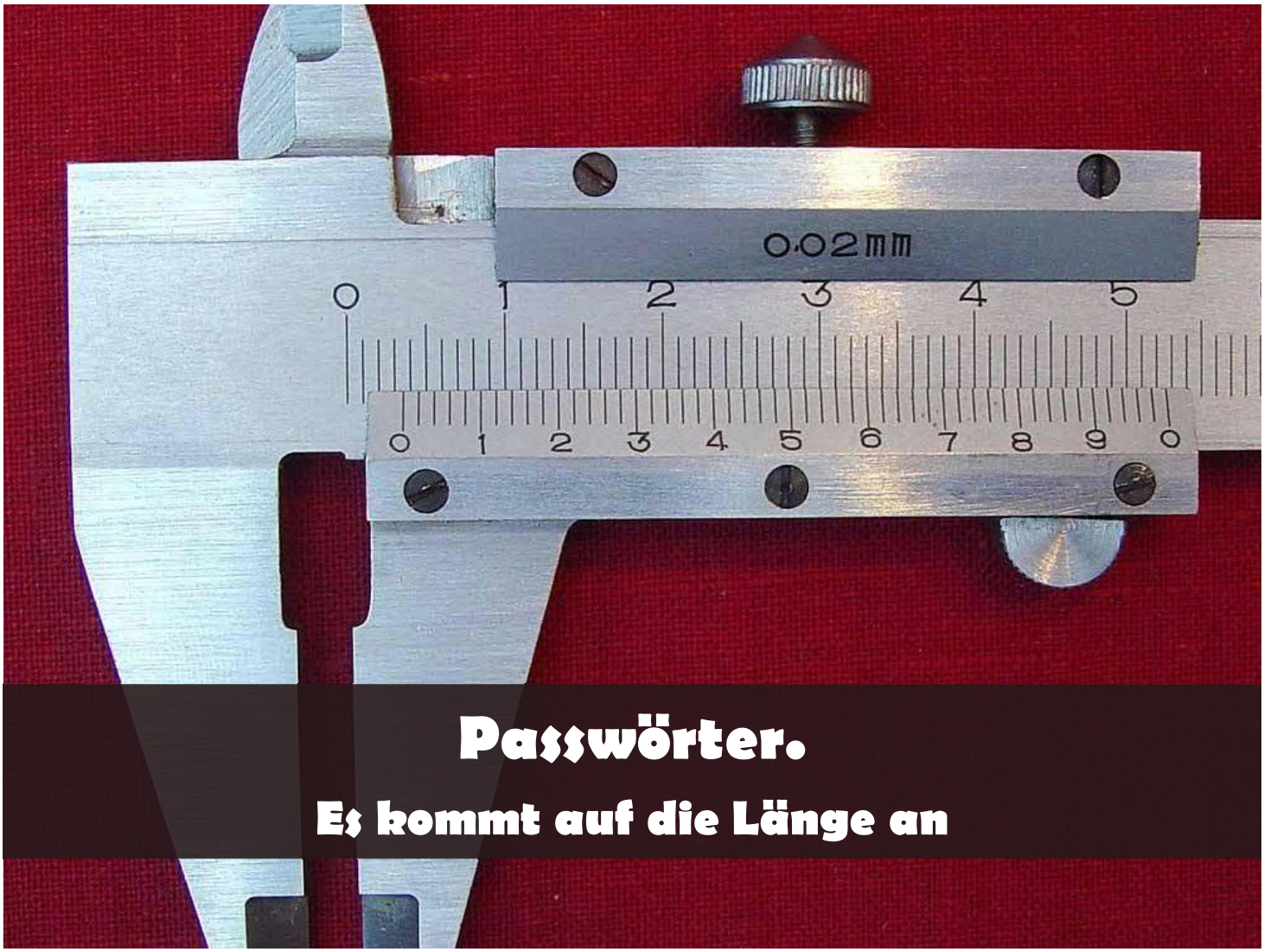


Passwörter.

Es kommt auf die Länge an

Dieses Schloss hat 10^3 Einstellungen: 10 * 10 * 10 = 1000

Zum Probieren einer Kombination benötigt man 2 Sekunden.

Wer die Kombination vergisst, braucht höchstens 2000 Sekunden bis das Schloss offen ist. Theoretisch.

Meist ist das Schloss nach 500 Versuchen offen.

Das sind 1000 Sekunden oder 16 Minuten.

