immoGenio

No. 02
Mai 2026

2FA

Zwei-Faktor-Authentifizierung in der Hausverwaltung: TOTP, Backup-Codes und der NIST-Hinweis, der SMS-2FA aussortiert

TOTP statt SMS-2FA für Hausverwaltungs-Software: RFC 6238, Backup-Codes, Recovery-Strategie und der NIST-SP-800-63B-Punkt, der SMS aussortiert.

AUTOR
ImmoGenio

VERÖFFENTLICHT
9. Mai 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

Eine Phishing-Mail, ein Klick, 17.500 Euro weg

Stellen Sie sich folgenden Vorgang vor. An einem Donnerstagvormittag bekommt der Buchhalter einer mittelgroßen Verwaltung eine Mail, die aussieht wie eine Sicherheitswarnung seines Software-Anbieters. „Ungewöhnlicher Login aus Frankfurt, bitte bestätigen Sie Ihr Konto." Der Mitarbeiter klickt auf den Bestätigungs-Link, landet auf einer Seite, die exakt wie die echte Login-Maske aussieht, und gibt Benutzername und Passwort ein. Es passiert scheinbar nichts. Er wundert sich kurz, schließt den Tab und arbeitet weiter.

Vierzehn Tage später meldet sich eine Eigentümergemeinschaft, weil eine Sammelüberweisung über 17.500 Euro auf ein Konto in einem anderen EU-Land gegangen ist, das niemand kennt. Der Vorgang ist im System dokumentiert, mit dem Account des Buchhalters, mit korrektem Login, mit einem ordnungsgemäßen SEPA-Lastschrift-Lauf. Es war kein Insider, es war kein Bug, es war ein gestohlenes Passwort. Der Schaden ist real, die Versicherung diskutiert über grobe Fahrlässigkeit, und der nächste Datenschutz-Audit-Termin steht in zwei Wochen an.

Der Vorfall ist kein hypothetisches Szenario. Er ist die Begründung, warum jedes Konto in einer Hausverwaltungs-Software mit Schreibrechten auf Bankverbindungen, SEPA-Mandaten oder Mahnwesen einen zweiten Faktor benötigt. Wer ein Passwort erbeutet, soll an einer zweiten Hürde scheitern, die er nicht aus einer Mail abphishen kann.

Warum 2FA in der Hausverwaltung nicht optional ist

Hausverwaltungs-Konten sind keine gewöhnlichen Office-Logins. An ihnen hängen Bankverbindungen über Open-Banking-Schnittstellen, SEPA-Mandate, Kautionsauszahlungen, Mahnläufe und im WEG-Bereich auch der Zugriff auf Eigentümerdaten und Beschlussunterlagen. Die typische Schadenshöhe einer kompromittierten E-Mail-Identität ist eine peinliche Mail. Die typische Schadenshöhe einer kompromittierten Verwalter-Identität ist eine fehlgeleitete Sammelüberweisung im fünfstelligen Bereich plus Datenschutz-Vorfall plus Reputationsschaden bei den Eigentümern.

Art. 32 DSGVO verlangt „dem Risiko angemessene technische und organisatorische Maßnahmen". Die Aufsichtsbehörden lesen das nicht abstrakt. Bei Software, die Banking-Schnittstellen einbindet und unter PSD2 mit starker Kundenauthentifizierung (SCA) interagiert, ist Mehr-Faktor-Authentifizierung schlicht Stand der Technik. Auch das BSI weist in seiner Technischen Richtlinie TR-03116 und im IT-Grundschutz-Baustein ORP.4 ausdrücklich auf MFA für privilegierte Zugänge hin. Wer als Verwalter mit Zugriff auf Treuhandkonten arbeitet und kein 2FA betreibt, hat im Schadensfall eine sehr unangenehme Beweislast.

Die drei Faktor-Klassen

Die ISO-Definition von Mehr-Faktor-Authentifizierung kennt drei Klassen, die unabhängig voneinander gestohlen werden müssen, damit der Schutz wirkt.

- **Wissen**: etwas, das nur der Nutzer weiß. Passwort, PIN, Sicherheitsfrage.
- **Besitz**: etwas, das nur der Nutzer hat. Smartphone mit Authenticator-App, Hardware-Token, Smartcard.
- **Inhärenz**: etwas, das der Nutzer ist. Fingerabdruck, Gesichts-Scan, Iris.

