Willkommen beim Meetup Bonn

#wpbn No. 99 - Zwei-Faktor-Authentifizierung (2FA)

Feb
4
7:00 PM

Florentiusgraben 21-23, SISTRIX Seminare, Bonn

Attend on m

By WordPress Meetup Bonn #wpbn

meetup

Wer kennt die Zwei-Faktor-Authentisierung (2FA) ?

Wer nutzt die Methode zum Login ?

Wer nutzt sie auf seiner Webseite ?

Was sind die Faktoren ?

Die Zwei-Faktor-Authentisierung (2FA) ist eine Sicherheitsmethode, bei der man die Identität durch zwei verschiedene Komponenten nachweisen, um Zugang zu einem Konto oder System zu erhalten.

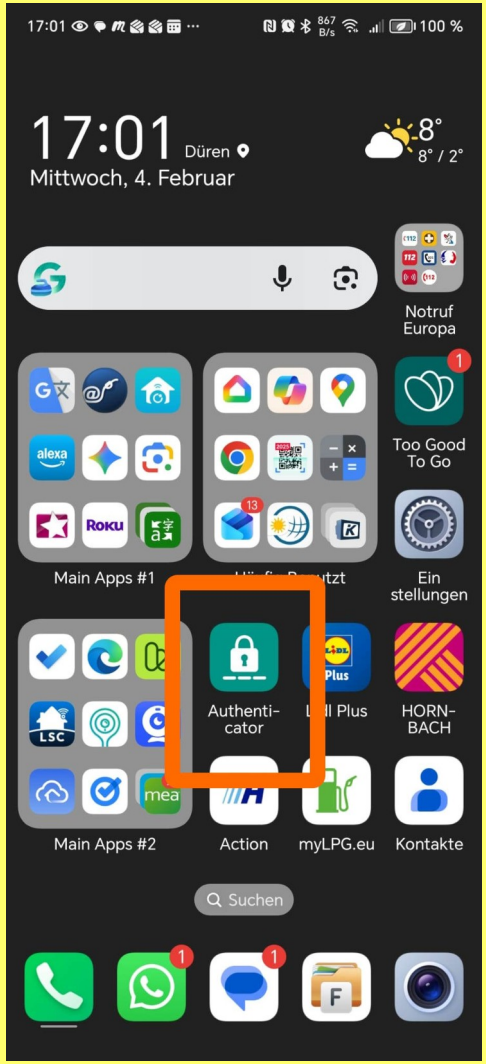
Die drei gängigen Kategorien von Faktoren

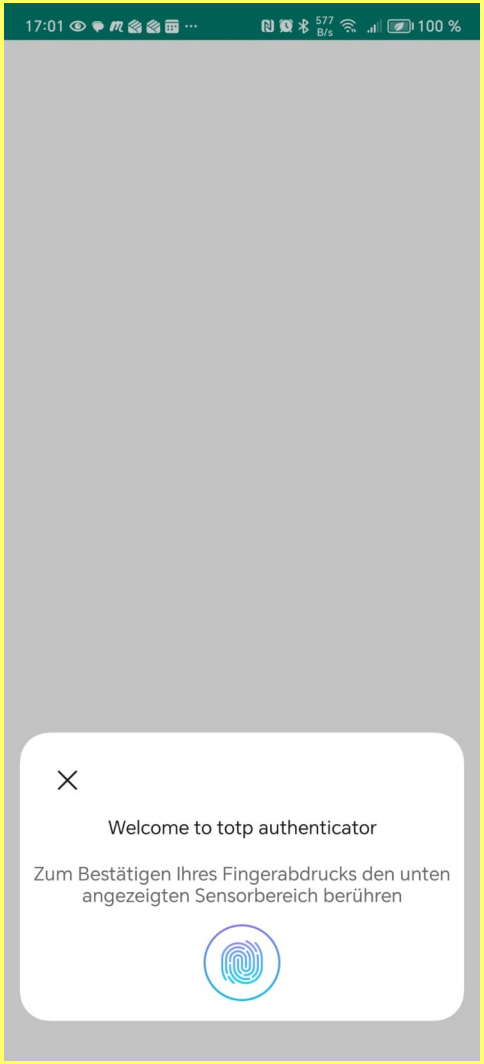
- **Wissen:** Etwas, das Sie wissen (z. B. Passwort, PIN oder Antwort auf eine Sicherheitsfrage).
- **Besitz:** Etwas, das Sie besitzen (z. B. Smartphone für SMS-Codes, eine Authentifikator-App wie der Google Authenticator oder ein physischer Sicherheitsschlüssel wie YubiKey).
- **Inhärenz:** Etwas, das Sie sind (Biometrie wie Fingerabdruck, Gesichtsscan oder Iris-Erkennung).

