DIGITALE SELBSTVERTEIDIGUNG: PASSWÖRTER

1 WO SIND DIE PROBLEME?

- Sicherheitslücken bei Passwort-Übermittlung oder -Speicherung:
  Auf dem (möglicherweise unverschlüsselten) Weg durch das Internet oder bei Sicherheitslücken der besuchten Webseiten können Passwörter in falsche Hände gelangen.
- Phishing:
  Passwörter werden durch mehr oder weniger gut gefälschte Webseiten abgefangen.
- Brute-Force:
  Wörterbücher mit häufigen Passwörtern werden systematisch durchprobiert.
- Bestandsdatenauskunft (in Kraft seit 1. Juli 2013):
  Unternehmen müssen Passwörter ihrer Kunden in vage bestimmten Fällen an Behörden rausgeben.

2 WAS KÖNNEN WIR TUN?

- für jeden Dienst unterschiedliche Passwörter
  - zumindest getrennte Passwörter für wirklich wichtige Dienste – Bank, Shops mit hinterlegten Kreditkarten-Daten, E-Mail

  ⇒ Lücke bei einem hat keine Auswirkungen auf andere
- zufällig generierte Passwörter
  - keine Namen, keine einfachen Wörterbuch-Wörter
  - nicht die Anfangsbuchstaben des Lieblings-Songs
  - nicht nur einfache Ersetzungen („o“ durch „0“ o. ä.)

  ⇒ Knacken durch systematisches Durchprobieren fast unmöglich
- oder: *mehrere*, völlig *unabhängige* Wörter hintereinander
  - 1 000 Wörter kann ein Rechner schnell durchprobieren
  - 1 000 * 1 000 * 1 000 Kombinationen von Wörtern nicht

  ⇒ leicht zu merken, schwer zu knacken

3 IST DAS NICHT VIEL ZU AUFWÄNDIG?

- Passwort-Safe, z. B. *KeePassX*
- viele Passwörter durch ein gemerktes Haupt-Passwort geschützt
- wenn Haupt-Passwort sicher genug:
  auch Online-Sicherheitskopie (Dropbox o. ä.) unbedenklich
- zufällige Generierung von einzigartigen Passwörtern für jede einzelne Website

PIRATEN INFORMIEREN