Ist Ihr Passwort noch sicher?
2FA in der Praxis

@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 3. April 2019

THOMAS KRENN®

Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG
  Niederlassung Österreich
- Diplomstudium
  Computer- und Mediensicherheit
- Erfahrung in Web Operations,
  Linux und HA
- Cyber-Security-Practitioner

Agenda

- Passwort-Leaks
- Richtlinien für Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentifizierung (2FA)

05.10.2018 10:40 Uhr | Security

Domainfactory-Hacker knackt Kundendatenbank der Telekom Austria

Bei einem Datenleck auf einem Server der Hosting-Sparte von A1 Telekom Austria sind Kundendaten und Passwörter im Klartext abhanden gekommen

WTF 30.03.2019 17:10 Uhr

Viermal die Null: Kostenloser Sprit dank Default-Passwort an Zapfsäule

...los an Tankstellen bedient. Sie ...

UPDATE 15.03.2019 13:59 Uhr | Security

Gearbest: Forscher warnt vor großem Datenleak bei chinesischem Online-Händler

Auf dem Server des Online-Händlers Gearbest lagen zeitweise 280.000 ungeschützte Kundendatensätze nebst Passwörtern im Klartext.

25.01.2019 12:51 Uhr | Security

Neue Passwort-Leaks: Insgesamt 2,2 Milliarden Accounts betroffen

Nach der Passwort-Sammlung Collection #1 kursieren nun auch die riesigen Collections #2-5 im Netz. So überprüfen Sie, ob Ihre Accounts betroffen sind.

heise + 15.02.2019 06:00 Uhr | c't Magazin

25 Gigabyte Passwortlisten von HavelBeenPwned schnell lokal durchsuchen

Auf haveibeenpwned.com kann man eine mehrere Gigabyte große Liste mit Hashes von Passwörtern herunterladen. Unser Python-Skript durchsucht sie blitzschnell.

21.03.2019 18:09 Uhr | Security

Facebook: Hunderte Millionen Passwörter im Klartext gespeichert

Offenbar seit 2012 hat Facebook intern Passwörter im Klartext gespeichert, einsehbar für viele Mitarbeiter. Der Konzern will keinen Missbrauch gefunden haben.

Quelle: heise.de

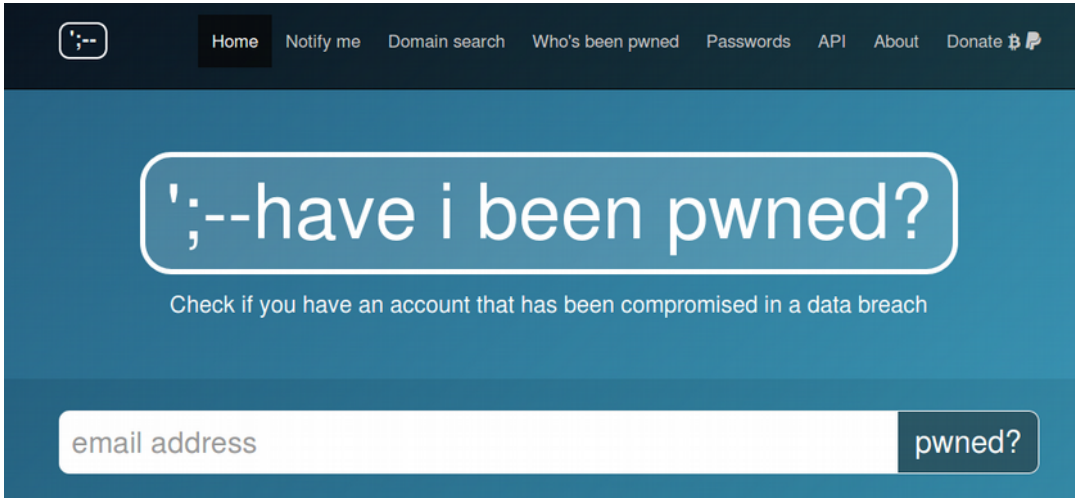
Passwort-Leaks

Quelle:commons.wikimedia.org/wiki/File:Steal_password.jpg

- Collection #1
  - Anfäng Jänner 2019
  - 2,7 Mrd Email/Passwort Kombinationen
  - zeitweise als kostenloser Download verfügbar
  - Inhalt: Email-Adressen, Passwörter (Klartext, Hashes)
  - Daten vielfach schon einige Jahre alt
- Collection #2,3,4,5
  - Ende Jänner 2019 aufgetaucht
  - 25 Mrd Email/Passwort Kombinationen
  - im Darkweb verfügbar
  - viele Daten von Yahoo, LinkedIn und Dropbox Hacks