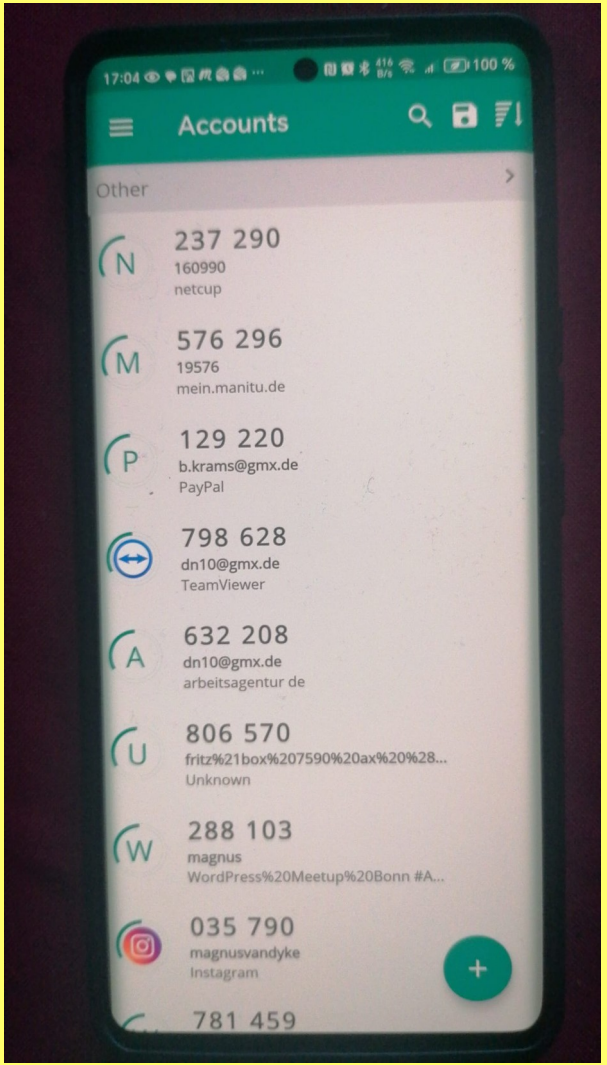
Warum 2FA im Jahr 2026 unverzichtbar ist.
Da Passwörter allein oft durch Datenlecks oder Phishing gestohlen werden können, bietet 2FA eine entscheidende zusätzliche Schutzschicht. Selbst wenn ein Angreifer Ihr Passwort kennt, kann er ohne den zweiten Faktor nicht auf Ihr Konto zugreifen.

Hardware-Sicherheitsschlüssel (FIDO2): Die sicherste Methode, die vor Phishing schützt.
Authentifikator-Apps (TOTP): Generieren zeitbasierte Codes lokal auf dem Gerät (z. B. Microsoft Authenticator).
Push-Benachrichtigungen: Bestätigung per Fingertipp auf einem vertrauenswürdigen Gerät.

SMS/E-Mail: Günstig und einfach, aber anfällig für SIM-Swapping oder Abfangen von Nachrichten.


17:01
Düren
Mittwoch, 4. Februar
8°
8° / 2°
Notruf Europa
Too Good To Go
Main Apps #1
Ein stellungen
Authenti-cator
HORN-BACH
Main Apps #2
Action
myLPG.eu
Kontakte
Suchen


Welcome to totp authenticator
Zum Bestätigen Ihres Fingerabdrucks den unten angezeigten Sensorbereich berühren


Accounts
Other
237 290
160990
netcup
576 296
19576
mein.manitu.de
129 220
b.krams@gmx.de
PayPal
798 628
dn10@gmx.de
TeamViewer
632 208
dn10@gmx.de
arbeitsagentur de
806 570
fritz%21box%207590%20ax%20%28...
Unknown
288 103
magnus
WordPress%20Meetup%20Bonn #A...
035 790
magnusvandyke
Instagram
781 459

Festung WordPress – 2FA gegen Brute-Force

1. Das Problem: Warum Passwörter versagen

Brute-Force erklärt: Automatisierte Skripte probieren tausende Kombinationen pro Sekunde.

