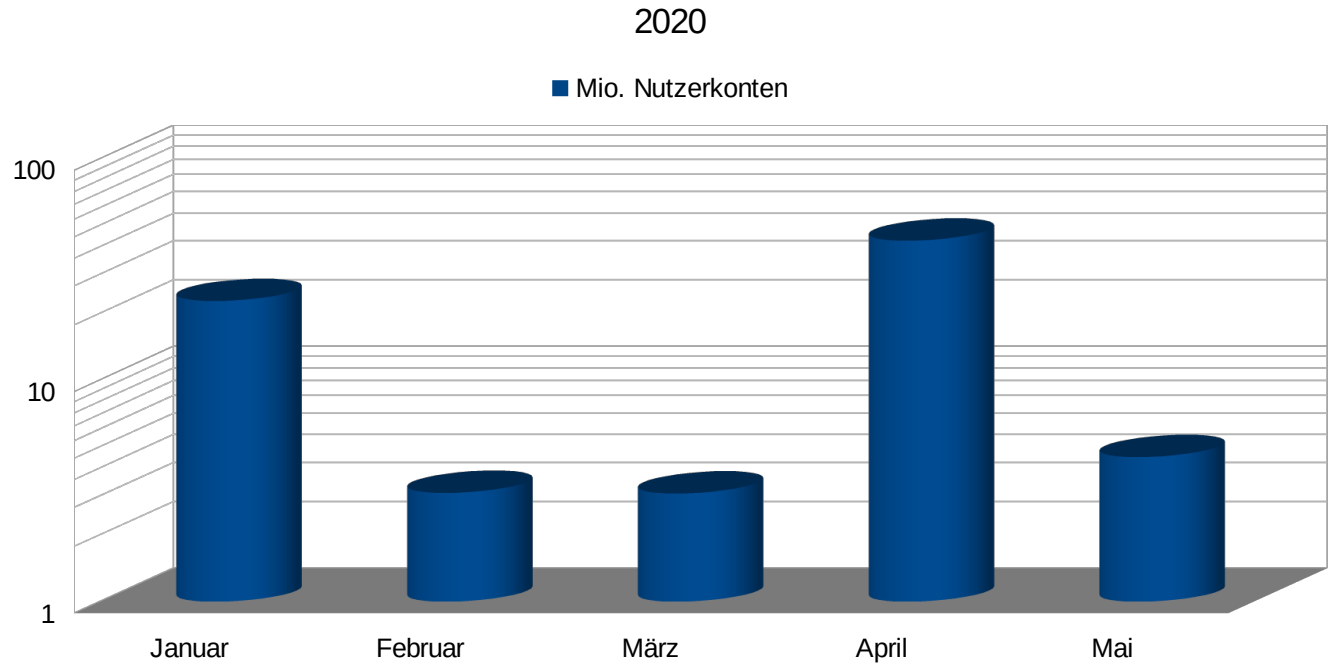
Sichere Passwörter

Agenda

- Sichere Passwörter
  - Wie werden Passwörter "geknackt"
  - Was macht Passwörter stark?
  - Starke Passwörter selber erzeugen
- Ein Zweiter Faktor machts noch stärker
- Passwortverwaltung

Kompromittierte Nutzerkonten



2020 bislang:

76.278.473

(Quelle: Hasso-Plattner-Institut, https://sec.hpi.de/ilc/statisics)

Passwörter Top 10

Passwort		Häufigkeit (in ‰)
1	**123456**	8,10
2	**123456789**	3,89
3	**password**	1,89
4	**qwerty**	1,85
5	**12345**	1,38
6	**12345678**	1,17
7	**111111**	1,17
8	**qwerty123**	1,02
9	**1q2w3e**	0,97
10	**123123**	0,85
,,,	**...**	…

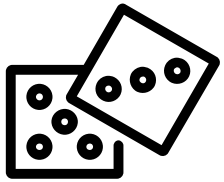
Wie werden Passwörter geknackt?