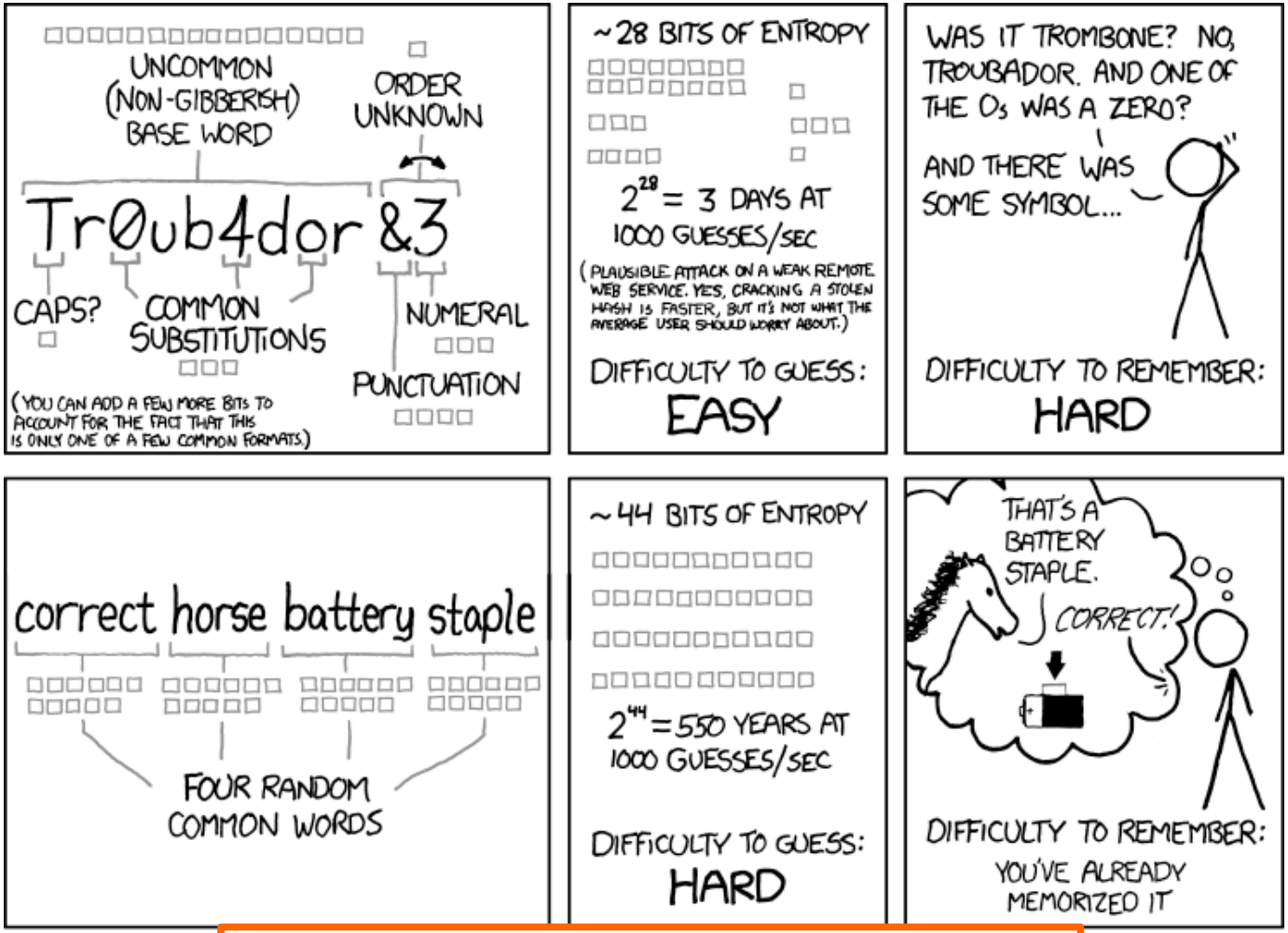
Have I Been Pwned?