Echte Zwei-Faktor-Authentifizierung ist die Kombination aus zwei verschiedenen Klassen. Passwort plus zweite Sicherheitsfrage ist kein 2FA, beides gehört zur Klasse Wissen. Passwort plus TOTP-Code aus dem Smartphone ist Wissen plus Besitz und damit echte 2FA. Im B2B-SaaS-Kontext der Hausverwaltung ist die Standardkombination Passwort plus TOTP, weil sie ohne Zusatz-Hardware auskommt und auf jedem Smartphone funktioniert.

TOTP technisch — was RFC 6238 wirklich beschreibt

Time-based One-Time Password ist in RFC 6238 standardisiert und basiert auf RFC 4226 (HOTP). Beim Setup wird zwischen Server und Authenticator-App ein gemeinsames Geheimnis ausgetauscht, üblicherweise 160 Bit zufällig erzeugt und Base32-kodiert. Dieses Geheimnis verlässt den Server genau einmal: beim Anzeigen des QR-Codes, der eine `otpauth://totp/...`-URI enthält. Die App speichert das Geheimnis lokal auf dem Gerät, der Server in einer per Schlüssel verschlüsselten Spalte.

Aus diesem Geheimnis und der aktuellen Unix-Zeit, geteilt durch 30 Sekunden, berechnen beide Seiten unabhängig voneinander einen HMAC-SHA1-Hash. Aus diesem Hash werden per dynamischer Truncation sechs Dezimalstellen extrahiert. Genau diese sechs Ziffern tippt der Nutzer ein. Weil beide Seiten das gleiche Geheimnis und dieselbe Zeit nutzen, kommen sie auf denselben Code, ohne dass das Geheimnis je übertragen wird.

Drei Punkte sind in der Implementierung kritisch.

- **Zeitsynchronisation**: Wenn die Uhr des Smartphones um 90 Sekunden falsch geht, schlägt jede Verifikation fehl. Server-seitig akzeptieren wir typischerweise das aktuelle Zeitfenster plus minus einen Slot, also 30 Sekunden Drift in beide Richtungen. Mehr Toleranz schwächt die Sicherheit, weniger erzeugt Support-Tickets.
- **Replay-Schutz**: Ein einmal verbrauchter Code darf im selben Zeitfenster nicht erneut akzeptiert werden, sonst kann ein Angreifer mit einem geschulterten Blick auf das Display einen Login wiederholen.
- **Brute-Force-Schutz**: Sechs Stellen sind eine Million Möglichkeiten. Ohne Rate Limiting hat ein Angreifer mit ausreichend vielen Versuchen statistisch innerhalb weniger

Stunden einen Treffer. Wir limitieren auf wenige Versuche pro Zeitfenster und sperren den Account temporär.

Algorithmus-Hinweis: RFC 6238 erlaubt SHA-1, SHA-256 und SHA-512. Authenticator-Apps wie Google Authenticator und Microsoft Authenticator unterstützen SHA-1 verlässlich, neuere Apps auch SHA-256. ImmoGenio verwendet SHA-1 für maximale Kompatibilität, was unter Krypto-Gesichtspunkten unkritisch ist, weil HMAC-SHA1 in dieser Konstruktion nicht angreifbar ist.

SMS-2FA und der NIST-Hinweis

SMS-2FA gilt umgangssprachlich oft als „auch 2FA". Technisch und regulatorisch ist es deutlich schwächer als TOTP. NIST SP 800-63B führt Out-of-Band-OTP über SMS bereits seit 2017 als „restricted authenticator". Die Revision 4, derzeit in der Konsultationsphase, hält an dieser Einstufung fest. Ein Restricted Authenticator darf eingesetzt werden, erfordert aber zusätzliche Risikoabwägungen und einen Migrationsplan auf einen stärkeren Faktor.

Die Gründe sind bekannt und gut dokumentiert.

- **SIM-Swapping**: Ein Angreifer überzeugt den Mobilfunk-Provider, die Rufnummer auf eine neue SIM zu portieren. Sämtliche SMS, auch der 2FA-Code, gehen ab diesem Moment an den Angreifer.
- **SS7-Schwachstellen**: Das Signalisierungsprotokoll der Mobilnetze erlaubt unter bestimmten Bedingungen das Mitlesen von SMS, ohne die SIM zu manipulieren.
- **Phishing über Echtzeit-Proxy**: Eine täuschend echte Login-Maske leitet das eingegebene Passwort und den nachgereichten SMS-Code in Echtzeit an die echte Anwendung weiter und erbeutet die Session.
- **Provider-Zustellungsfehler**: SMS sind kein Echtzeit-Medium mit Zustellungsgarantie. In Roaming-Situationen kommen Codes verspätet oder gar nicht an.

