Gute Passwörter

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.

Wie erschwert man das Knacken des Passworts?

- Brute Force
  - Länge = 10+ Zeichen
  - Verschiedene Zeichentypen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
  - Kein einzelnes Wort als Passwort verwenden
  - Keine Wörter aus dem persönlichen Umfeld verwenden (Namen, Geburtsdaten etc.)
- Social Engineering
  - Niemandem das Passwort verraten!

Starke Passwörter finden

- Wichtig:
  - Für jeden Dienst ein anderes Passwort verwenden!
  - Passwörter in regelmäßigen Abständen austauschen/ändern
- DBiR&dSd90M!
  - Merksatz: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMeloneBagger
  - Wortreihung
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwortgenerator

Zwei-Faktor-Authentifizierung

= Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

HowTo: Starke Passwörter merken?!

Passwortverwaltung

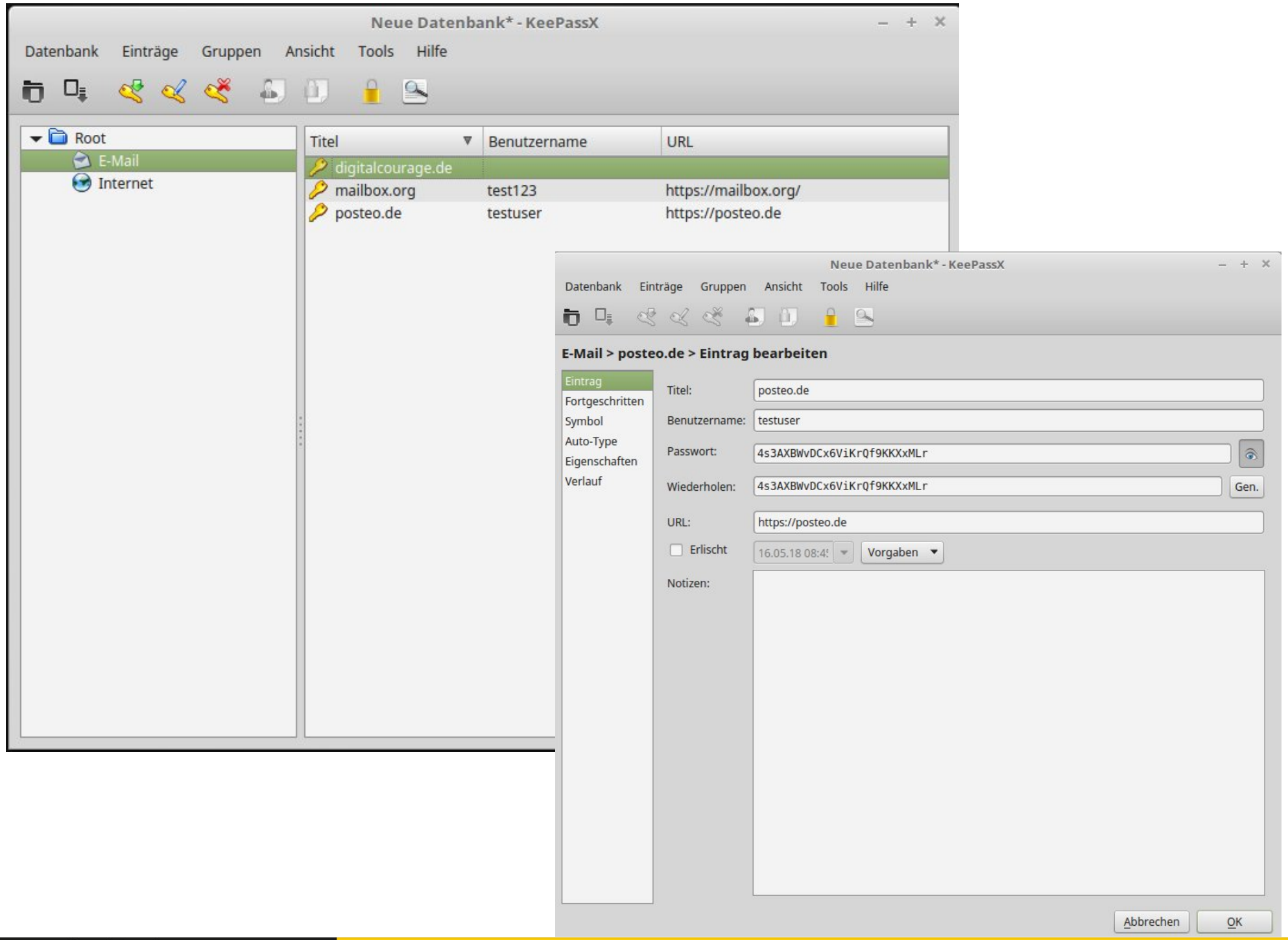
Software: **KeePassX**

Vorteile

- Freie Software
- Viele Plattformen
  - Win, Linux, Mac, Android
- 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


Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
Root
E-Mail
Internet
Titel
Benutzername
URL
digitalcourage.de
mailbox.org
test123
https://mailbox.org/
posteo.de
testuser
https://posteo.de
Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
E-Mail > posteo.de > Eintrag bearbeiten
Eintrag
Fortgeschritten
Symbol
Auto-Type
Eigenschaften
Verlauf
Titel:
posteo.de
Benutzername:
testuser
Passwort:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Wiederholen:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Gen.
URL:
https://posteo.de
Erlischt
16.05.18 08:4
Vorgaben
Notizen:
Abbrechen
OK

Starkes Masterpasswort finden

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

Dateiverschlüsselung

Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - Bei Verlust/Diebstahl des Laptops oder USB-Stick
  - Jeder der personenbezogene Daten speichert

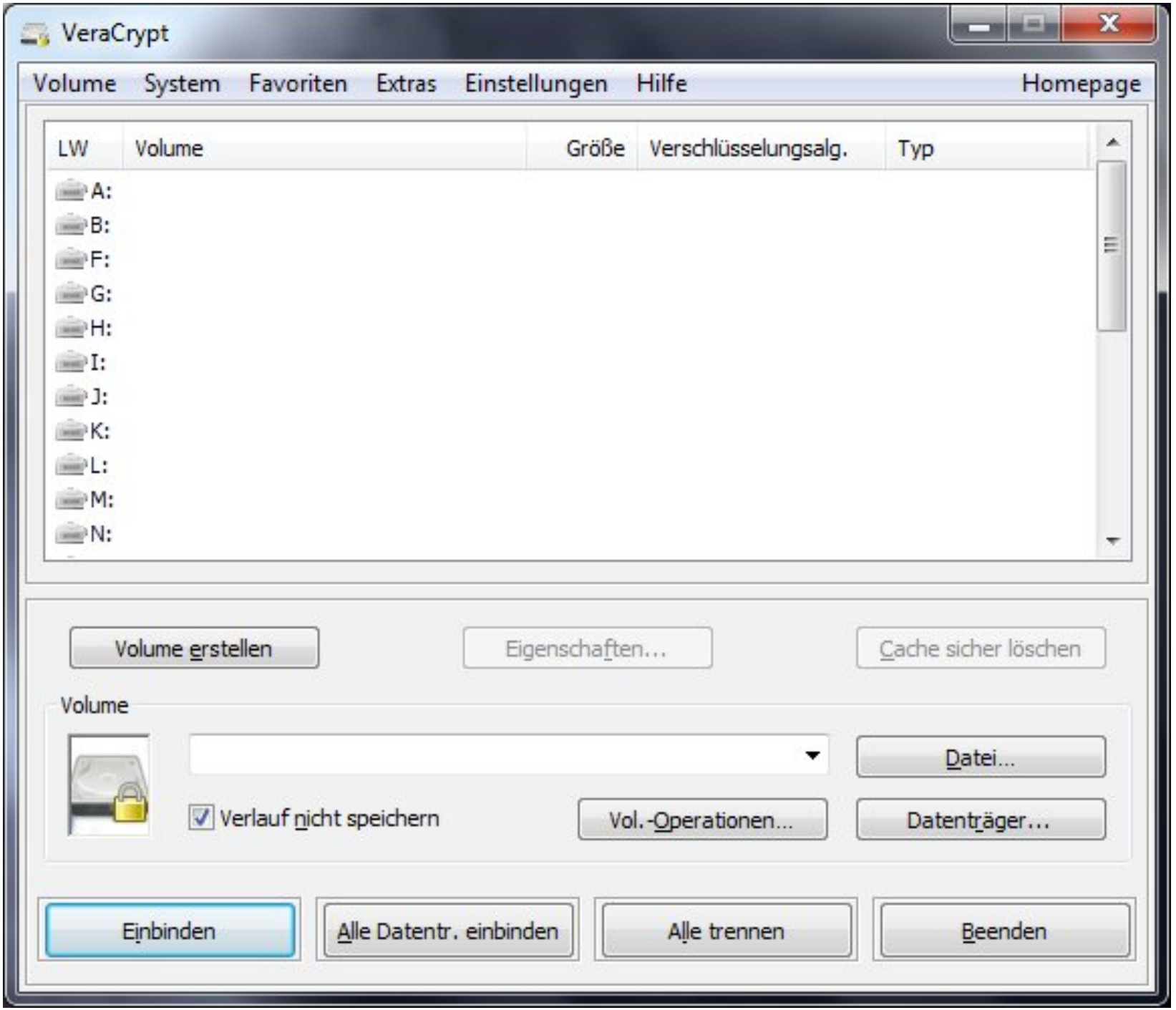
- Weil Ihr ein Grundrecht auf digitale Privats- und Intimsphäre habt!
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
  - sog. IT-Grundrecht, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

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


VeraCrypt
Volume
System
Favoriten
Extras
Einstellungen
Hilfe
Homepage
LW
Volume
Größe
Verschlüsselungsalg.
Typ
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Volume erstellen
Eigenschaften...
Cache sicher löschen
Volume
Datei...
Verlauf nicht speichern
Vol.-Operationen...
Datenträger...
Einbinden
Alle Datentr. einbinden
Alle trennen
Beenden

Über VeraCrypt

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

- **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 für 7z-Archive

- 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