- viele Dienste im Internet zur Prüfung verfügbar
  - Verwendung dieser generell mit großer Vorsicht zu genießen
  - HPI Identity Leak Checker von Uni Potsdam
    https://sec.hpi.uni-potsdam.de/ilc/search
  - Have I Been Pwned? (HIBP), von Troy Hunt aus Australien
    Suche nach Email/Username und Passwort möglich, Download der Daten
    https://haveibeenpwned.com/
  - sinnvoller ist eine lokale Prüfung



Agenda

- Passwort-Leaks
- Richtlinien für Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentifizierung (2FA)



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Quelle:xkcd.com/936/

Richtlinien für Passwörter

- NIST (National Institute of Standards and Technology) Standard für Behörden von 2003 hat sich etabliert (800-63, Appendix A)
- Update vom Juni 2017 bricht mit vielen etablierten Regeln
  - kein periodischer Passwort-Wechsel mehr empfohlen (bisher „alle 90 Tage“ weit verbreitet)
  - min. 8 Zeichen (bisher 6 Zeichen)
  - mind. 64 Zeichen möglich (bisher keine Empfehlung), keine Truncation mehr!
  - alle ASCI Zeichen, Unicode empfohlen (bisher >=90 Zeichen)
  - von Passwort-Hinweisen („Name von erstem Haustier“) wird abgeraten
  - keine Composition Rules empfohlen („mind. 1 Großbuchstabe, Sonderzeichen, …“)
  - Prüfung auf Wörterbuch-Attacken und Passwort-Leaks empfohlen

  → soll benutzerfreundlicher werden
  → Ziel sind längere Passphrasen statt Passwörtern

BSI Faktenblatt

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/sichere_passwoerter_faktenblatt.pdf
- eine A4 Seite
- Version vom 1.2.2019

Umgang mit Passwörtern

- ☑ Passwörter unter Verschluss halten; Passwort-Manager sind eine gute Hilfe
- ☑ Passwörter spätestens bei Verdacht auf Missbrauch ändern
- ☑ Keine einheitlichen Passwörter für Accounts verwenden
- ☑ Voreingestellte Passwörter ändern
- ☑ Passwörter nicht an Dritte weitergeben und nicht per E-Mail versenden

Ein gutes Passwort ...

AleiPm4Z+eK!*

- ... sollte mindestens acht Zeichen lang sein, je länger desto besser.
- ... besteht nicht aus einer Kombination mit Geburtstagen oder Namen des Haustieres.
- ... sollte nicht im Wörterbuch stehen.
- ... darf keine gängigen Wiederholungs- oder Tastaturmuster (asdfgh oder 1234abcd) enthalten.
- ... ist kein simples Passwort, das einfach um ein Sonderzeichen am Anfang oder Ende ergänzt wird.
- ... kann aus Groß- und Kleinbuchstaben, Sonderzeichen (?!%+) und Ziffern bestehen.

Bei Reisen ins Ausland können Umlaute auf landestypischen Tastaturen evtl. nicht eingegeben werden. !

*) Die Eselsbrücke: Indem Sie sich jeweils den ersten Buchstaben eines jeden Wortes in einem Satz merken, können Sie sich ganz einfach an ein Passwort mit mehr als acht Zeichen erinnern. Schon sind Sie bestens geschützt. Beispiel: „Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!" wird zum Passwort: AleiPm4Z+eK!

Agenda

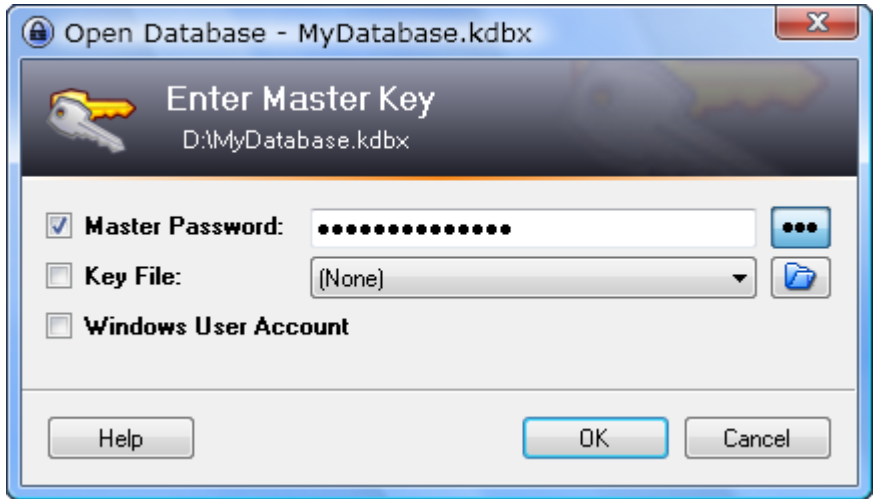
- Passwort-Leaks
- Richtlinien für Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentifizierung (2FA)