Für Hausverwaltungs-Konten mit Banking-Zugriff lautet die Empfehlung deshalb klar: TOTP oder, wo verfügbar, Hardware-Token nach FIDO2/WebAuthn. SMS nur als Übergangsfaktor mit zusätzlichem Risk-Scoring (geographische Anomalien, neue Geräte, ungewöhnliche Tageszeiten). Wer SMS als alleinigen zweiten Faktor anbietet, lebt regulatorisch auf Bewährung.

Backup-Codes als Recovery-Anker

Was passiert, wenn der Buchhalter sein Smartphone verliert oder die Authenticator-App durch ein OS-Update unbrauchbar wird? Ohne Recovery-Pfad ist der Account gesperrt, und genau diese Lockout-Angst ist der häufigste Grund, warum Verwaltungen 2FA gar

nicht erst ausrollen. Die saubere Antwort sind Backup-Codes.

Beim Aktivieren von TOTP generiert der Server zehn Einmal-Codes, je acht oder zehn Zeichen lang, und zeigt sie genau einmal im UI. Der Nutzer druckt sie aus, klebt sie in den Tresor, legt sie ins Bankschließfach oder hinterlegt sie im Passwort-Manager. Drei Eigenschaften sind technisch zwingend.

- **Hash-only in der Datenbank**: Backup-Codes liegen niemals im Klartext. Sie werden mit bcrypt oder Argon2 gehasht, exakt wie Passwörter. Bei Verifikation wird der eingegebene Code durch dieselbe Hash-Funktion geschickt und mit dem gespeicherten Hash verglichen.
- **Single-Use**: Jeder Code gilt genau einmal. Nach erfolgreicher Verwendung wird der Datensatz als verbraucht markiert oder gelöscht.
- **Audit-Eintrag pro Verwendung**: Jede Verwendung eines Backup-Codes erzeugt einen Eintrag im Audit-Trail mit Timestamp, IP-Adresse und User-Agent. Das ist die Grundlage für die forensische Aufklärung im Schadensfall.

Wenn weniger als drei Codes übrig sind, weist die Software den Nutzer aktiv darauf hin und bietet eine Neugenerierung an. Bei Neugenerierung werden alle alten Codes invalidiert. Wer das versäumt, hat irgendwann einen Stapel halb verbrauchter Code-Listen im Tresor und keine klare Quelle mehr.

Recovery ohne Lockout

Backup-Codes sind die erste Verteidigungslinie. Wenn auch sie verloren gehen, braucht es einen abgestuften Recovery-Pfad, der weder den Nutzer aussperrt noch zur Hintertür für Angreifer wird.

- **Stufe 1 — Backup-Code (Self-Service)**: Der Nutzer wählt im Login-Dialog „Backup-Code verwenden", tippt einen seiner Codes, der Code wird verbraucht, ein Audit-Eintrag entsteht. Kein Eingriff durch Dritte nötig.
- **Stufe 2 — Tenant-Admin-Reset (Vier-Augen)**: Der Tenant-Admin kann für einen anderen Nutzer den 2FA-Faktor zurücksetzen. Der Vorgang erzeugt einen Audit-Eintrag mit Begründung und benachrichtigt den betroffenen Nutzer per Mail. Beim nächsten Login muss der Nutzer einen neuen TOTP-Faktor einrichten. Damit ein Tenant-Admin nicht beliebig fremde Konten übernehmen kann, ist der Reset auf die explizite Permission `mfa.reset` beschränkt und im Audit besonders gekennzeichnet.
- **Stufe 3 — Identity-Verification durch Support**: Wenn der einzige Tenant-Admin selbst sein Smartphone verliert und keine Backup-Codes mehr hat, übernimmt der ImmoGenio-Support. Die Verifikation läuft über die im Vertrag hinterlegten Kontaktdaten und gegebenenfalls einen Video-Call mit Ausweisabgleich. Erst nach

erfolgreicher Identitätsprüfung wird der MFA-Faktor zurückgesetzt. Auch dieser Vorgang landet im Audit-Trail des Tenants.

