PALAIS
Macht Menschen stark fürs Leben.

Crypto-Sticks

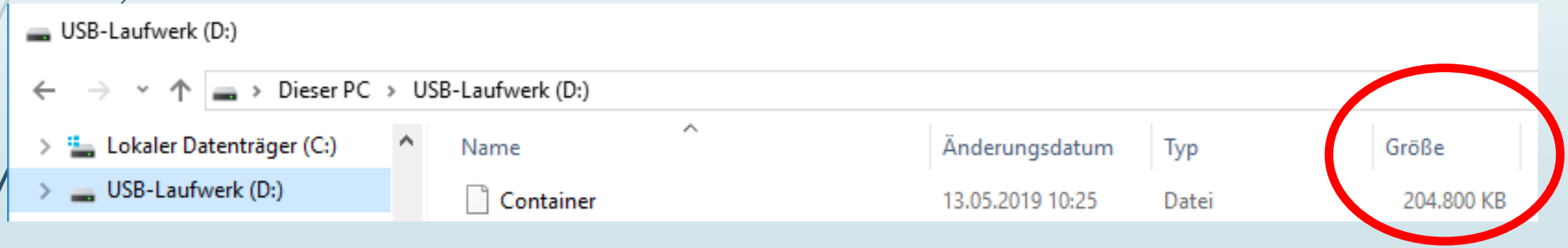
Verschlüsselte Datenspeicherung in unbekannter IT-Infrastruktur

Problemstellung – Schulsozialarbeit

- Schulsozialarbeiter arbeiten als Angestellte des freien Trägers in einem IT-Netzwerk des Schulträgers.
- Der Administrator dieses Netzwerks bzw. der PCs in der Schule hat Zugriff auf alle Daten, die auf den PCs gespeichert sind.
- Der Schulsozialarbeiter muss für seine Dokumentation sensible Daten (Schüler: „Ich bin schwul, traue aber nicht mich zu outen.“) auf dem PC speichern.
- Der Schul-Administrator darf auf diese Daten keinen Zugriff haben.

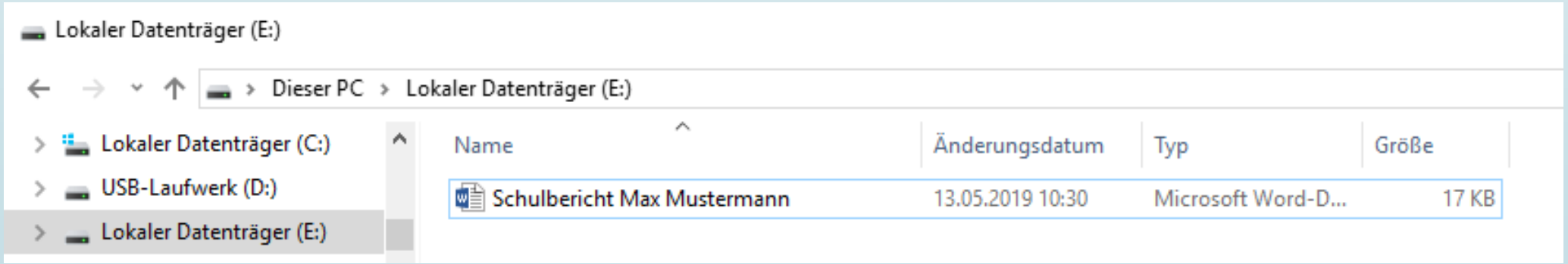
Lösung: Crypto-Sticks

- Es wird ein verschlüsselter „Container“ auf einem USB-Stick abgelegt in dem der Mitarbeiter alle seine Daten speichert.
- Der verschlüsselte Container gibt sich als beliebige Datei aus.



Lösung: Crypto-Sticks

- Es wird ein verschlüsselter „Container“ auf einem USB-Stick abgelegt in dem der Mitarbeiter alle seine Daten speichert.
- Der verschlüsselte Container gibt sich als beliebige Datei aus.
- Das Programm „VeraCrypt“ übernimmt die Verschlüsselung und Entschlüsselung des Containers.
- Entschlüsselt erscheint der Container als virtuelle Festplatte im System.



Lösung: Crypto-Sticks

- Es wird ein verschlüsselter „Container“ auf einem USB-Stick abgelegt in dem der Mitarbeiter alle seine Daten speichert.
- Der verschlüsselte Container gibt sich als beliebige Datei aus.
- Das Programm „VeraCrypt“ übernimmt die Verschlüsselung und Entschlüsselung des Containers.
- Entschlüsselt erscheint der Container als virtuelle Festplatte im System.
- Auf dieser virtuellen Festplatte speichert der MA seine Dateien.
- Beim verschlüsseln verschwindet die virtuelle Festplatte wieder aus dem System.

VeraCrypt

- Freie, quelloffene Software zur Festplattenverschlüsselung.
- „Frei“ = verursacht keine Kosten
- „Quelloffen“ (Open-Source) = keine unbekannten Hintertüren
- Unterstützt alle bekannten und als sicher geltenden Verschlüsselungsalgorithmen.
  - z.B. „AES“, „Serpent“, „Twofish“, etc.
- => Die Verschlüsselung ist nur über das Passwort zu knacken.