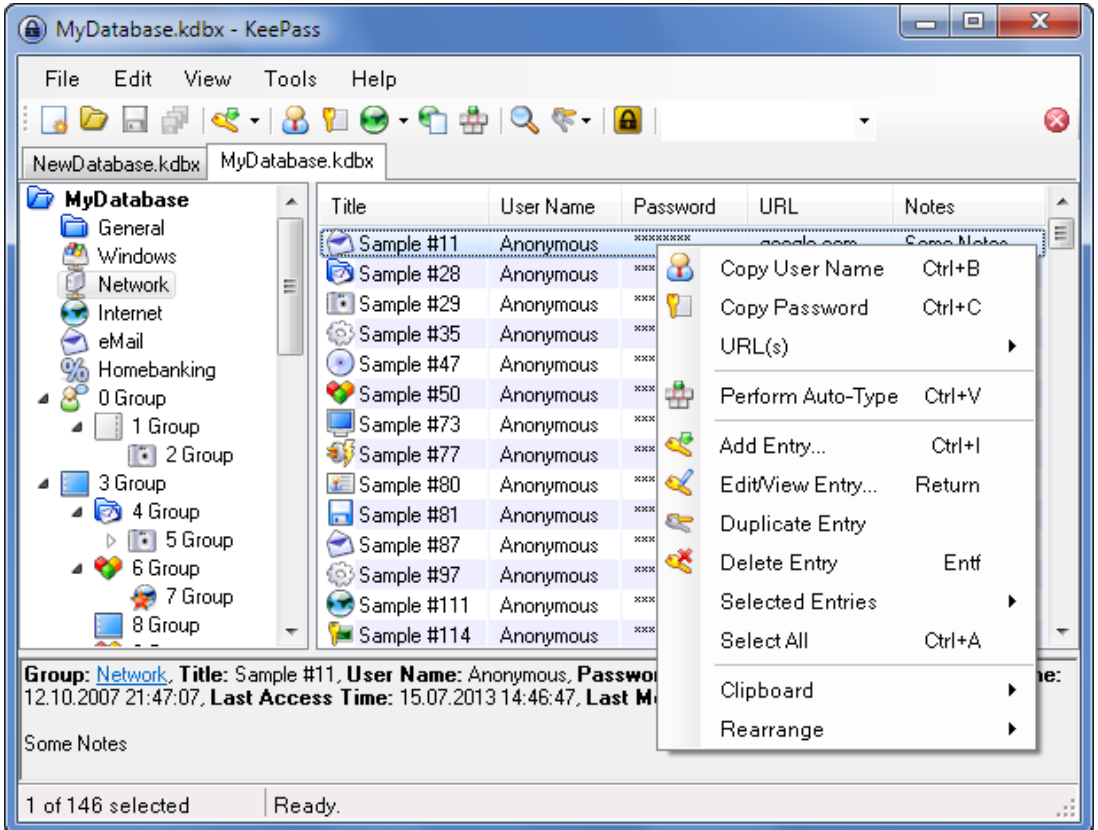
Passwort Manager

- verhindert Passwort-Recycling
- eingebaute Passwort-Generatoren
- Master-Passwort ist Jackpot für Hacker
  → zweiter Faktor z.b. mit Schlüssel-Datei wichtig
- Ablage in der Cloud kritisch
- Online-Passwort-Manager fraglich
- Softwarequalität essentiell (OpenSource hilft)
- Einsatz muss genau geplant werden
  - IT-Grundschutz Maßnahme „M 4.306 Umgang mit Passwort-Speicher-Tools“
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04306.html

KeePass

- für Windows, Linux, macOS, Windows Mobile, Android, iOS, Blackberry OS, Java
- Seit 2003, GPL
- Browser Plugin





Agenda

- Passwort-Leaks
- Richtlinien für Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentifizierung (2FA)

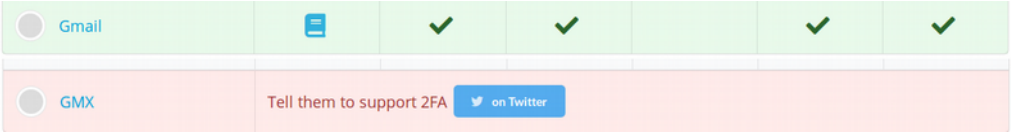
Umfrage

- Wer von Ihnen setzt Zwei- oder Multi-Faktor-Authentifizierung in der Firma ein?

