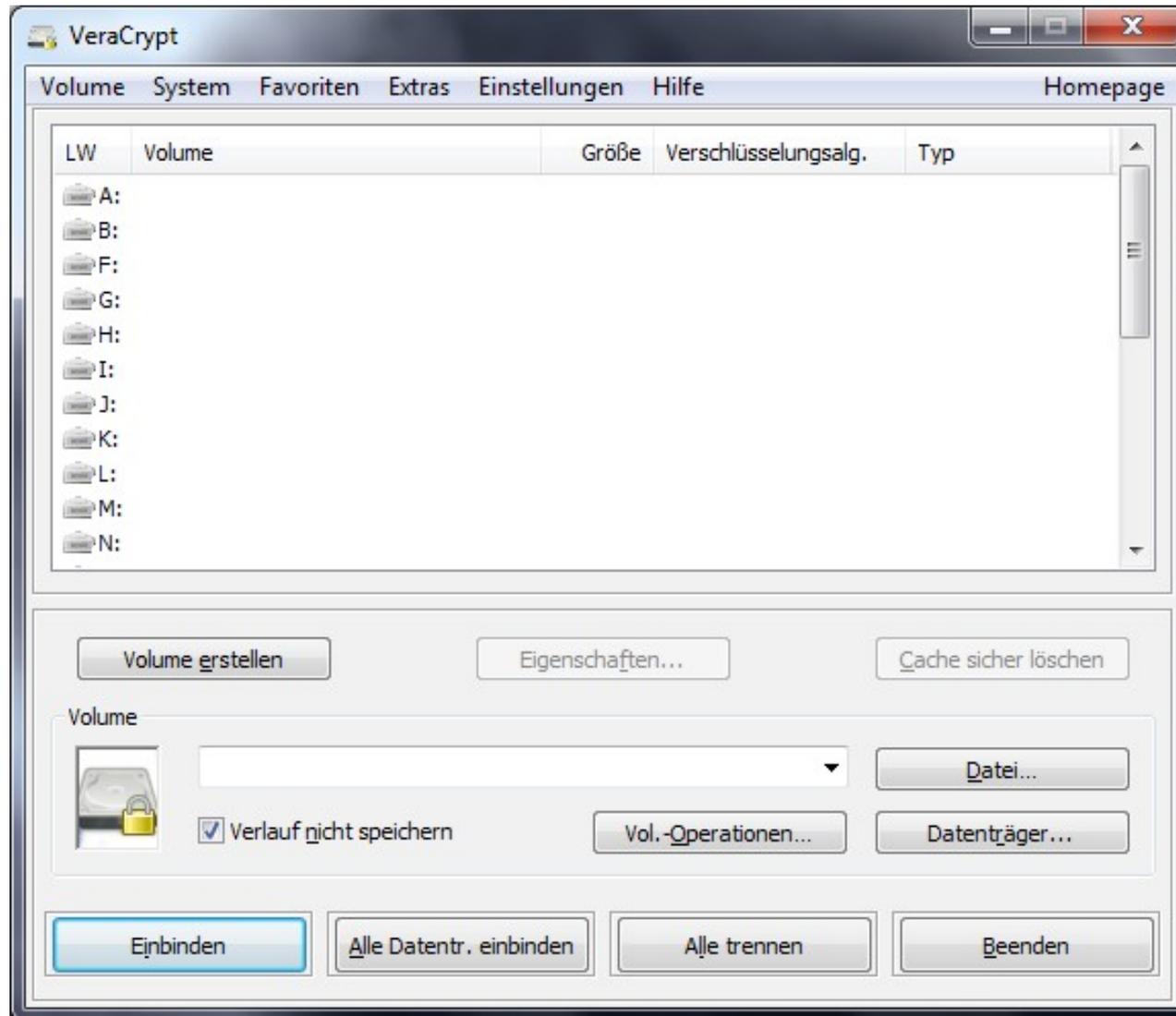
- ▶ Software zur Dateiverschlüsselung
- ▶ quelloffen und auf allen gängigen Plattformen verfügbar
- ▶ Freie Software



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



– Ende Datei-/Datenträgerverschlüsselung –

Digitalcourage in der Nähe

▶ Digitalcourage-Hochschulgruppe

- ▷ Treffen an jedem 1. und 3. Montag im Monat um 18:00 Uhr im SozCafé (X-C2-116, X-Gebäude Uni Bielefeld)
- ▷ <https://digitalcourage.de/hochschulgruppe-bielefeld>

▶ Digitalcourage e.V.

