



# Zwei-Faktor-Authentifizierung am Beispiel Web.de

PC-Treff-BB Aidlingen

Günter Waller



# Agenda

- Motivation
- Diskussion Passwort-Authentifizierung
- Zweiter Faktor
- One Time Passwort
- Vorgehen bei Web.de
- Links

# Motivation

- Ständig fehlgeschlagene Login-Versuche beim vermutlich wichtigsten Online-Konto, dem E-Mail Account. Was tun?



## Passwörter im Internet

- Passwörter sind im Internet allgegenwärtig.
  - Man braucht also viele davon. Häufige Fehler: Mehrfachverwendung, Trivialpasswörter, leicht zu merken = leicht zu erraten
- Man ist auf die Sorgfalt der Serviceprovider angewiesen, hat keinen Einfluss. Risiken:
  - Provider leicht hackbar
  - Passwörter im Klartext gespeichert statt (**salted**) Hash
  - Checken: <https://haveibeenpwned.com/>
- Ist die Passwortdatei gestohlen, haben Angreifer alle Zeit, alle Möglichkeiten, z.B. Brute Force, Wörterbuchattacke (Rainbow-Tabellen)

## Passwörter – wie schützen?

- Langes oder komplexes Passwort wählen
  - BSI: 25 Zeichen mit 2 Zeichenarten
  - BSI: 8 Zeichen mit 4 Zeichenarten
    - Groß-, Kleinbuchstaben, Sonderzeichen, Ziffern
  - Merkbarkeit: Anfangsbuchstaben eines Merksatzes, KEINE Namen, Geburtsdaten, etc.
- Es gibt wichtige und weniger wichtige Passwörter
  - Passwortmanager sind eine Option, mit der Vielfalt fertig zu werden, müssen aber ihrerseits sicher sein (Cloud??)
- NSA und Konsorten heben einfach mal alles auf für die Zukunft (Quantencomputing)

## Passwörter alleine reichen nicht

- Web.de unterstützt (und empfiehlt) die Verwendung von Zwei-Faktor Authentifizierung.
- Was ist das? Im Grunde steht alles [hier](#) :-)
- Also: Multi-Faktor Authentifizierung begnügt sich nicht mit dem einen Faktor Passwort. Es gibt 3 Kategorien:
  - Was ich weiß: Passwort/Passphrase, Sicherheitsfrage, PIN
  - Was ich habe/besitze: Handy, TAN-Generator, Sicherheits-Token, Chipkarte
  - Was ich bin: in der Regel Biometrie (Fingerabdruck, Iris, Face ID, Stimme)

## Zwei-Faktor Authentifizierung

- Zwei-Faktor Authentifizierung (2FA) verlangt zwei der drei.
- Beispiel Banking: PIN und TAN
- Web.de verwendet als zweiten Faktor ein One-Time Passwort (OTP). Was ist das?
- Es gibt im wesentlichen 2 Typen: HOTP und TOTP.
- HOTP (HMAC-based OTP) arbeitet in der Regel auf Basis eines Zählers, den Server und Client App gemeinsam führen. Dieser muss immer gleich sein.
- TOTP (Time-based OTP) arbeitet auf Basis der Uhrzeit, d.h. Server und Client App müssen synchron sein.

## OTP Grundlagen

- Beim Einrichten auf dem (Web-)Server wird ein Initialwert generiert.
- Der Client (die App) liest diesen Wert ein, d.h. beide Seiten haben dann ein gemeinsames Geheimnis (Secret Key).
- Daraus und aus einer Variablen (Uhrzeit oder Zähler) errechnen beide den gleichen (6-stellig numerischen) Wert.
- Der Server fragt ihn nach Prüfung des Passwortes ab und vergleicht. Bei Übereinstimmung ist das Login erfolgreich.