FaaS and Furious by Forrest Brazeal A CLOUD GURU

Zwei-Faktor-Authentifizierung (2FA)

- Bekanntestes Beispiel:
  Geldautomat mit Karte (Besitz) und PIN (Wissen)
- Mögliche Faktoren:
  - Wissen (Passwort, PIN)
  - Besitz (Token, Smartphone-App, Smartcard, Datei)
  - biometrische Merkmale (Fingerabdruck, Iris, Stimme, Gesicht)
- Welche Dienste 2FA können:
  https://twofactorauth.org/



- SMS und Google Authenticator am populärsten
  - SMS haben viele Angriffsmöglichkeiten (z.b. zweite SIM-Karte)

Zwei-Faktor-Authentifizierung (2FA)

- Schützt vor ...
  - Shouldersurfing (z.B. Zugfahrt, Flughafen, ...)
  - schwachen Passwörtern
  - unsicheren Passwort-Datenbanken (Klartext, schwacher Hash-Algorithmus)
  - Man-in-the-Middle Angriff
  - Konfigurationsfehlern (z.B. unverschlüsselter LDAP-Zugriff auf AD)

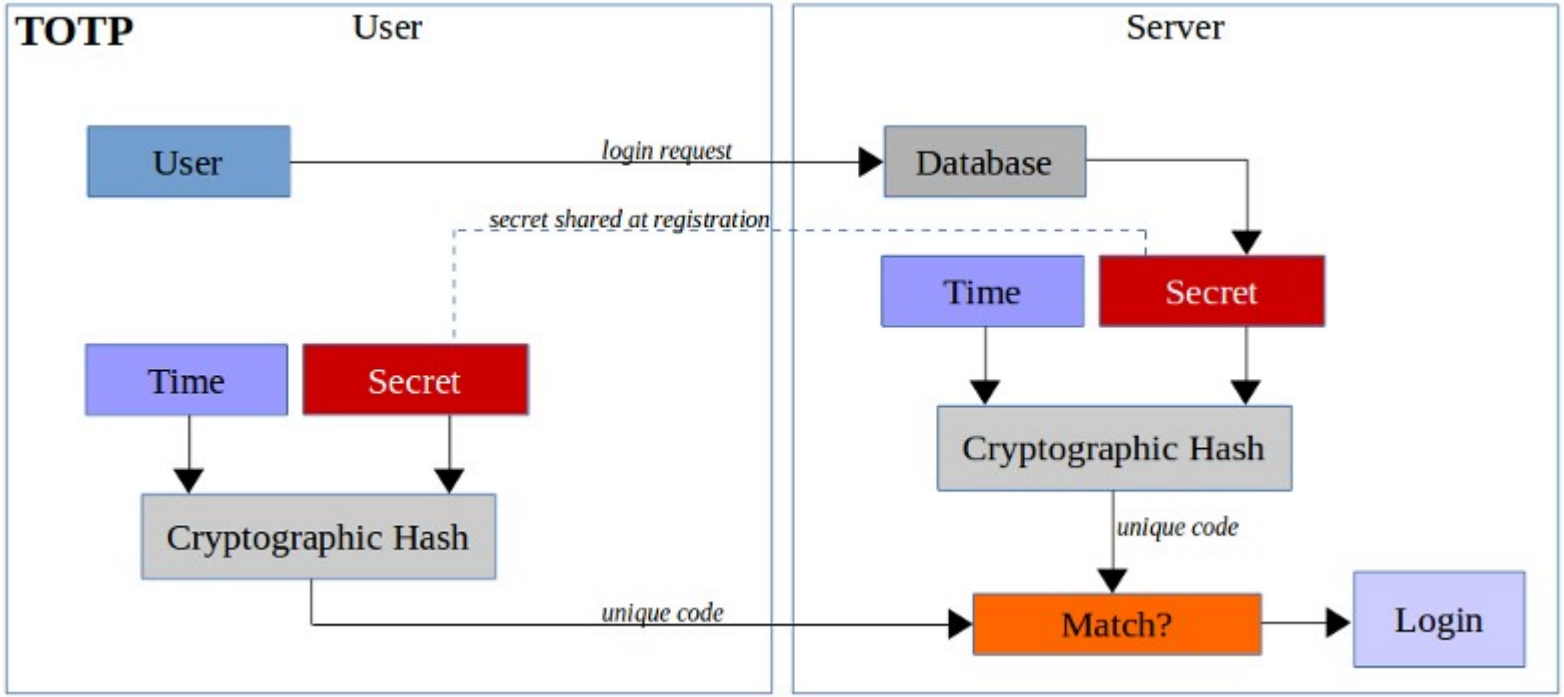
23 Google: Security Keys Neutralized Employee Phishing

JUL 18

Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes, the company told KrebsOnSecurity.