Die Reihenfolge ist nicht kosmetisch. Sie sorgt dafür, dass der Standardfall (verlorenes Handy) ohne menschliches Zutun lösbar ist, der Sonderfall (Sole-Admin ohne Backup-Codes) trotzdem nicht im Datenfriedhof endet, und Angreifer nicht über einen freundlichen Support-Anruf eine Authentifizierung umgehen können.

Wer 2FA bekommen sollte

Nicht jedes Konto muss zwingend 2FA tragen. Eine Pflicht, die zu breit greift, wird im Alltag aufgeweicht und damit wertlos. Eine Pflicht, die zu schmal greift, schützt den falschen Bereich. Praxisgerechte Abstufung sieht so aus.

- **Pflicht**: alle Admin-Rollen (Tenant-Admin, Buchhalter mit Schreibrecht, Mietverwalter mit SEPA-Zugriff). Hier ist 2FA nicht verhandelbar, sondern Voraussetzung für die Aktivierung der Rolle.
- **Empfehlung**: WEG-Verwalter und alle Nutzer mit Lese-Zugriff auf Eigentümerdaten. Hier ist 2FA optional, aber dringend empfohlen, und kann durch eine Tenant-Policy zur Pflicht gemacht werden.
- **Empfehlung**: alle externen Dienstleister mit API-Zugang. Service-Accounts werden zusätzlich durch IP-Whitelisting und kurzlebige API-Keys abgesichert.
- **Optional**: Mieter im Self-Service-Portal. Wer eine Schadensmeldung anlegt oder eine Abrechnung herunterlädt, verändert keine kritischen Daten. Eine 2FA-Pflicht würde die Akzeptanz des Portals senken und im Notfall (Wasserschaden um 23 Uhr) den Mieter aussperren.

Diese Abstufung ist tenant-konfigurierbar. Eine Verwaltung, die für ihre Mieter ebenfalls 2FA verpflichten möchte, kann das per Policy aktivieren. Der Default ist bewusst unaufgeregt.

Praxis-Beispiel: ein WEG-Verwalter, ein gestohlenes Passwort, kein Schaden

Frau Berger ist WEG-Verwalterin und aktiviert TOTP über Google Authenticator. Sie scannt im Setup-Dialog den QR-Code, gibt einmal den aktuellen sechsstelligen Code ein, druckt die zehn Backup-Codes aus und legt sie in den Bürotresor. Beim nächsten Login nach Session-Ablauf tippt sie ihr Passwort und anschließend den TOTP-Code aus der App. Insgesamt drei Sekunden Mehraufwand.

Drei Wochen später wird ihr E-Mail-Konto bei einem Provider-Vorfall kompromittiert. Der Angreifer probiert das gleiche Passwort beim ImmoGenio-Login. Er kommt durch den ersten Faktor, scheitert aber am zweiten. Das System protokolliert mehrere fehlgeschlagene 2FA-Versuche aus einer ungewöhnlichen Geo-Region, sperrt den Account temporär und schickt eine Anomalie-Alert-Mail an Frau Berger und an den Tenant-Admin. Frau Berger setzt ihr Passwort zurück, der Tenant-Admin prüft den Audit-Trail, kein Schaden, kein Datenabfluss, kein Datenschutz-Vorfall.

Genau das ist der Punkt. 2FA verhindert nicht den Diebstahl von Passwörtern, sondern entwertet ihn.

Wie ImmoGenio das umsetzt

Die Implementierung lebt im Service `mfa.service.ts`, der in die Auth-Pipeline eingehängt ist. Drei Tabellen sind in der Baseline-Migration angelegt: das verschlüsselte TOTP-Geheimnis pro Nutzer, `mfa_backup_codes` mit bcrypt-gehashten Einmal-Codes und `mfa_challenge_tokens` für die kurzlebigen Tokens, die zwischen erstem und zweitem Faktor den Login-Zustand halten.

Ablauf bei Login: Nutzername plus Passwort werden geprüft, bei Erfolg wird ein Challenge-Token mit kurzer Lebensdauer ausgestellt und der Client zur 2FA-Eingabe weitergeleitet. Die TOTP- oder Backup-Code-Verifikation tauscht den Challenge-Token gegen das eigentliche Session-Token. Jeder Schritt erzeugt einen Audit-Eintrag, jeder Fehlversuch fließt in das Rate Limiting ein. Beim Aktivieren wird das TOTP-Geheimnis erst nach erfolgreicher Verifikation des ersten Codes persistiert, damit ein abgebrochenes Setup keinen halbgaren 2FA-Status hinterlässt.