Der menschliche Faktor: Wiederverwendete Passwörter aus Datenlecks (Credential Stuffing).

Die Statistik: Ein Großteil aller erfolgreichen WordPress-Hacks erfolgt über den Login-Bereich.

2. Die Lösung: Was ist 2FA?

Das Prinzip: Etwas, das du *weißt* (Passwort) + Etwas, das du *hast* (Smartphone/Key).

Warum im Repo suchen?

Weil es dort exzellente Open-Source-Lösungen, die kein Abo erfordern.

3. Top 3 Plugin-Vorstellungen aus dem Repository

A. WP 2FA (von Melapress) – Der Allrounder

Vorteile: Sehr geführte Einrichtung (Wizard), unterstützt viele Methoden (Google Authenticator, E-Mail, Backup-Codes).

Besonderheit: Man kann 2FA für bestimmte Benutzerrollen (z. B. nur Admins) erzwingen.

Demo-Punkt: Zeige den Einrichtungs-Assistenten, der auch für Laien verständlich ist.

B. Two Factor (Das "Community-Original")

Vorteile: Extrem schlank, kein Schnickschnack, wird von WordPress-Core-Entwicklern gepflegt.

Besonderheit: Unterstützt **Passkeys (WebAuthn)** und FIDE U2F (Hardware-Keys wie Yubikey).

Demo-Punkt: Zeige, wie man sich per Fingerabdruck (Passkey) am Laptop einloggt.

WP 2FA / Two Factor

A. **WP 2FA (von Melapress)**

Dies ist aktuell die wohl benutzerfreundlichste Lösung. Sie bietet einen geführten Assistenten (Wizard) für deine Nutzer, was die Akzeptanz im Team deutlich erhöht.

Methoden: Google Authenticator, Authy, E-Mail-Codes, Backup-Codes.

Besonderheit: Man kann die Aktivierung von 2FA für bestimmte Benutzerrollen erzwingen (z. B. nur für Admins und Redakteure).

B. **Two Factor (von Plugin Contributors)**

Dieses Plugin ist quasi der "halboffizielle" Standard. Es wird von vielen WordPress-Core-Entwicklern gepflegt und dient oft als Testwiese für Funktionen, die eventuell irgendwann in den WordPress-Kern wandern könnten.

Methoden: FIDO Universal 2nd Factor (U2F/FIDO2), Authenticator-Apps (TOTP), E-Mail, Backup-Codes.

Besonderheit: Extrem schlank, kein Schnickschnack, sehr performant.

Was du bei der Auswahl beachten solltest

- **Benutzererfahrung:** Müssen sich deine Kunden oder technisch weniger versierte Autoren einloggen? Dann wähle ein Plugin mit einem einfachen Onboarding (wie **WP 2FA**).
- **Multisite-Support:** Wenn du ein Netzwerk betreibst, achte darauf, dass das Plugin global über das Netzwerk-Dashboard verwaltet werden kann.
- **DSGVO:** Bei E-Mail-basierten Codes werden Daten versendet. Achte darauf, dass dein Mail-Server (oder Versanddienst) datenschutzkonform arbeitet.

Wichtiger Tipp: Generiere und speichere **immer** die Recovery-Codes (Backup-Codes), bevor du die 2FA scharf schaltest. Wenn dein Handy verloren geht oder die App gelöscht wird, sperrst du dich sonst selbst aus deiner eigenen Website aus!

4. Best Practices für Administratoren

Gnadfrist (Grace Period): Wie man Usern Zeit gibt, 2FA einzurichten, bevor sie ausgesperrt werden.

Backup-Codes: Warum man den Teilnehmern einschärfen muss, die Notfall-Codes auszudrucken.

XML-RPC: Warum man diesen alten Zugang deaktivieren sollte, da er 2FA oft umgeht.

5. Live-Showdown: 2FA in Action

Versuche dich mit einem falschen Passwort einzuloggen (Fehlermeldung).

Logge dich mit korrektem Passwort ein → **Abfrage des 6-stelligen Codes**.

Öffne die Authenticator-App auf deinem Handy und gib den Code ein.

Aha-Effekt: Erkläre, dass der Hacker selbst mit deinem Passwort jetzt hier scheitern würde.