Normale heutige Computer probieren

600 Millionen

Passwörter (1)

REFA-Zeitaufnahmebogen
für Abläufe ohne Wiederholungen
Ablage-Nr.
Blatt
des Arbeitsauftrages
Beginn
Uhrzeit
Menge
Dauer
Zeit in
3JEWELS
SHOCKPROOF

pro Sekunde

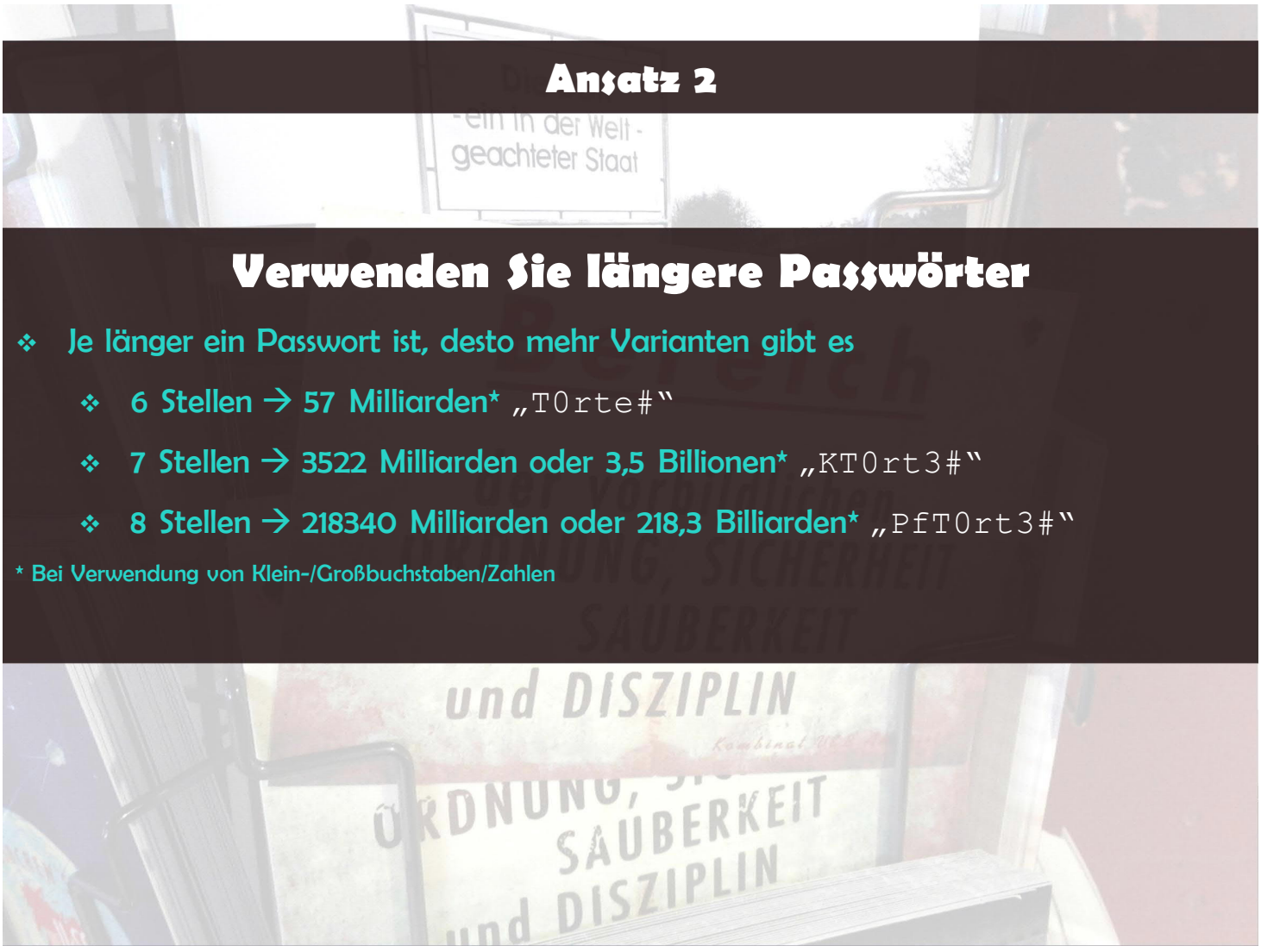
Wie können Sie sicherere Passwörter verwenden?