- Brute Force
  - alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
  - Phishing, Person austricksen um Passwort zu erfahren
  - gerne auch durch Facebook, LinkedIn etc.

Was macht ein Passwort stark

- Geheimhaltung

- Zufall

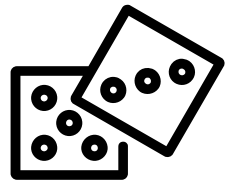


- Länge

Geheimhaltung: gar nicht so einfach...

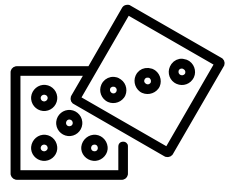
- Abhören / Abfilmen
  - Keylogger, Überwachungskameras, Handys anderer Leute, Staatstrojaner, unverschlüsselte Emails (Google), der Blick von Hinten über die Schulter
- Schlechte Verstecke
  - Post-Its, Schreibtischunterseiten, Zettel in der Geldbörse, dropbox/cloud, Klartextdateien
- Social Engineering
  - Liebe Menschen: Kolleg.innen, Freunde, Familie, Vorgesetzte, vorgebliche Vorgesetzte
  - Nicht so liebe Menschen: Erpressung, Schmerzandrohung

Die Macht des Zufalls - Entropie



- Der Mensch ist nicht gut darin, sich zufällige Worte auszudenken
- Verknüpfung von Sinneseindrücken und Vorstellung unter Einbeziehung bereits gelernten --> Prozess = Denken
- Problem: das menschliche Gehirn assoziiert immer
- Biespiel auf der folgenden Folie

Die Macht des Zufalls - Entropie



- Situation
  - Jemand sitzt am Schreibtisch im Arbeitszimmer und isst dabei eine Melone
  - Im Arbeitszimmer befinden sich viele Bürogegenstände; auf dem Tisch stehen zB ein Locher und ein Hefter, sowie Stifte und der PC
- "Spontan und zufällig ausgedachtes Passwort" durch aneinanderreihung von Worten
  - **HausLocherTasteMeloneBagger**
  - Gehirn hat Gegenstände aus der konkreten Situation verknüpft
- Wörterbuchangriff möglich, da alle Wörter in einem handelsüblichen Wöterbuch stehen

Passwort vs Passphrase

- Passwort = wenige Zeichen (oftmals ≤ 6)
- Passphrase = aneinanderreihung von vielen Zeichen (≠ Wörter)
  - Ziel: Angreifer zu möglichst vielen Rateversuchen zwingen
  - Stärke Passphrasen = mehr Anzahl möglicher Kombinationen
- Merkmale einer guten Passphrase
  - Auf die länge kommt es an!
  - Länge durch viele Zeichen (Länge, z.B. 16+)
  - aus einem großen Alphabet (Zeichenvorrat: Ziffern, Groß-/Kleinbuchstaben)
  - zufällig ausgewählt (nicht: selbst ausgedacht)

Starkes Passwort erzeugen

- Länge + Zufall entscheidend!
- Passwort "auswürfel"
  - Diceware
  - Würfellisten (Link am Ende des Passwortteils)
- Beispiel:
  - UAVM-3nKAEclSKDMa/WhT2En9

Zwei-Faktor-Authentifizierung

Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

Funktionsweise

- Teilprozesse eines Anmeldevorgangs welche zusammengesetzt werden (im Sprachgebrauch synonym)
  - Fehlen = Anmeldevorgang nicht erfolgreich
- Authentisierung
  - Benutzer.in meldet sich mittels eindeutiger Informationen an einem System an (zB Passwort oder Chipkarte)
- Authentifizierung
  - System überprüft Gültigkeit der Anmeldedaten und "erkennt" Benutzer.in

Funktionsweise

- Elemente
  - Besitz (z.B. Chipkarte, TAN-Generator, physischer Schlüssel)
  - Geheimes Wissen (zB Passphrase, PIN, TAN)
  - oder Biometrie (z.B. Fingerabdruck, Retina, menschliche Gang, Stimme)
- Keine zwingende Verschiedenheit, aber idR getrennte Übertragungskanäle
- In Stufen hintereinander geschaltet oder in Kombination miteinander