# Login-Dialog (nach Passwort)

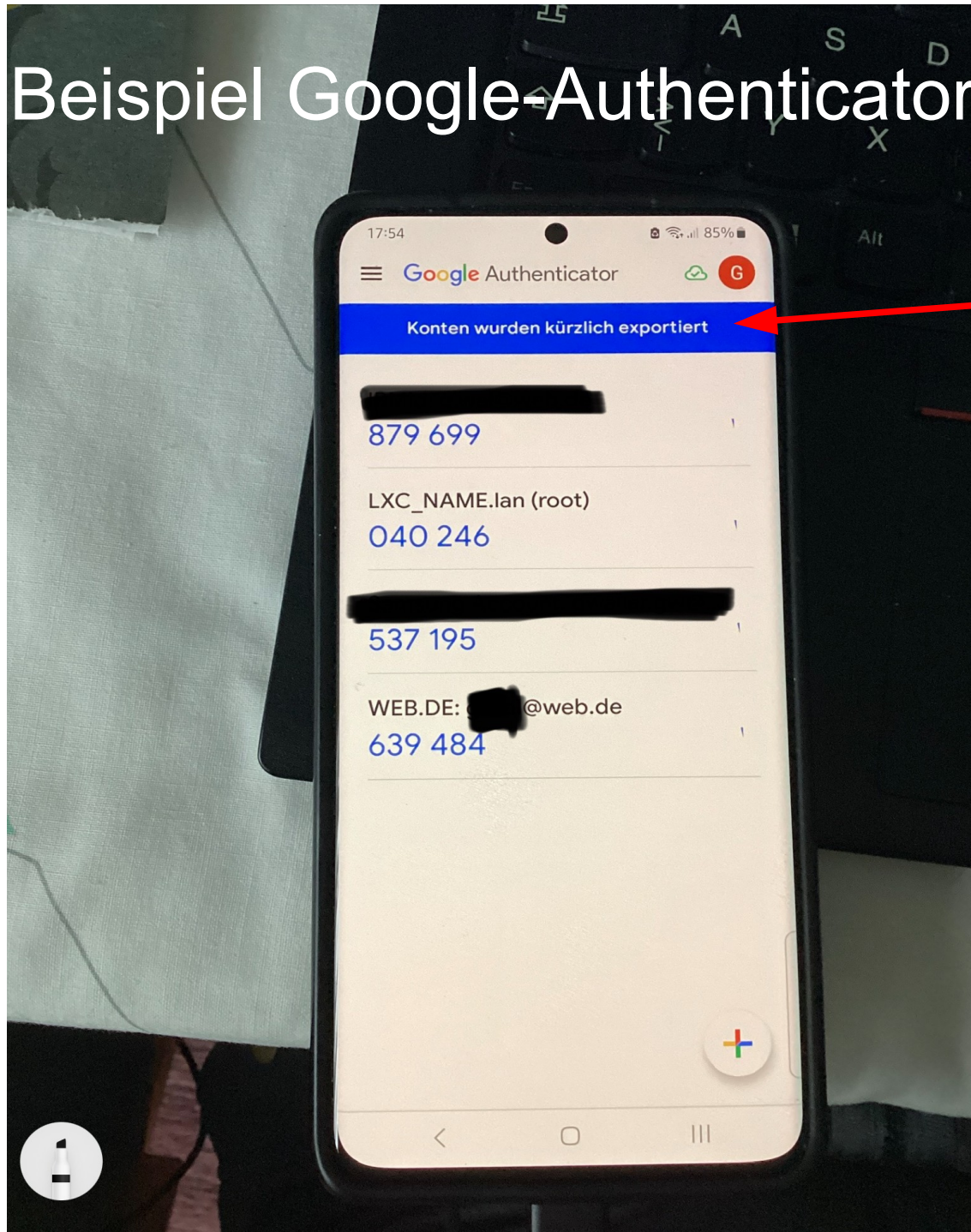
The image displays two screenshots of a two-factor authentication (2FA) dialog box. Both screenshots feature the 'WEB.DE' logo at the top, which consists of a yellow square with a black icon of a classical building and the text 'WEB.DE' below it.