Ein wenig Mathematik

Ansatz 1

Erhöhen Sie die Anzahl verwendeter Zeichen

- Ein 6stelliges Passwort kann man so schreiben
  - **Kleinbuchstaben** und **Zahlen** "t0rt3n"
    → **2** Milliarden Varianten
  - **Klein-/Großbuchstaben/Zahlen** "T0Rt3n"
    → **57** Milliarden Varianten
  - **Klein-, Großbuchstaben/Zahlen/Zeichen** "T0rt3#"
    → **208** Milliarden



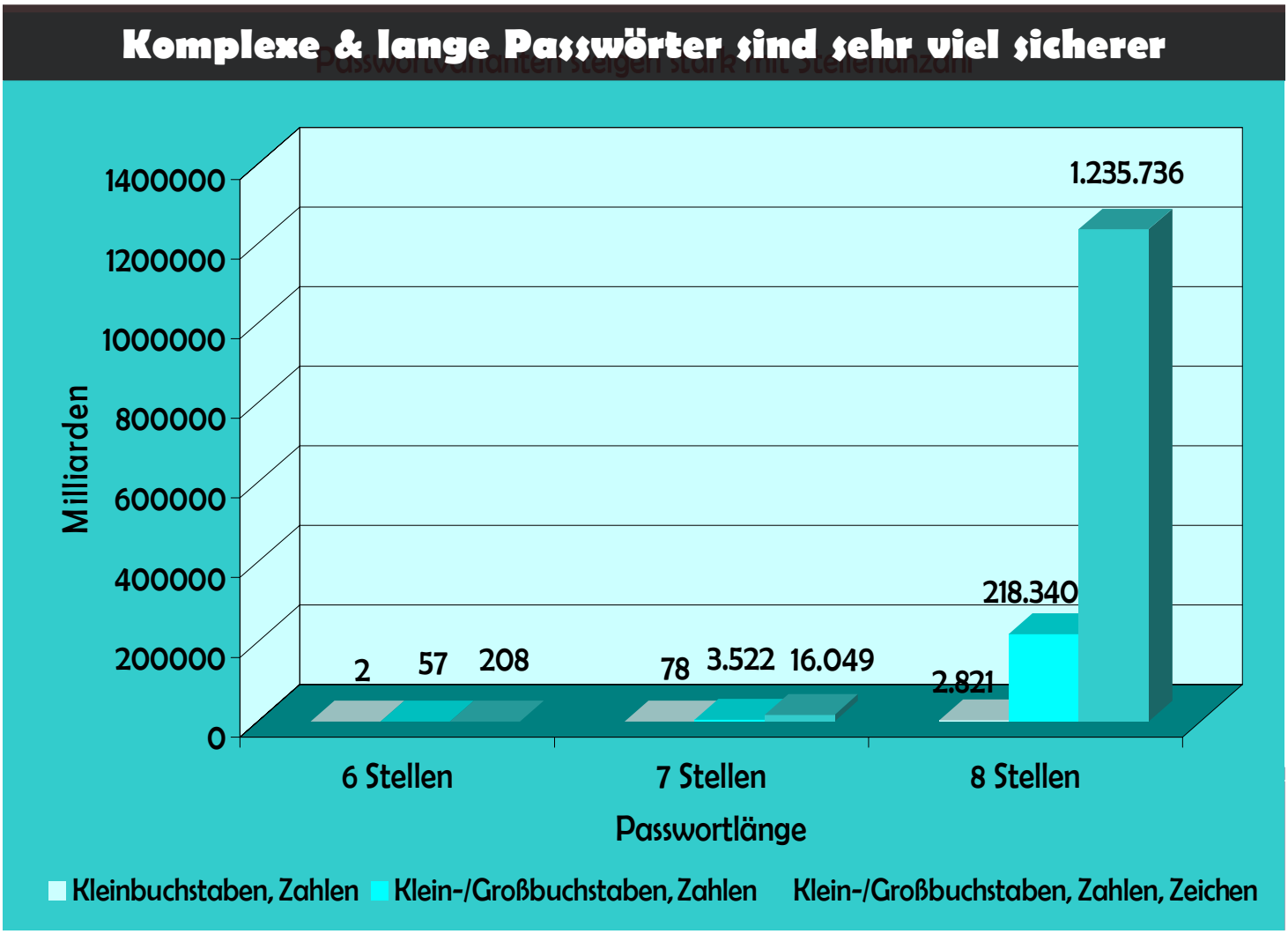
Ansatz 2

Verwenden Sie längere Passwörter

- Je länger ein Passwort ist, desto mehr Varianten gibt es
  - 6 Stellen → 57 Milliarden* „T0rte#“
  - 7 Stellen → 3522 Milliarden oder 3,5 Billionen* „KT0rt3#“
  - 8 Stellen → 218340 Milliarden oder 218,3 Billiarden* „PfT0rt3#“