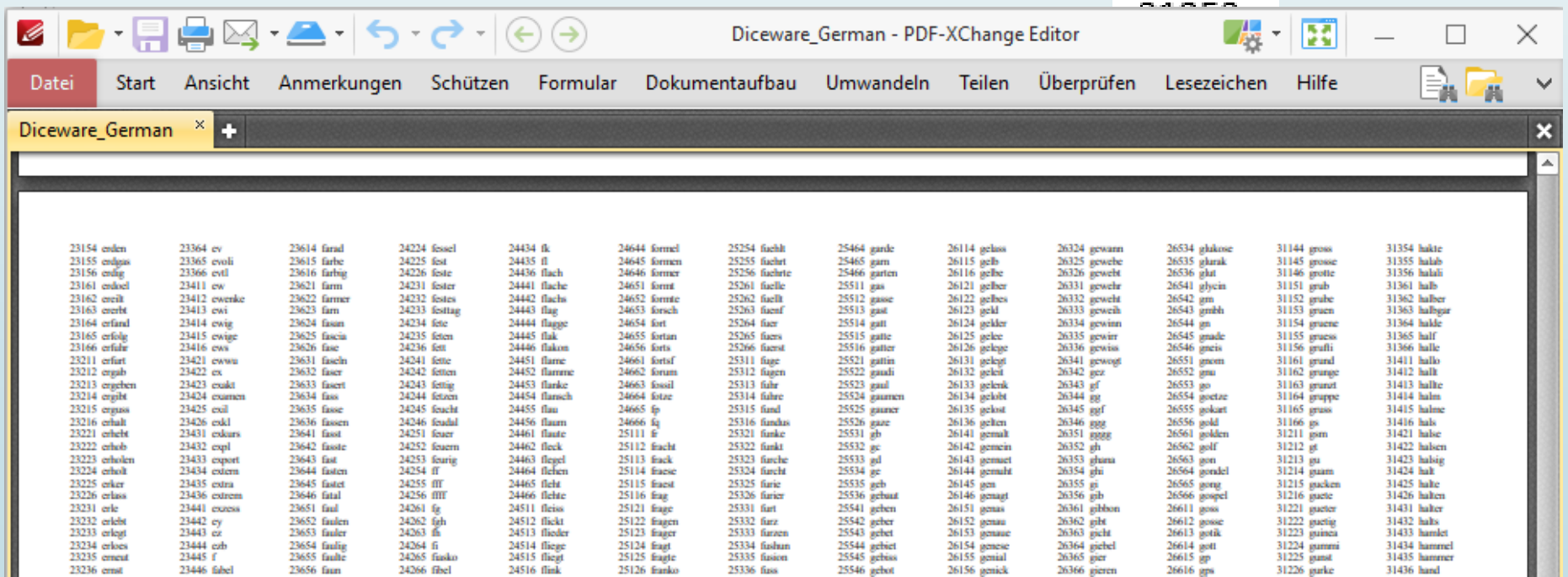
Sicheres Passwort erstellen

- Das Passwort ist das entscheidende Element
- Dem Mitarbeiter wird das Passwort vorgegeben.
  - => Das Passwort ist sicher genug.
  - => Das Passwort geht nicht verloren, da in der IT separat abgelegt.
- Der Mitarbeiter muss auf die Sicherheitsbedeutung des Passworts geschult werden.
  - *Kein Passwort an den Bildschirm heften!*
- Anforderungsprofil des Passworts:
  - Ausreichende Länge besitzen, um sicher zu sein.
  - Der Mitarbeiter muss es sich merken können.
- Lösung: ***Diceware***-Methode

Diceware-Methode

- Es werden mit einem Würfel 6 fünfstellige Zahlenblöcke ausgewürfelt.
- Vergleich mit der *Diceware*-Liste
  - Eine Liste mit 7776 Wörtern und Zeichenketten

23253
45234



Diceware-Methode

- Es werden mit einem Würfel 6 fünfstellige Zahlenblöcke ausgewürfelt.
- Vergleich mit der *Diceware*-Liste
  - Eine Liste mit 7776 Wörtern und Zeichenketten
- Das Passwort lautet dann:
  - ersatz odor gz junker sofa frager
- ~77-Bit Entropie
- Benötigte Zeit zum knacken des Passworts:
  - ~$1{,}76 * 10^{41}$ Jahre
- Genauso sicher wie: Dh$245Sdf%GDFG$%ASfgsdfg345,.!

23253	23253 ersatz
45234	45234 odor
31252	31252 gz
34142	34142 junker
55333	55333 sofa
25123	25123 frager

Einrichtung der Crypto-Sticks

- Veracrypt muss auf dem PC installiert werden
- Der verschlüsselte Container muss auf dem USB-Stick erstellt werden
  - Macht die IT-Abteilung vorab
- Das Entschlüsseln des Containers muss so vorkonfiguriert werden, dass der Mitarbeiter nach einstecken des USB-Sticks nur das Passwort eintippen muss.
- Dies wird über TeamViewer von der IT direkt beim Mitarbeiter eingerichtet. Dabei wird der Mitarbeiter in der Handhabung des Programms geschult.
- Alternativ:
  - Anleitungen
  - Schulungen & Vorführungen

Arbeitsablauf im Alltag

- 1. USB-Stick einstecken.
- 2. Passwort in das automatisch erscheinende Fenster eintippen.
- 3. *Arbeiten*
- 4. Auf die Veracrypt-Verknüpfung klicken.
- 5. „Trennen“ klicken.

Probleme

- Zur Installation von Veracrypt werden Admin-Rechte benötigt.
- Datensicherung/Backups
  - Aufgrund der Datensicherung wird auch nicht der gesamte Stick verschlüsselt sondern mit dem Container gearbeitet.
- Virenscanner/Firewalls
- KeyLogger
  - Verschlüsselung kann nur über das Passwort aufgebrochen werden.

PALAIS
Macht Menschen stark fürs Leben.

Vielen Dank! ☺