Quelle: krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

Time-based One-time Password (TOTP)

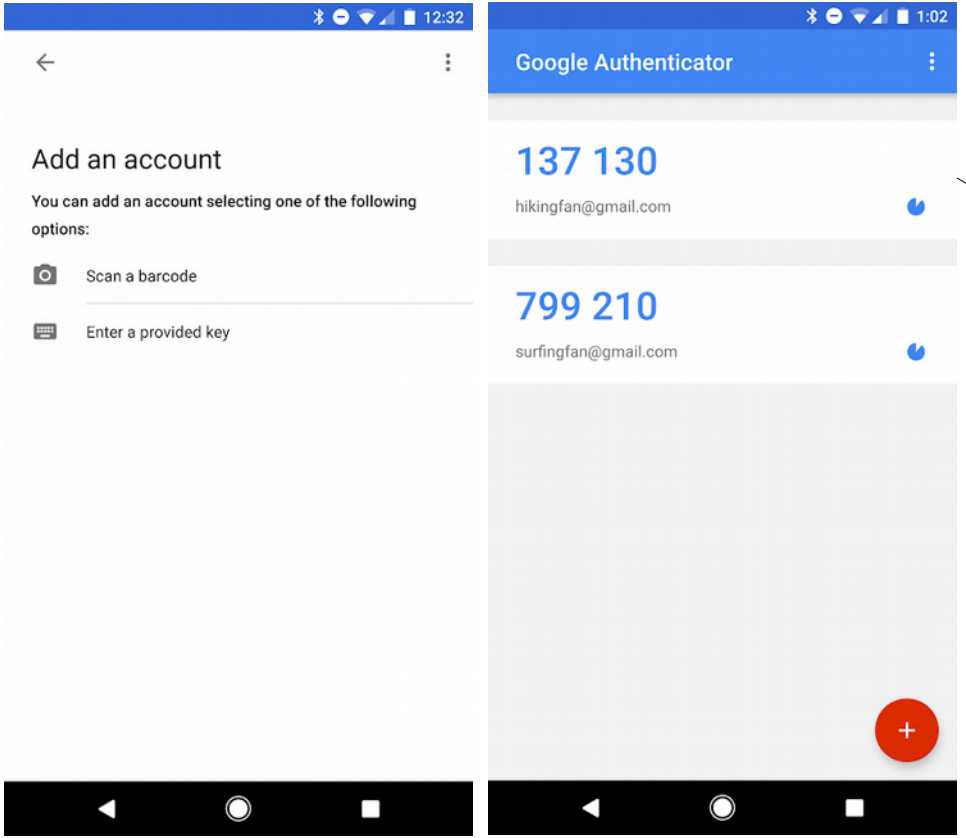


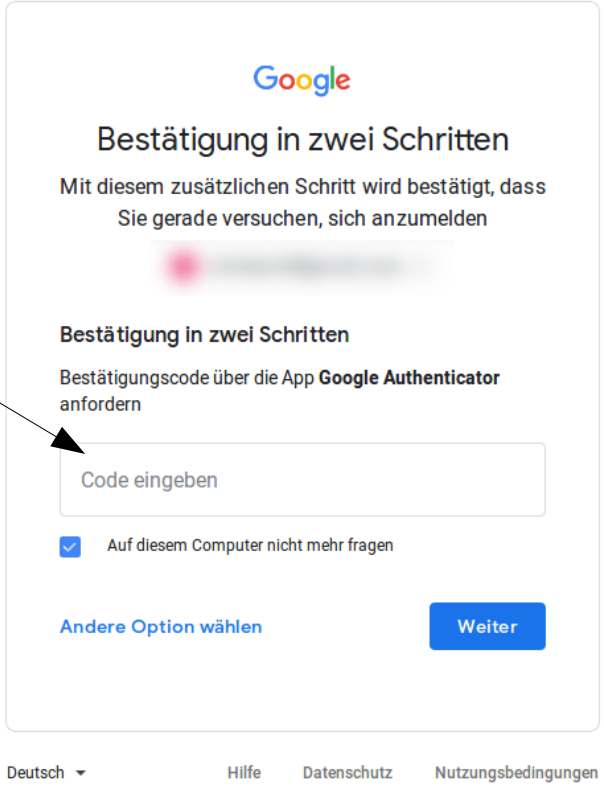
Quelle: blog.trezor.io/why-you-should-never-use-google-authenticator-again-e166d09d4324