- ▷ offenes Treffen jeden Dienstag ab ca. 20:30 Uhr im TaverNio (Niederwall 23).
- ▷ <https://digitalcourage.de/treffen-vor-ort>

Derzeit nur Online!
Bei Interesse, bitte eine E-Mail an die HSG oder den Verein senden.

Weitere Projekte

▶ **PRISM Break**

▷ prism-break.org/de/all/

Liste datenschutzfreundlicher Software und Anbieter

▶ **Digitalcourage: Digitale Selbstverteidigung**

▷ digitalcourage.de/digitale-selbstverteidigung

Übersichts-Flyer hier im Raum zum Mitnehmen!

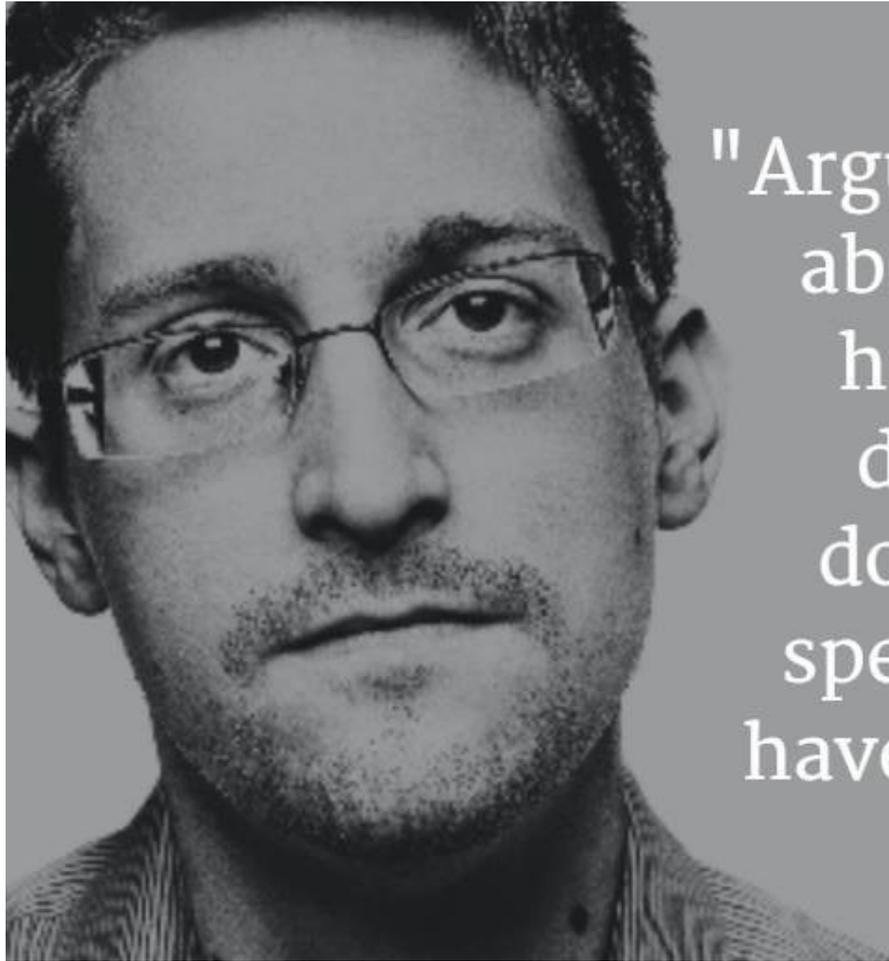
▶ **CryptoPartys weltweit!**

▷ cryptoparty.in (auf Englisch)

▶ **Freifunk Bielefeld**

▷ freifunk-bielefeld.de

Click to edit the title text format



"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."