* Bei Verwendung von Klein-/Großbuchstaben/Zahlen

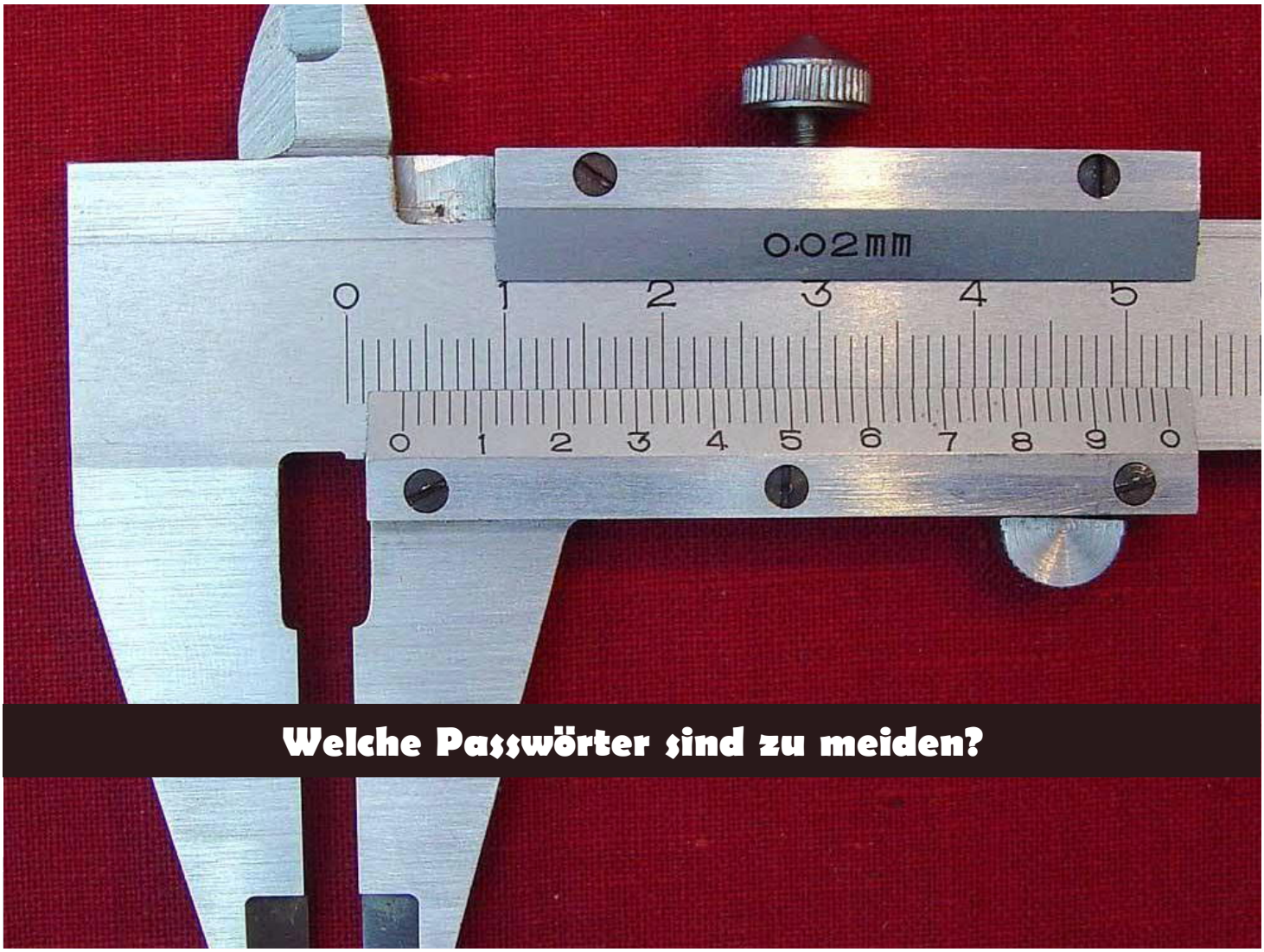
Komplexe & lange Passwörter sind sehr viel sicherer



Frage
Bereich
der vorbildlichen
ORDNUNG, SICHERHEIT
SAUBERKEIT
Wie viel Stellen hat Ihr nächstes Passwort?

Anmeldung zum kostenfreien Newsletter

http://www.daleth-datenschutz.de/newsletter.html



Welche Passwörter sind zu meiden?

