



Technische
Universität
Braunschweig



Stabsstelle CISO



IT-Sicherheitstipps für AnwenderInnen (un)sichere Passwörter und wie man es besser macht

Dr. Christian Böttger / Sebastian Homann, 10.09.2021



(un)sichere Passwörter

- Einführung
- Geschichte der Passwortregeln
- Passwortregeln (im GIZ)
- Ein „gutes“ Passwort
- Tipps zum Erstellen
- Testen von Passwörtern
- Tools

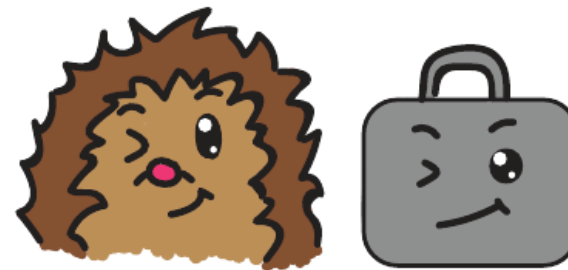


Wieviele Passwörter haben Sie?

- A) 1
- B) <10
- C) <20
- D) >50

Einführung

- Identifizierung
- Stichwort „Parole“
- Geheimnis, das eigentlich schon offenbart wurde
- Weiterentwicklung 2-Factor-Authentication
 - Zwei verschiedenen Merkmale
 - „Wissen“
 - „Haben“



Geschichte der Passwortregeln

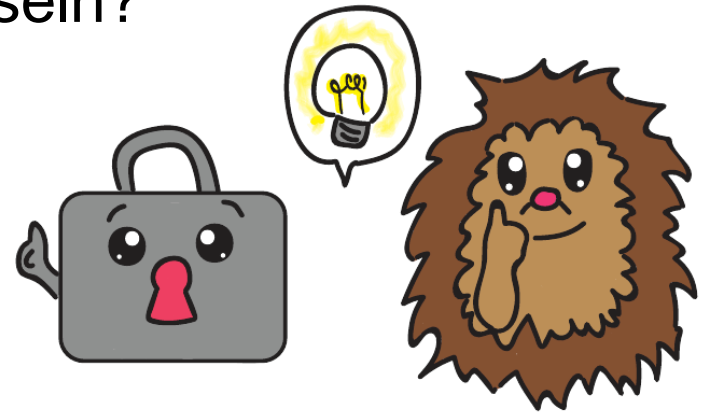
- Passwortregeln unterliegen einem Wettbewerb
- Ständiger Kampf um die Parameter

Aufschreiben vs. nicht aufschreiben?

Wie lang ist denn nun lang genug?

Wie oft soll man das Passwort wechseln?

Komplexität vs. Merkbarkeit



Passwortregeln (im GITZ)

Es muss Zeichen aus mindestens 3 der folgenden Gruppen enthalten:

- Großbuchstaben A - Z
- Kleinbuchstaben a - z
- Ziffern 0 - 9
- folgende Sonderzeichen:
▪ + _ . , : -



Weiterhin gilt:

- Es darf nicht Teile des Namens oder der Benutzerkennung enthalten, die länger als 2 Zeichen sind
- Es muss 12 bis 30 Zeichen lang sein
- Es darf nicht mit Minuszeichen (-) anfangen
- Es sollte nicht den letzten 10 Passwörtern entsprechen

Passwortregeln (im GITZ)

Es muss Zeichen aus mindestens 3 der folgenden Gruppen enthalten:

- Großbuchstaben A - Z
- Kleinbuchstaben a - z
- Ziffern 0 - 9
- folgende Sonderzeichen:
▪ + _ . , : -



Ihr temporäres Kennwort lautet: **hi4Tohqu**

Bitte ändern Sie Ihr Kennwort schnellstmöglich unter

<https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern>

Schriftprobe:

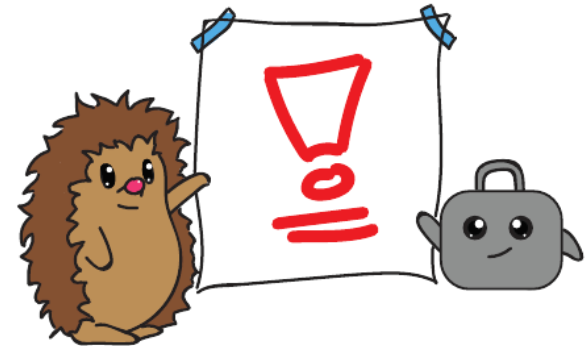
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

0123456789

Ein „gutes“ Passwort

- ... das gibt es nicht
- Gegenbeispiele
 - „asdf1234“
 - „qwertz123“
 - „Passwort“
 - Persönliche Daten
- Anwendungszweck
- Login
 - Unterbindung von Angriffsversuchen
- Brute-Force (z. B. ZIP-Datei, Crypto-Container)
 - Kein Schutz gegen wiederholte Versuche
- WLAN



Tipps

- Unser Tipp: FAQ#1000795 im Ticketsystem
- Sätze auswählen, Anfangsbuchstaben verwenden
- Eigene Regeln ausdenken um einen Namen einfließen zu lassen
- „Fiese“ Passwörter generieren lassen
 - <https://www.tu-braunschweig.de/it-sicherheit/pwsec>
- Für jeden Dienst ein eigenes Passwort
 - sonst Zugriff auf das elektronische Leben



Testen von Passwörtern

Interaktiver Part – Wie gut ist meine Passwort-Idee?

<https://password.kaspersky.com/de/>

<https://haveibeenpwned.com/>

Tools

- Notizbuch in Papier
- Passwortgenerator
- Passwortcontainer
 - Eigene Anforderung
 - Für verschiedene Betriebssysteme verfügbar
 - **KeePass**-kompatible Produkte (KeePass, KeePassXC, ...)
- Letzter Tipp: Hinterlegen Sie bei uns Ihre Mobilfunknummer im BDD!



Geschafft!

**Vielen Dank
für die Aufmerksamkeit!**

Einfache Fragen? ;-)



Weitere Infos:

https://studip.tu-braunschweig.de/seminar_main.php?auswahl=bc863707104006d8b2c63d11f6a60ed0
<http://it-sicherheit.tu-braunschweig.de/>
<https://blogs.tu-braunschweig.de/it/category/informationssicherheit/informationssicherheit-auf-einen-blick/>

und beim IT-Service-Desk des Gauß-IT-Zentrums

Tel. +49.531.391.5555

it-service-desk@tu-braunschweig.de

<https://www.tu-braunschweig.de/it/service-desk>

Vielen Dank für Ihre Aufmerksamkeit!



<https://pixabay.com/de/baby-lernen-laptop-frage-2709666/>
CC0 Lizenz



**Technische
Universität
Braunschweig**

10. September 2021 | Sebastian Homann + Christian Böttger | (un)sichere Passwörter | Seite 13



IT-SAD
IT Security Awareness Days