Arten

- TAN (Transaktionsnummer)/OTP-Systeme (One-Time-Passwort)
  - Einmalkennwort, dass zeit- oder ereignisbasiert stets neu generiert wird und zusätzlich übermittelt werden kann
  - Früher: Papierlisten (iTAN)
  - Heute: TAN-Generatoren (Hardware) bzw. Authenticator Apps (Software)
  - Teilw. auch unter Einbeziehung von Transaktionsdaten (Kontonummer und Betrag); eTAN, Chip TAN
- TAN als SMS (mTAN, smsTAN)
  - Niemals dasselbe Gerät für Log-In und TAN nutzen
  - Zweite Faktor fällt weg!

Arten

- Kryptographische Token, gemeint "Schlüssel"
- Speicherung eines privaten kryptographischen Schlüssel
  - Softwarezertifikat (bekannt von ELSTER)
  - Hardware auf einer Chipkarte (HBCI, Signaturkarten) oder einem speziellen USB-Stick/NFC-Token (FIDO/U2F).
- Biometrische Systeme: Überprüfung des Vorhandenseins von zuvor erfassten körperlichen Merkmalen (Fingerabdruck, Gesicht, Retina).
  - Normalerweise nicht Geheim (Sichtbarkeit des eigenen Gesichts) --> Lebenderkennung
  - Problem: Lässt sich schwer/gar nicht ändern

How-To: Starke Passwörter merken?!