Sichere Passwörter – eine Investition in Hirnschmalz

Ungeeignete Passwörter

- **Reihen** oder **Wiederholungen** von Zahlen oder Buchstaben
  - 123456
  - 111111
  - Abc123
  - Qwertzu1

Sichere Passwörter – eine Investition in Hirnschmalz

Ungeeignete Passwörter

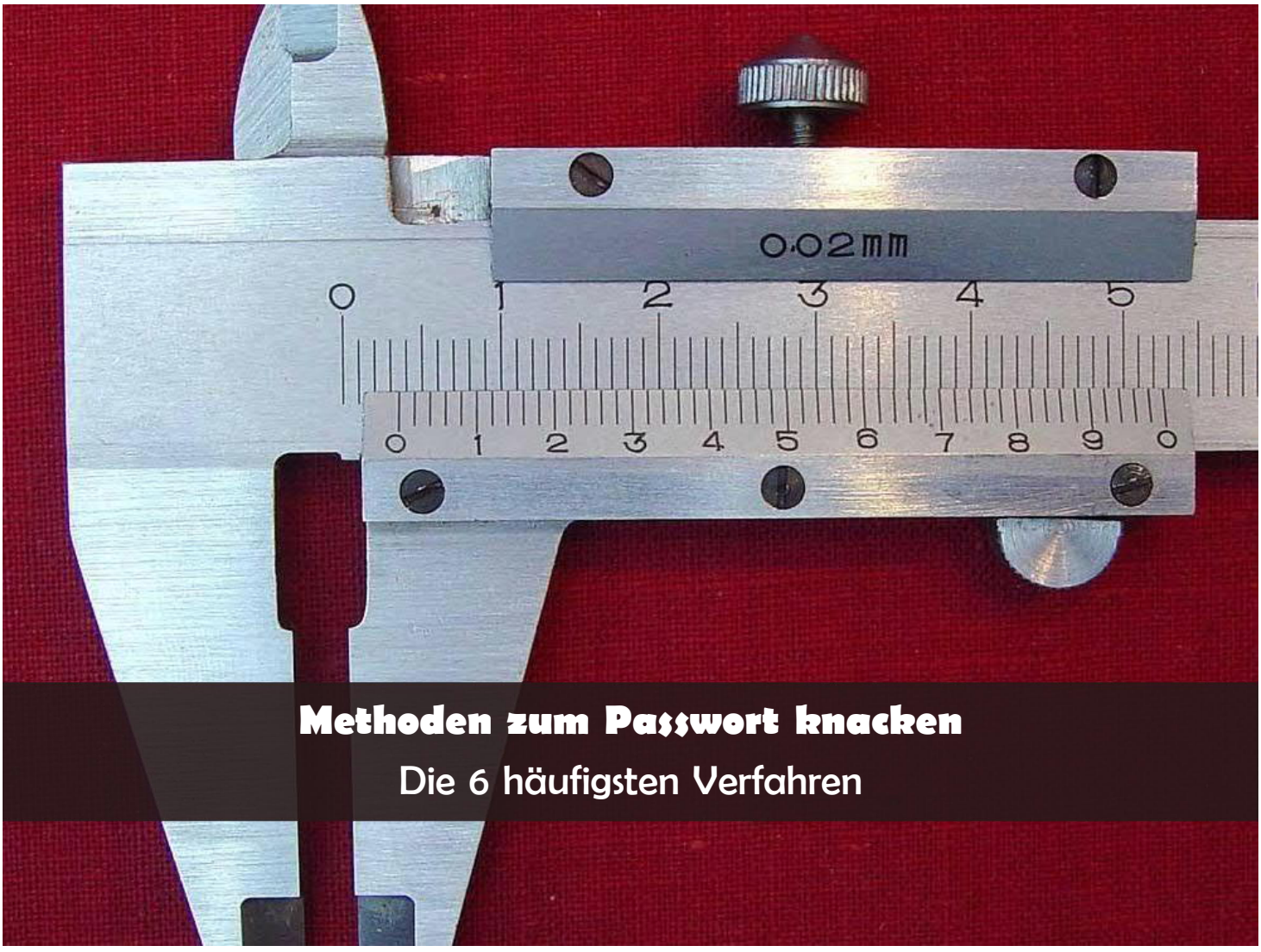
- Namen von **Partnern, Tieren oder Pflanzen, Comic-Helden, Bands, Städten, Sportarten, Autos.**
- Auch nicht mit angehängten Zahlen
  - fussball – maus – rose – audi – clio – batman – beatles – bonn
  - stones1 - puhdys42 – fixfax2 – atze2

Sichere Passwörter – eine Investition in Hirnschmalz

- Ungeeignete Passwörter
- Ganz simple Passwörter
  - passwort als Passwort ist uncool
  - youtube für Youtube
  - Usw.