"Was tun, wenn ich ausgesperrt bin?" (Wichtiger Notfall-Teil)

Per FTP den Plugin-Ordner umbenennen.

Per `wp-config.php` den Zugriff erlauben.

(Das nimmt den Leuten die Angst vor der Technik!)

Plugin: Two Factor (Repo) Vorteile

Kein Werbe-Ballast: Im Gegensatz zu vielen anderen Plugins gibt es hier keine nervigen Banner oder "Upgrade auf Pro"-Hinweise.

Passkey-Support: Unterstützt modernste Login-Methoden wie Biometrie (TouchID/FaceID) oder Hardware-Schlüssel (Yubikey).

Zukunftssicher: Sehr nah am WordPress-Standard programmiert; die Wahrscheinlichkeit für Konflikte mit anderen Plugins ist minimal.

Flexibilität: Jeder Nutzer kann selbst entscheiden, welche Methode er bevorzugt (z.B. App oder E-Mail).

Plugin: Two Factor (Repo) Nachteile

Kein "Zwang"-Feature: In der Standard-Version kann man Nutzer nicht dazu zwingen, 2FA zu aktivieren (hierfür bräuchte man Zusatz-Code oder ein anderes Plugin).

Minimalistisches Design: Es gibt kein schickes Dashboard. Die Einstellungen verstecken sich schlicht im jeweiligen Benutzerprofil.

Wenig Dokumentation: Da es ein Community-Projekt ist, gibt es kein professionelles Support-Team oder umfangreiche Handbücher.

Notfall-Plan: "Hilfe, ich bin ausgesperrt!"

Keine Panik! Wenn dein Handy weg ist oder der Code nicht akzeptiert wird, gibt es drei Wege zurück in dein WordPress-Dashboard:

Methode 1: Die Backup-Codes (Der offizielle Weg)

Prävention: Lade dir bei der Einrichtung der 2FA die **Backup-Codes** herunter und speichere sie an einem sicheren Ort (nicht nur auf dem Handy!).

Anwendung: Gib beim Login statt des App-Codes einfach einen deiner 10 Einmal-Codes ein.

Methode 2: Der "Ordner-Trick" (Über FTP/Dateimanager)

Wenn du keinen Zugriff mehr hast, kannst du das Plugin von außen deaktivieren:

- Verbinde dich per **FTP** (z. B. FileZilla) oder über das Hosting-Panel mit deinem Server.
- Navigiere zum Ordner: `/wp-content/plugins/`.
- Suche den Ordner des 2FA-Plugins (z. B. `two-factor`).
- Benenne den Ordner um in `two-factor-STOP`.
- **Ergebnis:** WordPress findet das Plugin nicht mehr, deaktiviert es automatisch, und du kannst dich wieder nur mit deinem Passwort einloggen. (Danach den Ordner wieder zurückbenennen!).

Methode 3: Die WP-CLI (Für Profis)

Wenn du Zugriff per SSH hast, kannst du 2FA pro Benutzer mit einem Befehl deaktivieren:

```
wp two-factor disable [username]
```

(Oder das Plugin komplett deaktivieren: `wp plugin deactivate two-factor`*)*

Goldener Rat

"Ein Backup-Code in deinem physischen Geldbeutel ist sicherer als jeder Cloud-Speicher."

Benutzerfreundliche 2FA mit dem Plugin "WP 2FA"

Zwei-Faktor-Authentifizierung einrichtet, die auch für Kunden oder weniger technikaffine Nutzer einfach zu bedienen ist.

1. Warum WP 2FA? (Der USP)

Der Wizard: Während andere Plugins kryptische Einstellungen haben, führt WP 2FA den Admin und die Nutzer durch einen **Einrichtungs-Assistenten**.

Flexibilität: Es bietet mehr als nur Apps; es unterstützt auch E-Mail-Codes (gut für Nutzer ohne Smartphone-Affinität).

Kontrolle: Du kannst 2FA für das gesamte Team zur Pflicht machen.

2. Die Einrichtung
(Live-Demo oder Screenshots)

Schritt 1: Globale Einstellungen. Lege fest, welche Methoden erlaubt sind (TOTP-Apps wie Google Authenticator, E-Mail-Codes oder Backup-Codes).

Schritt 2: Die "Gnadenfrist" (Grace Period). Erkläre die Funktion: *"Ihr habt 3 Tage Zeit, 2FA einzurichten, danach wird der Zugang gesperrt."* Das verhindert Frust am ersten Tag.

