DIGITALE SELBSTVERTEIDIGUNG: FESTPLATTEN-VERSCHLÜSSELUNG

1 WO SIND DIE PROBLEME?

- diverse sensible Daten auf unseren Festplatten – von privaten Fotos bis zu Geschäftsgeheimnissen
- gerade auf mobilen Geräten größere Gefahr, in die falschen Hände zu geraten

2 WAS KÖNNEN WIR TUN?

- *TrueCrypt* – Festplatten-Verschlüsselung
- entweder ganze Festplatte/Partition oder Datei-Container mit enthaltener virtueller Festplatte
- Verschlüsselung mit Passwort oder Schlüssel-Datei (auf USB-Stick o. ä.)
- Problem: Zwang zur Passwort-Herausgabe
- Lösung: „Hidden Container“
  - Es ist nicht erkennbar, ob innerhalb eines Containers noch ein zweiter, mit einem anderen Schlüssel verschlüsselter Container vorhanden ist.
  - Bei Zwang wird Schlüssel des äußeren Containers heraus gegeben und Existenz des inneren abgestritten.
    ⇒ Plausible Abstreitbarkeit – Plausible Deniability
  - Weniger kritische Daten (z. B. Kontoauszüge) im äußeren Container, hochsensible Daten (z. B. Gesundheut) im inneren.

3 ALTERNATIVEN

- *Ubuntu*: Benutzerverzeichnis standardmäßig verschlüsselt
  (allerdings Datei-weise ⇒ Anzahl, Größe und Verteilung der Dateien auch in verschlüsselten Daten sichtbar)
- Alle Linux-Distributionen: *dm-crypt* zur Verschlüsselung ganzer Festplatten (und Partitionen)

PIRATEN INFORMIEREN