Google Authenticator

- App für Android, iOS und Blackberry
- 80-Bit-Geheimcode als shared secret (OATH-HOTP)
  - Mittels QR-Code oder Text übertragen
- Einmalpasswort aus Uhrzeit und Geheimcode berechnet
  - Time-based One-time Password Algorithm (TOTP)
  - 30 Sekunden lang gültig
- nicht nur für Google Dienste einsetzbar
- funktioniert auch ohne Internetverbindung
- Geheim-Code oder Backup-Codes wichtig bei neuem Gerät

Funktionsweise

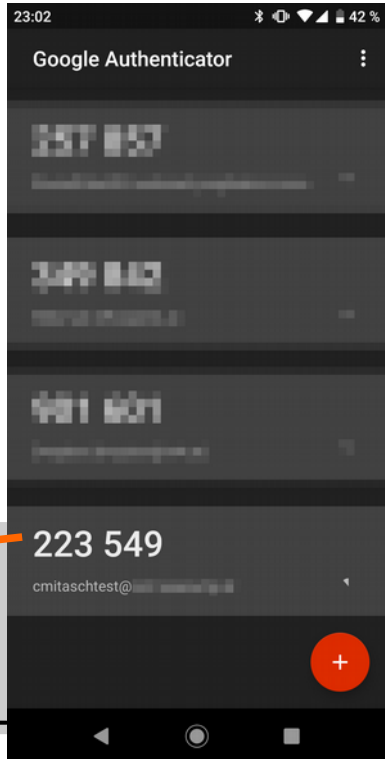




sshd mit Google Authenticator

- Installation Ubuntu 16.04
  # apt-get install libpam-google-authenticator
- /etc/ssh/sshd_config anpassen:
  ChallengeResponseAuthentication yes
- /etc/pam.d/sshd als neue Zeile hinzufügen:
  auth required pam_google_authenticator.so nullok
- service sshd restart
- → Login mit Passwort und OTP Code von App

```
$ ssh cmitaschtest@testserver
Password:
Verification code: 223549
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-143-generic x86_
```



Settings Datei anlegen und in App übertragen

```
cmitaschtest@server:~$ google-authenticator
Do you want authentication tokens to be time-based (y/n) y
Your new secret key is: XXXXXXXXXXXXXXXX
Your verification code is 123456
Your emergency scratch codes are:
  12345678
 ...
  12345678

Do you want me to update your "/home/cmitaschtest/.google_authenticator" file (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
size of 1:30min to about 4min. Do you want to do so (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting (y/n) y
```

Google Authenticator

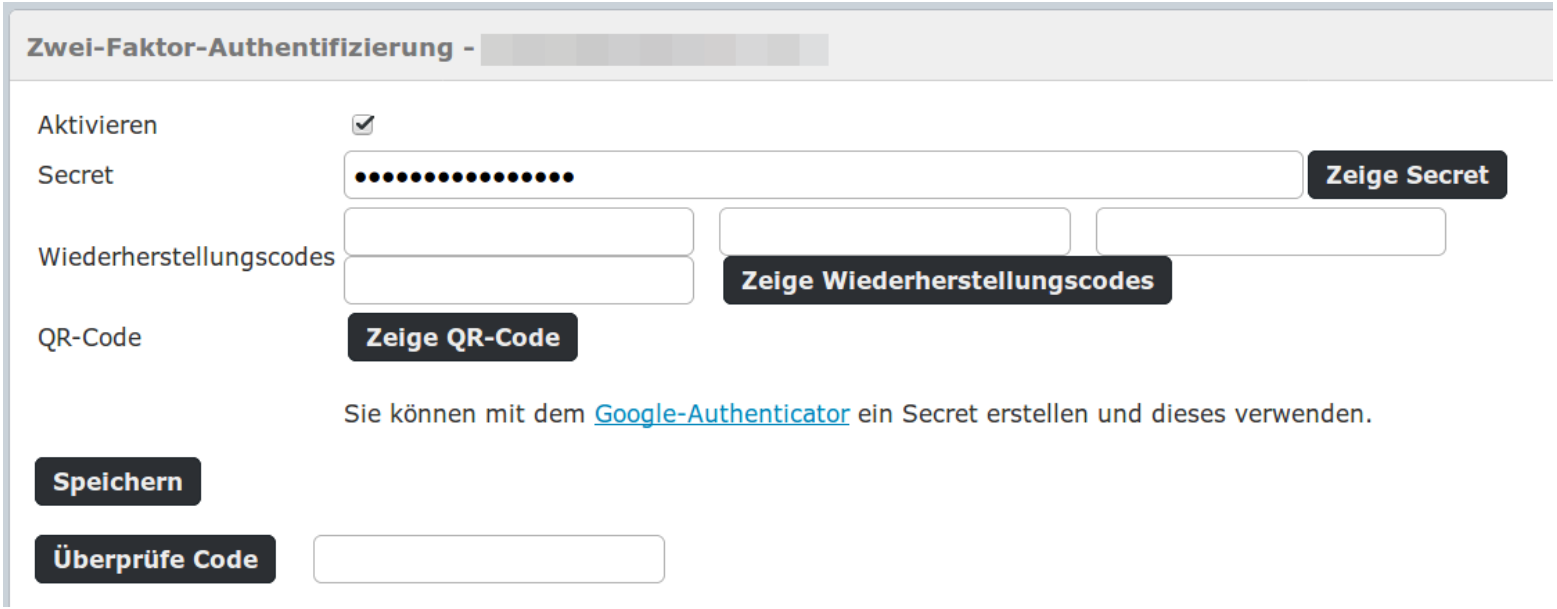
- Schwächen
  - Probleme bei Zeitabweichungen von Client/Server
  - Geheimcode unverschlüsselt auf Server/Smartphone gespeichert
  - Bei unverschlüsselten Dateisystem auch in ausgeschaltetem Zustand auslesbar
  - → Sicherheit von Server und Client essentiell
  - Sicherer Austausch von Shared Secret und Recovery Codes wichtig
  - App ist keine OpenSource Software mehr