Schritt 3: Custom Design. Zeige kurz, dass man die 2FA-Seite (in der Free-Version begrenzt, aber vorhanden) an das eigene Branding anpassen kann.

3. Die Nutzer-Perspektive (Der "User Flow")

Zeige, was passiert, wenn sich ein Redakteur das nächste Mal einloggt.

Der Nutzer bekommt eine einfache Anleitung: "Scanne diesen QR-Code".

Aha-Erlebnis: Es ist kein technisches Vorwissen nötig, da das Plugin den Nutzer an die Hand nimmt.

4. Features der kostenlosen Version (Repository)

Support für alle gängigen Apps: Google Authenticator, Authy, Microsoft Authenticator.

Backup-Codes: Werden automatisch generiert und dem Nutzer zum Download angeboten.

E-Mail-Verifizierung: Ein Code wird per E-Mail gesendet (wichtig für Firmen-Accounts ohne Diensthandy).

5. Vergleich: Free vs. Premium (Kurz anreißen)

Free: Alles Nötige für Sicherheit ist drin.

Premium: Bietet zusätzliche Features wie "Trusted Devices" (man muss den Code nur alle 30 Tage eingeben) oder SMS-Versand.

Tipp für das Meetup: Erwähne, dass die Free-Version für 95% der Blogs völlig ausreicht.

WP 2FA (Free) / Vorteile

Beste User-Experience im Repository.

Sehr detaillierte Berichte (Wer hat 2FA schon aktiviert?).

Hohe Kompatibilität mit WooCommerce und individuellen Login-Seiten.

Etwas "schwerfälliger" als das schlanke *Two Factor*.

Enthält dezente Hinweise auf die Premium-Version.

Two Factor - Anleitung

Aktivierung: Wo findet man die Einstellungen nach der Installation (Profilseite vs. globale Einstellungen)?

Priorisierung: Wie legt man fest, welche Methode (App oder E-Mail) primär genutzt werden soll?

Notfall-Plan: Wie sieht der Prozess für die Backup-Codes aus?

Besonderheit: Kann man bestimmte Methoden für Nutzer komplett deaktivieren?

Two Factor in WordPress einrichten

1. Installation

   Gehe in deinem WordPress-Backend auf **Plugins → Installieren**.

   Suche nach **"Two Factor"**.

   Achte darauf, dass es das Plugin von *Plugin Contributors* ist (oft mit dem blauen Icon).

   Klicke auf **Jetzt installieren** und dann auf **Aktivieren**.

2. Die Einrichtung im Benutzerprofil

Das Plugin ist sofort aktiv, aber noch für keinen Nutzer konfiguriert.

Navigiere zu **Benutzer → Profil** (oder klicke oben rechts auf deinen Namen).

Scrolle nach unten zum neuen Abschnitt **Zwei-Faktor-Authentisierung**.

Two Factor in WordPress einrichten

3. Methoden wählen und priorisieren

Du siehst nun eine Tabelle mit verschiedenen Optionen. Hier ist die empfohlene Vorgehensweise:

- **Zwei-Faktor-App (TOTP):** Setze den Haken bei **Aktiv**. Scrolle zum QR-Code, scanne ihn mit deiner App (z. B. Google Authenticator, Authy oder Bitwarden) und gib den Bestätigungscode ein.
- **Backup-Codes:** Aktiviere diese unbedingt! Klicke auf "Codes generieren" und speichere sie an einem sicheren Ort (Passwortmanager oder Ausdruck). Sie sind dein "Notfallschlüssel".
- **E-Mail:** Kann als Fallback aktiviert werden, ist aber weniger sicher als die App.

Wichtig: Wähle in der Spalte **Primär** deine bevorzugte Methode aus (meistens die App).

Two Factor in WordPress einrichten

4. Testen

   Melde dich aus WordPress ab.

   Gib deine normalen Zugangsdaten (Benutzername & Passwort) ein.

   Im zweiten Schritt wirst du nun nach dem **6-stelligen Code** aus deiner App gefragt.

Profi-Tipp für Administratoren

Wenn du erzwingen möchtest, dass alle Benutzer (oder nur bestimmte Rollen) 2FA nutzen, stößt das Plugin "Two Factor" an seine Grenzen, da es eher auf Freiwilligkeit setzt.