Sichere Passwörter – eine Investition in Hirnschmalz

- Ungeeignete Passwörter
  - Geburtstag,
  - Postleitzahl,
  - Telefonnummer oder
  - Hausnummer



Methoden zum Passwort knacken

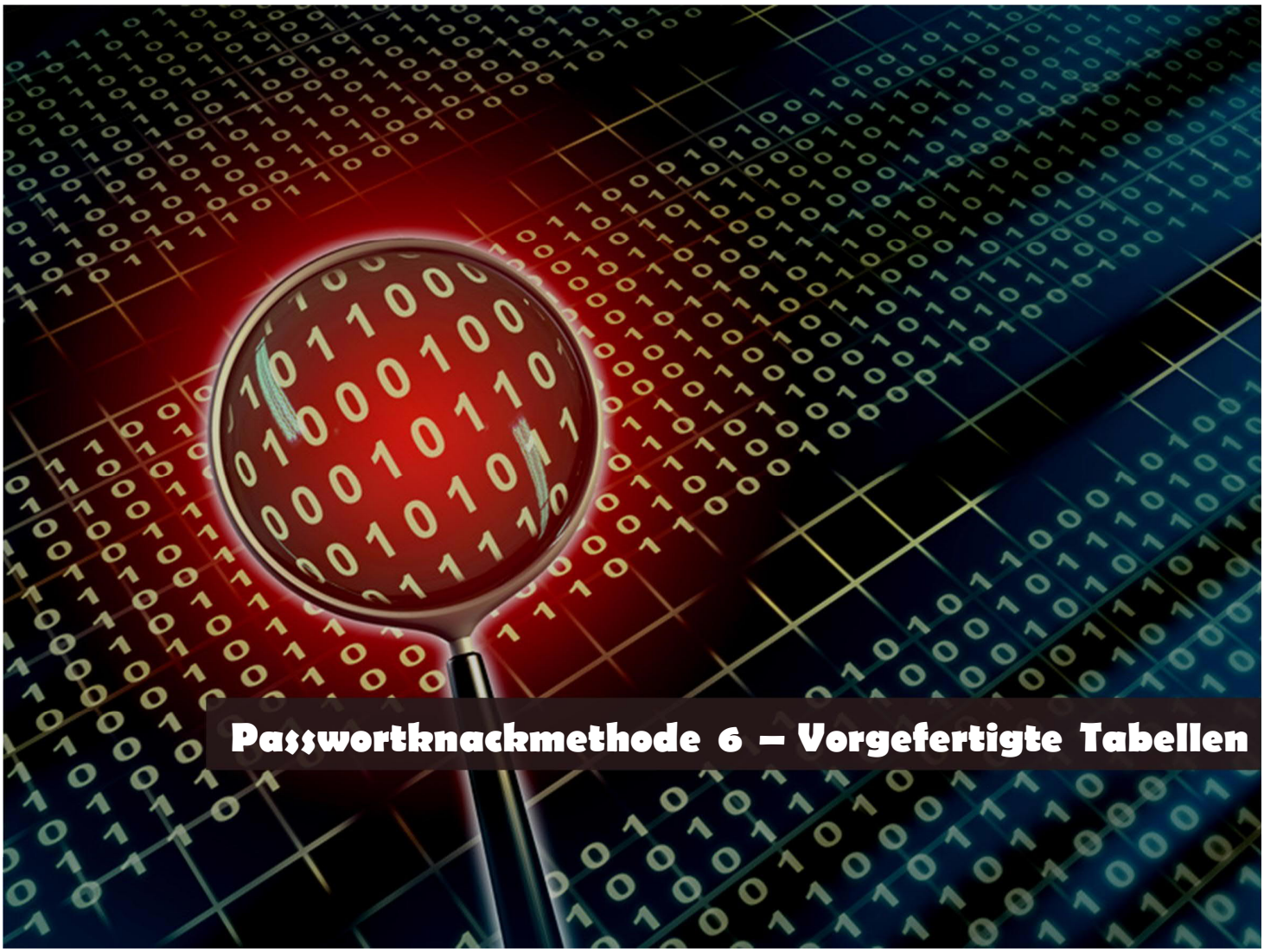
Die 6 häufigsten Verfahren

Passwortknackmethode 1 – Raten

Passwortknackmethode 2 – Klauen

Passwortknackmethode 3 – Wörterbuchvergleich

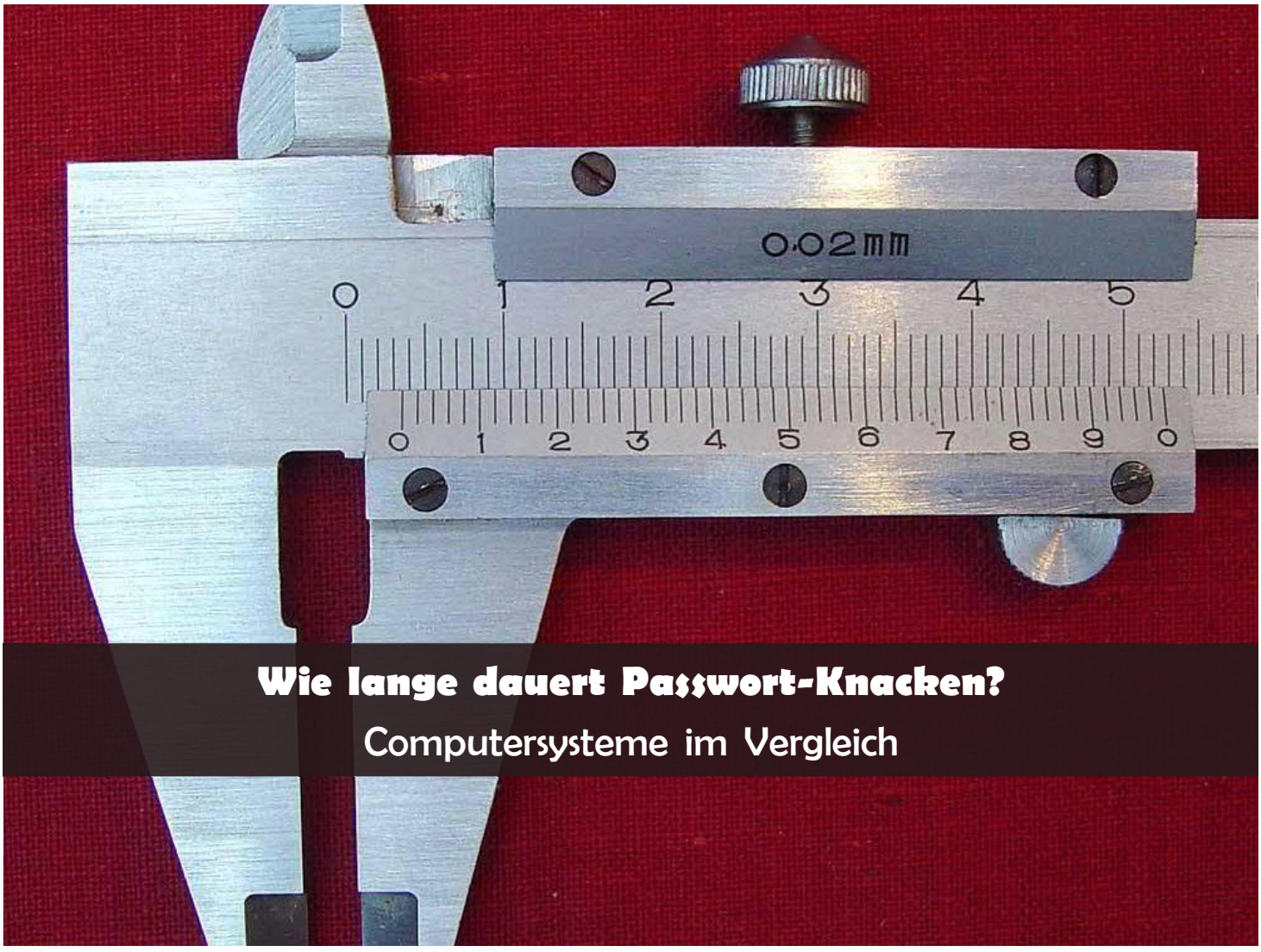
Passwortknackmethode 5 – Brutale Gewalt



Passwortknackmethode 6 – Vorgefertigte Tabellen

Anmeldung zum kostenfreien Newsletter

http://www.daleth-datenschutz.de/newsletter.html



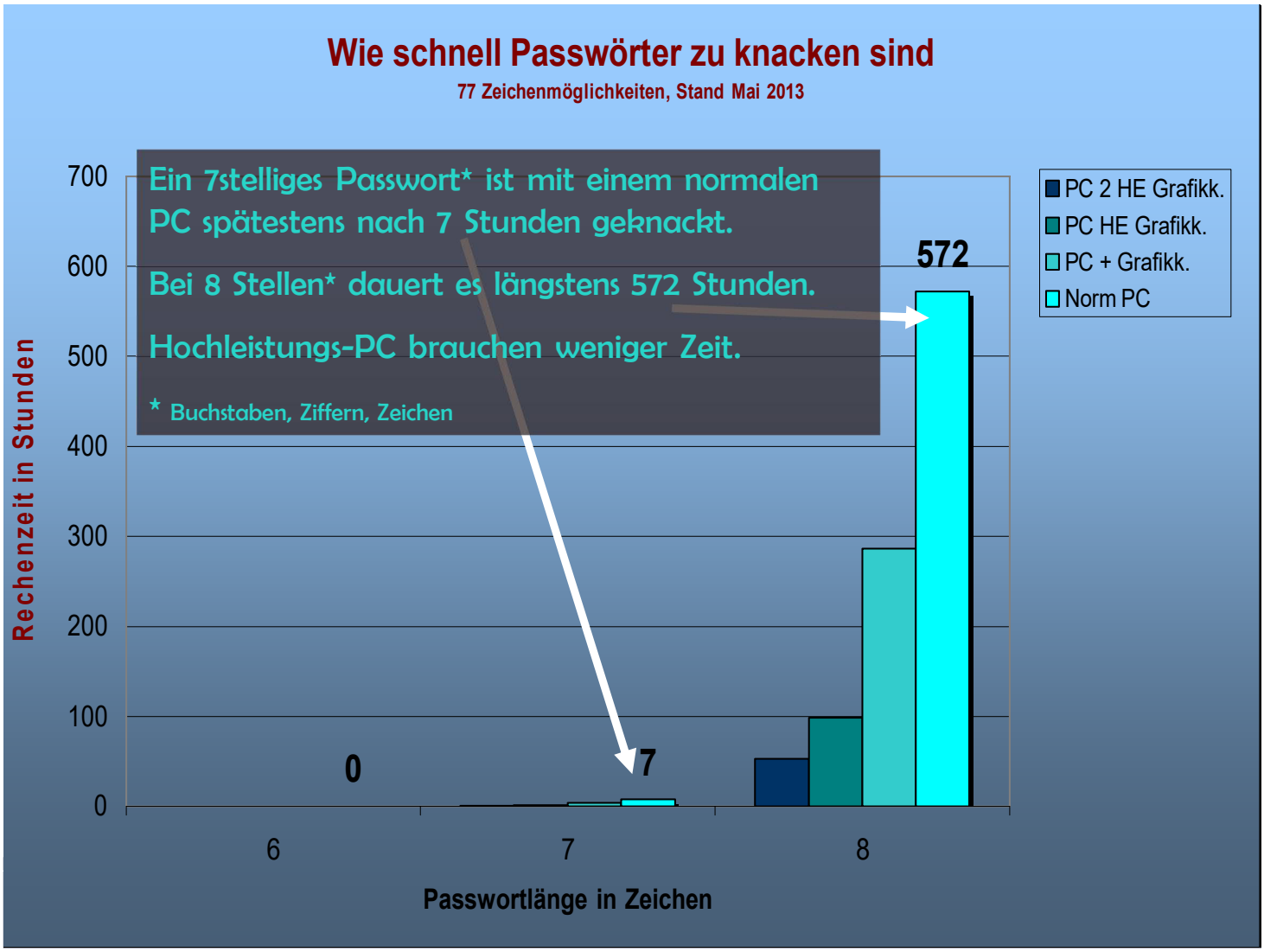
Wie lange dauert Passwort-Knacken?

Computersysteme im Vergleich

Passwortknacken mit Computern