Roundcube mit Google Authenticator

- Plugin für Webmail Software
  - https://plugins.roundcube.net/packages/alexandregz/twofactor_gauthenticator
  - Config-Datei:

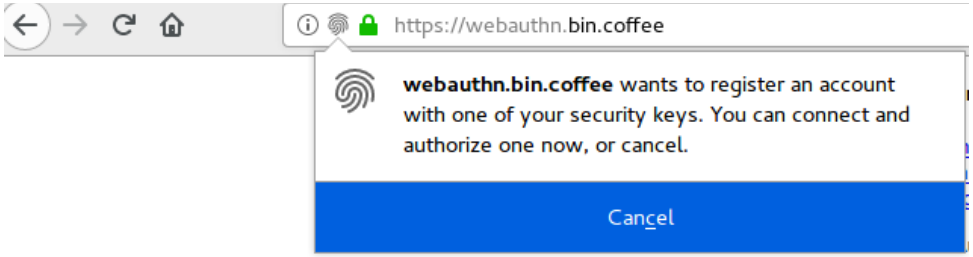
```
<?php
// if true ALL users must have 2-steps active
$rcmail_config['force_enrollment_users'] = false;

// whitelist, CIDR format available
// NOTE: we need to use .0 IP to define LAN because the class CIDR have a iss
for example)
$rcmail_config['whitelist'] = array('192.168.1.0/24', '::1', '192.168.0.9');

// Admin can disable saving devices for all users (paranoid mode)
// Default: allow saving devices (true)
$rcmail_config['allow_save_device_30days'] = true;

// Make the 2-step field a masked password input type
// Default: form field will be text (false)
$rcmail_config['twofactor_formfield_as_password'] = false;
```


roundcube
Benutzername
Passwort
Anmelden
roundcube
Zwei-Faktor-Bestätigungscode
123456
Nicht erneut nach dem Code fragen für die nächsten 30 Tage
Anmelden


Zwei-Faktor-Authentifizierung -
Aktivieren
Secret
Zeige Secret
Wiederherstellungscodes
Zeige Wiederherstellungscodes
QR-Code
Zeige QR-Code
Sie können mit dem Google-Authenticator ein Secret erstellen und dieses verwenden.
Speichern
Überprüfe Code

Zusammenfassung/Ausblick

- 2FA generell für externen Zugriff sinnvoll
- Passwort-Richtlinien aktualisieren
- An Qualität der Passwörter arbeiten, automatische Prüfung
- WebAuthn wurde im März 2019 vom W3C standardisiert
  - Anmeldung im Browser mit krytografischen Schlüssel statt Passwort
  - kein Shared Secret wie bei TOTP sondern Schlüsselpaar (public/private)
  - Universal Secondary Factor (U2F) – Hardware Key mit USB/NFC/Bluetooth



Quelle: cloud.google.com/titan-security-key/

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®