KeePass XC

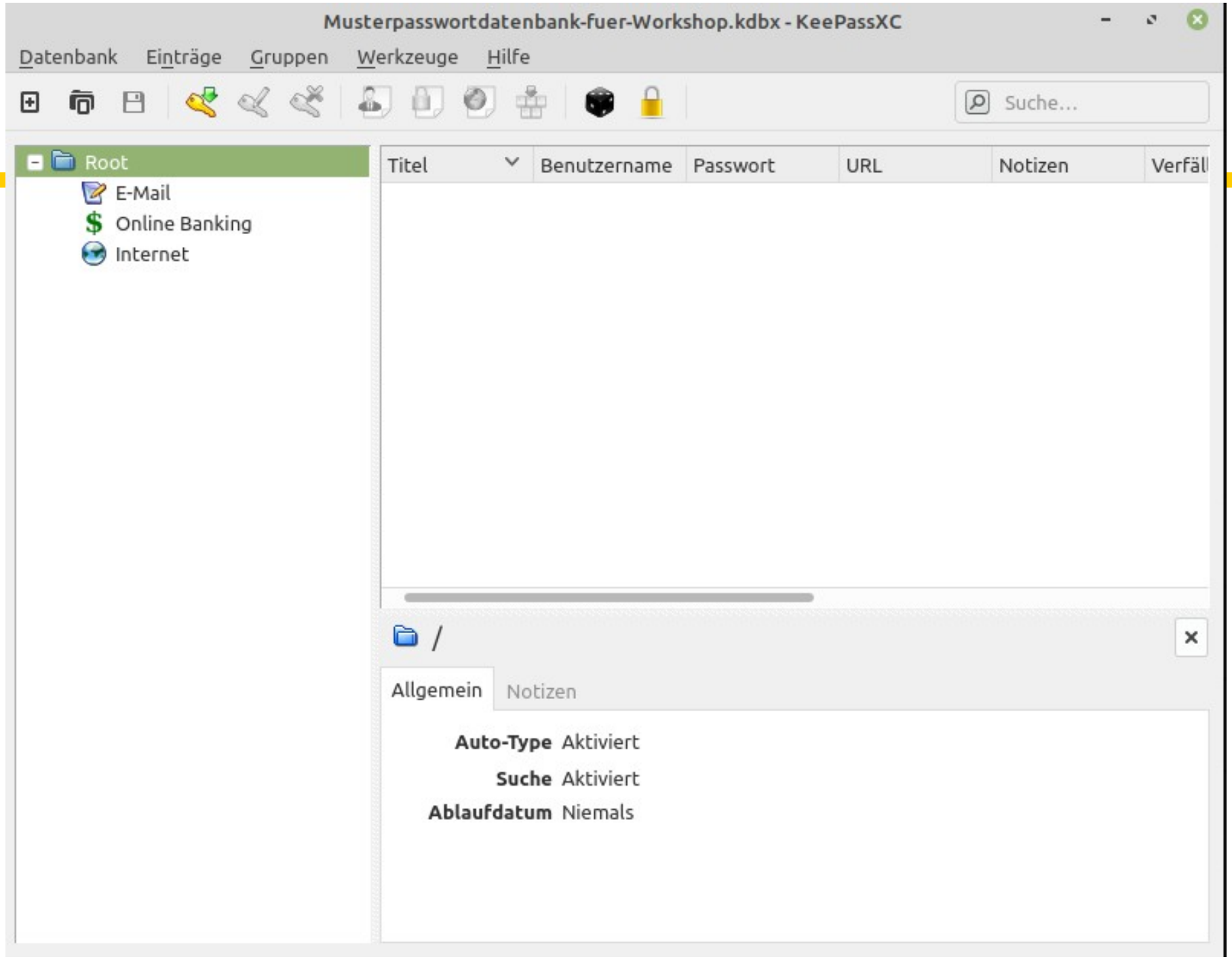
https://keepassxc.org/

Vorteile

- Freie Software
- Viele Plattformen
  - Win, Linux, Mac
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
  - Darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
  - „Setzt alles auf eine Karte“: PW-Datenbank gut sichern!
- *Komfort*
  - *Kein Sync zwischen verschiedenen Geräten*


Musterpasswortdatenbank-fuer-Workshop.kdbx - KeePassXC
Datenbank
Einträge
Gruppen
Werkzeuge
Hilfe
Suche...
Root
E-Mail
Online Banking
Internet
Titel
Benutzername
Passwort
URL
Notizen
Verfäll
/
Allgemein
Notizen
Auto-Type Aktiviert
Suche Aktiviert
Ablaufdatum Niemals

Starkes Masterpasswort finden

- Passwörter würfeln mithilfe einer Passwortliste
- Warum? → Entropie!
- Vorteil: nur dieses Passwort muss man sich merken
  - Masterpasswort
- Tipp: mind. 6 Wörter würfeln

How-To: Masterpasswort würfeln

- Zubehör
  - Wortliste mit deren Hilfe sich die Passphrase würfeln lässt (Link am Ende des Passwortteils)
  - 6-seitiger Würfel
- Funktionsweise
  - Je Wort wird 5 Mal gewürfelt und die Zahlen notiert
  - Dieses wird mind 6 Mal durchgeführt (also 6 * 5 = 30)
  - Alle worte hintereinander geschrieben (ohne Leerzeichen), ergeben die Passphrase
  - Diese muss man sich merken und kann als Masterpasswort für die Passwortdatenbank dienen

Weiterführende Literatur

- Kurzweilige Zusammenfassung des eben gesagten von Alexander Lehmann: „Passwörter einfach erklärt": https://vimeo.com/138839266
- Mike Kuketz, Sicheres Passwort wählen: Der Zufall entscheidet; abrufbar unter: https://www.kuketz-blog.de/sicheres-passwort-waehlen-der-zufall-entscheidet/
- Diceware-Liste zum „Würfeln“ von Passwörtern: http://world.std.com/~reinhold/diceware.html
- Zwei-Faktor-Authentifizierung: https://de.wikipedia.org/wiki/Zwei-Faktor-Authentifizierung