**Left Screenshot: 'Zwei-Faktor-Authentifizierung'**  
The title is 'Zwei-Faktor-Authentifizierung'. Below it, the text reads: 'Geben Sie den Code ein, der von Ihrer Authentifizierungs-App angezeigt wird.' There is a light gray input field with the placeholder text 'Authentifizierungs-Code eingeben' and six empty square boxes for digits. Below the input field is a checkbox labeled 'Für dieses Gerät merken', which is highlighted with a red rectangular border. At the bottom, there is a yellow button labeled 'Weiter', a blue link 'Abbrechen', and a blue link 'Benötigen Sie Hilfe?'.

**Right Screenshot: 'Zwei-Faktor-Authentifizierung'**  
The title is 'Zwei-Faktor-Authentifizierung'. Below it, the text reads: 'Geben Sie den Code ein, der von Ihrer Authentifizierungs-App angezeigt wird.' There is a light gray input field with the placeholder text 'Authentifizierungs-Code eingeben' and six empty square boxes for digits. Below the input field is a red warning triangle icon followed by the text: 'Die eingegebene Nummernfolge ist nicht korrekt. Bitte geben Sie die 6-stellige Nummernfolge erneut ein.' Below this is a checkbox labeled 'Für dieses Gerät merken'. At the bottom, there is a yellow button labeled 'Weiter', a blue link 'Abbrechen', and a blue link 'Benötigen Sie Hilfe?'.

Merke: Das „merken“ basiert auf Cookies.

# Beispiel Google-Authenticator



Die Daten wurden auf ein anderes Gerät exportiert zur Vermeidung eines Single Point of Failure (SPOF).

Das initiale Secret (oder Startwert) kann per QR-Code oder durch Abtippen eingerichtet werden.

Schützt man die App mit Biometrie, bekommt man den dritten Faktor dazu.

## Aber was ist mit der Praktikabilität?

- Damit das ganze nicht zur Qual wird, gibt es (bei Web.de) eine ganze Reihe von flankierenden Maßnahmen:
  1. Sicherheits-Mobilfunknummer
  2. Geheimschlüssel für den Postfachzugang im Notfall
  3. Geheimfrage (für telef. Kontakt mit Support)
  4. Anwendungsspezifische Passwörter
  5. „Merken“ von vertrauenswürdigen Geräten
- 1-3 für Wiederherstellung des Zugangs dürften selbsterklärend sein.

## Web.de schreibt zu Accountsicherung

- Sie haben verschiedene Möglichkeiten, Ihr Konto abzusichern:
  - Hinterlegen Sie eine Mobilfunknummer oder eine alternative E-Mail-Kontaktadresse. Damit können sie Ihr Passwort bei Verlust zurücksetzen.
  - Aktivieren Sie die Zwei-Faktor-Authentifizierung. So sorgen Sie für einen sicheren Login über Geräte, die sie autorisiert haben.
  - Hinterlegen Sie persönliche Daten und eine Geheimfrage in Ihrem Konto. Durch einen Abgleich der persönlichen Daten und der Geheimfrage kann der Mitarbeiter des WEB.DE Kundenservice Sie als Inhaber Ihres Kontos erkennen, falls Sie uns kontaktieren möchten.
- Wenn Sie keine der zuvor genannten Informationen hinterlegt haben, müssen Sie sich bei einer Kontaktaufnahme mit dem WEB.DE Kundenservice gegebenenfalls über einen mehrstufigen Prozess ausweisen.



# Geheimschlüssel

- Dient zur einmaligen Verwendung im Notfall. Ausdrucken wird empfohlen. Abspeichern? Na ja.