Mögliche Versuche pro Sekunde

1.	Normaler PC	0,6 Milliarden
2.	PC mit Grafikkarte	1,2 Milliarden
3.	PC mit High-End Grafikkarte	3,5 Milliarden
4.	PC mit 2 High-End Grafikkarten	6,5 Milliarden


Wie schnell Passwörter zu knacken sind
77 Zeichenmöglichkeiten, Stand Mai 2013
Ein 7stelliges Passwort* ist mit einem normalen PC spätestens nach 7 Stunden geknackt.
Bei 8 Stellen* dauert es längstens 572 Stunden.
Hochleistungs-PC brauchen weniger Zeit.
* Buchstaben, Ziffern, Zeichen
Rechenzeit in Stunden
700
600
500
400
300
200
100
0
0
7
572
6
7
8
Passwortlänge in Zeichen
PC 2 HE Grafikk.
PC HE Grafikk.
PC + Grafikk.
Norm PC

Wie schnell ist Ihr Passwort geknackt?

Messen Sie selbst: http://zuse.et-inf.fho-emden.de/rechner.php

Nach einer Passwortänderung ist die Wahrscheinlichkeit des Vergessens am größten.
Ein Zettel in der Brieftasche hilft über die ersten Tage.

Anmeldung zum kostenfreien Newsletter

http://www.daleth-datenschutz.de/newsletter.html

Daleth-Datenschutz: c/o Speech & Phone GmbH, Bredereckstr. 4, 12621 Berlin, www.daleth-datenschutz.de
Bilder: Flickr – malegets, Flickr – GuySie, Flickr – jslahoe, Flickr – dierk schaefer, Flickr – murdelta, Wikimedia – Minute, Brockhaus-Efron, Grappling - **Quellen:** (1) http://zuse.et-inf.fho-emden.de/rechner.php 14.10.13, (2) http://www.t-online.de/computer/sicherheit/id_42545412/viele-passwoerter-wegen-moderner-grafikkarten-bald-unsicher.html