Falls du das Meetup-Publikum beeindrucken willst: Erwähne, dass man für einen "Zwangsumstieg" (Enforcement) oft zusätzliche Plugins wie **WP 2FA** benötigt oder ein kleines Code-Snippet nutzen muss, das prüft, ob der User 2FA aktiv hat, bevor er das Dashboard betreten darf.

Der Notfall #1

1. Der Weg über FTP (Der "Stecker-ziehen"-Trick)

Dies ist die schnellste Methode, um die Sperre temporär aufzuheben:

Logge dich per **FTP** (z. B. FileZilla) oder über den Dateimanager deines Hosters auf deinem Server ein.

Navigiere zum Ordner `/wp-content/plugins/`.

Benenne den Ordner des Plugins um (z. B. von `two-factor` in `two-factor-DEAKTIVIERT`).

Ergebnis: WordPress findet das Plugin nicht mehr, die 2FA-Abfrage ist sofort deaktiviert und du kannst dich nur mit Passwort einloggen. Sobald du drin bist, benenne den Ordner zurück und richte 2FA neu ein.

Der Notfall #2

2. Der Weg über die Datenbank (Für Profis)

Wenn du Zugriff auf **phpMyAdmin** hast, kannst du die 2FA-Einstellung gezielt für deinen User löschen, ohne das Plugin für alle anderen zu deaktivieren:

Suche die Tabelle `wp_usermeta`.

Suche nach Einträgen mit dem `meta_key`, der mit `_two_factor` beginnt (z. B. `_two_factor_enabled_providers`).

Lösche diesen Wert für deine `user_id`.

Nun ist 2FA nur für deinen Account abgeschaltet.

Der Notfall #3

3. Der Weg über WP-CLI (Die eleganteste Lösung)

Falls du SSH-Zugriff hast, reicht ein einziger Befehl, um die 2FA-Einstellungen eines Nutzers zurückzusetzen: `wp user meta delete [DEIN_USERNAME] _two_factor_enabled_providers`

3 Open-Source Authenticator-Apps

1. Aegis Authenticator (Der Goldstandard für Android)

Aegis ist unter Android-Nutzern extrem beliebt, weil es Sicherheit mit massivem Komfort verbindet.

Vorteile: Komplett Open Source, unterstützt verschlüsselte Backups, Biometrie-Sperre (Fingerabdruck) und man kann die Icons der Einträge anpassen.

Highlight: Du kannst deine Datenbank als Datei exportieren – du bist also nie an die App gebunden.

3 Open-Source Authenticator-Apps

2. Ente Auth (Modern & Cross-Platform)

Wenn du eine Lösung suchst, die auf **iOS, Android und dem Desktop** funktioniert, ist Ente Auth aktuell der Geheimtipp.

- **Vorteile:** Wunderschönes Design, Open Source und bietet eine **Ende-zu-Ende-verschlüsselte Cloud-Synchronisation**.
- **Highlight:** Perfekt für Leute, die ihre Codes auf mehreren Geräten (z.B. Handy und Tablet) synchron halten wollen, ohne auf Sicherheit zu verzichten.

3 Open-Source Authenticator-Apps

3. FreeOTP / FreeOTP+

Ursprünglich von Red Hat entwickelt, ist dies die puristischste Variante.

Vorteile: Extrem schlank, keine unnötigen Berechtigungen, absolut werbefrei.

Nachteil: Die Bedienung ist sehr funktional und bietet weniger Komfort-Features (wie Backups) als Aegis.

Argumente für Open-Source-Apps

Es gibt drei starke Argumente für Open-Source-Apps, die bei deinem Publikum (besonders bei Technik-Affinen) gut ankommen:

Kein "Vendor Lock-in": Bei Google Authenticator war es lange Zeit extrem schwer, die Codes auf ein neues Handy zu übertragen, ohne beide Geräte gleichzeitig zu haben. Open-Source-Apps wie Aegis erlauben den einfachen Export in standardisierte Formate.

Privatsphäre: Google und Microsoft wissen theoretisch, bei welchen Diensten du 2FA nutzt. Eine lokale Open-Source-App wie Aegis teilt diese Info mit niemandem.

Sicherheit durch Transparenz: "Security through obscurity" (Sicherheit durch Geheimhaltung) funktioniert selten. Offener Code bedeutet, dass Schwachstellen schneller gefunden und behoben werden.