– Ende Passwörter –

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

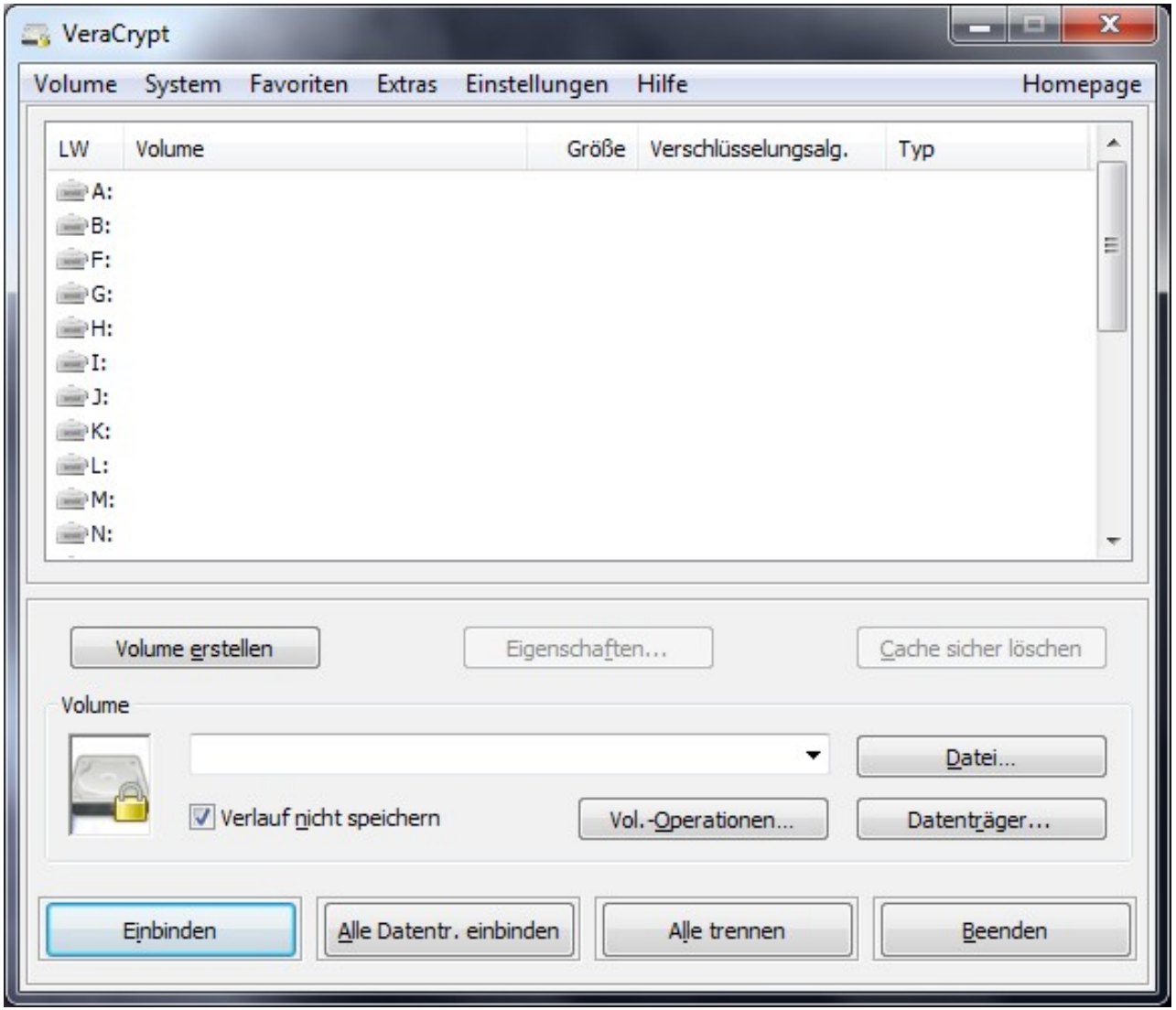
Software-Auswahl: VeraCrypt

- 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

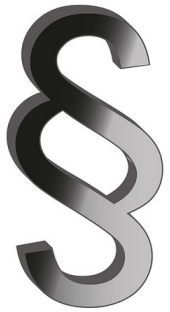
- Was will ich verschlüsseln?
- Starkes Passwort wählen
- Adminrechte notwendig
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen
- Größtes Sicherheitsrisiko ist fast immer der Nutzer!

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 –