The screenshot shows the 'Kundencenter' web interface. The top navigation bar includes icons for Start, E-Mail, Online-Speicher, Adressbuch, mehr, Suche, and Logou. The left sidebar contains a menu with items like Übersicht, Persönliche Daten, Login & Sicherheit (highlighted), Verträge, Vertrag kündigen, Kündigung zurücknehmen, Zahlungsdaten, Rechnungen, Vertragsdokumente, Datenschutz & Privatsphäre, Weitere Einstellungen, Konto löschen, and Kontakt. The main content area displays a progress bar with four steps: 1. Mobilfunknummer verifizieren (checked), 2. App einrichten (checked), 3. Geheimschlüssel sichern (current step), and 4. Angaben prüfen & Aktivierung abschließen. Below the progress bar, the title 'Geheimschlüssel für den Postfachzugang im Notfall' is shown. A text box explains that the key provides access to the mailbox in specific cases: no access to the authentication app, a new smartphone, or a new mobile number. A yellow button 'Geheimschlüssel sichern' is at the bottom right, and a blue link 'Zurück' is at the bottom left.

The screenshot shows a modal window titled 'Kundencenter' with a yellow header bar. The main text reads 'Geheimschlüssel für die Zwei-Faktor-Authentifizierung' and 'Ihr Notfallzugang ins Postfach.' Below this, it says 'Geheimschlüssel (zur einmaligen Verwendung)' and 'Erstellt am: 09.08.2023'. At the bottom, a long string of 'X' characters represents the generated key.

## Anwendungsspezifische Passwörter erzeugen

- Diese erzeugt man im Kundencenter. Es handelt sich um lange, zufallsgenerierte Zeichenketten. Man benötigt sie für externe E-Mail-Programme via POP/IMAP (z.B. Thunderbird oder Mail-Apps) und CardDav/CalDav-Clients.
- Sie werden verwendet statt des Original-Passworts (das ja immer noch aktiv ist), müssen also im jeweiligen Programm hinterlegt werden.
- Wird Zwei-Faktor ausgeschaltet, müssen diese Programme wieder das Original-Passwort verwenden.

# Anwendungsspezifische Passwörter verwalten


Kundencenter

Start
 E-Mail
 Online-Speicher
 Adressbuch
 mehr
 Suche
 Logout

- Übersicht
- Persönliche Daten
- Login & Sicherheit
- Verträge
- Vertrag kündigen
- Kündigung zurücknehmen
- Zahlungsdaten
- Rechnungen
- Vertragsdokumente
- Datenschutz & Privatsphäre
- Weitere Einstellungen
- Konto löschen
- Kontakt

## Anwendungsspezifische Passwörter

Für die Nutzung externer E-Mail-Programme über POP3/IMAP oder die Einbindung Ihres WEB.DE Kalenders/Adressbuchs (mit CalDav bzw. CardDav) in ein externes Programm, können Sie hier Anwendungsspezifische Passwörter erstellen und verwalten.

Name	Letzte Nutzung
T470-TB-Mail	09.08.2023
IPAD	12.08.2023
KMPC-TB-Mail	09.08.2023
KMPC-TB-Carddav	09.08.2023
IPAD-Carddav	11.08.2023
T470-TB-Carddav	09.08.2023
Samsung-Carddav	12.08.2023

[Anwendungsspezifische Passwörter verwalten](#)

## So geht es bei Web.de

- <https://hilfe.web.de/sicherheit/2fa/ueber-zweifaktor.html>
- <https://hilfe.web.de/sicherheit/2fa/einrichten.html>
- <https://hilfe.web.de/sicherheit/2fa/otp-apps.html>
- <https://hilfe.web.de/sicherheit/2fa/login.html>
- <https://hilfe.web.de/sicherheit/2fa/deaktivieren.html>
- <https://hilfe.web.de/sicherheit/2fa/verlorene-logindaten.html>



## Links

- [OTP-Erklärung](#) von S.6 (englisch)
- [Diskussion](#) von Wörterbuch-Attacken, Rainbow-Tables, Salted Hash
- Uni Münster, ausführliche [Beschreibung](#), wie man deren OTP-Service nutzt, deshalb von allgemeinem Nutzen
- [Have I been pwned](#) von S. 4
- „[Offizielle Beschreibung](#)“ bei Web.de
  - [News-Blog-Eintrag](#) als Ergänzung