Backup-Codes werden bei der Aktivierung als bcrypt-Hash gespeichert, einmalig im Klartext angezeigt und bei Verwendung als verbraucht markiert. Die Anzeige der Restzahl im UI ist nicht Spielerei, sondern Teil der Lockout-Prävention.

Verbindung zu Google OAuth und Single Sign-On

Wer sich per Google-Konto anmeldet, bekommt 2FA über Google geschenkt, sofern beim Google-Konto selbst 2FA aktiv ist. Das ist bequem und für viele Standardnutzer ausreichend. Für Admin-Konten empfehlen wir trotzdem zusätzlich TOTP direkt in ImmoGenio. Defense in Depth bedeutet, dass eine Kompromittierung des Identity-Providers nicht zum vollständigen Verlust der Authentifizierungsbarriere führt. Wenn ein Google-Konto kompromittiert wird und der Verwalter dort kein 2FA aktiv hat, schützt der zweite Faktor in ImmoGenio den eigentlichen Wertzugang.

Verbindung zum RBAC

Die rollenbasierte Zugriffssteuerung in ImmoGenio kann an den MFA-Status gekoppelt werden. Eine Permission wie `banking.sepa.export` lässt sich so konfigurieren, dass sie nur dann effektiv wird, wenn der Nutzer einen aktiven zweiten Faktor besitzt und in der laufenden Session erfolgreich verifiziert ist. Damit gibt es keine Privilegieneskalation über ein Konto, das aus historischen Gründen ohne 2FA läuft. Das passt zum Prinzip „Sensitive Actions step-up", wie es OWASP im Authentication Cheat Sheet beschreibt: kritische Aktionen können einen erneuten zweiten Faktor erfordern, auch wenn die Session noch gültig ist.

Verbindung zum Audit-Trail

Jeder MFA-Vorgang ist ein eigener Eintrag im Audit-Trail. Setup, Reset, erfolgreicher Login, fehlgeschlagener Login, Backup-Code-Verwendung — alles append-only mit Timestamp, IP, User-Agent und Begründung. Das ist nicht nur Compliance-Hygiene, sondern auch der wichtigste Datensatz im Schadensfall. Wenn ein Vorfall analysiert wird, ist die erste Frage immer: Wie kam der Login zustande, was war der zweite Faktor, gab es Anomalien? Ohne Audit-Trail ist diese Frage nicht beantwortbar.

Verbindung zum Offboarding

Beim User-Offboarding werden alle TOTP-Geheimnisse und Backup-Codes desselben Nutzers in einer einzigen Transaktion invalidiert. Das ist nicht trivial, denn ein vergessenes 2FA-Geheimnis nach Offboarding ist exakt der Fall, in dem ein gekündigter Mitarbeiter mit altem Endgerät noch eine Weile Codes generieren könnte. Die saubere Lösung ist, die Geheimnisse zusammen mit der Account-Deaktivierung zu löschen und im Audit zu dokumentieren.

Verbindung zum Onboarding

Bereits im Onboarding-Wizard wird der initiale Tenant-Admin durch das 2FA-Setup geführt. Wer beim ersten Login die Backup-Codes nicht generiert, wird bei jedem weiteren Login darauf hingewiesen, bis es erledigt ist. Das ist absichtlich freundlich-penetrant, weil ein nachgelagertes Hinzufügen von 2FA in der Praxis selten passiert, sobald der Alltag eingekehrt ist.

Wo wir bewusst noch nicht sind

Drei Punkte bleiben auf der Roadmap.

- **WebAuthn / Passkeys**: Der modernere Faktor, geräte-gebunden, phishing-resistent, ohne Geheimnis-Sharing. Geplant für eine spätere Version. TOTP bleibt erhalten, weil es im B2B-Kontext mit gemischten Endgeräten universeller funktioniert.
- **FIDO2-Hardware-Token**: YubiKey und Vergleichbares wären für Buchhalter mit besonders hohem Risiko die ideale Lösung. Noch nicht im Standard-Pricing, auf Anfrage über die Roadmap diskutierbar.
- **Adaptives Risk-Based Auth**: Step-up-Authentifizierung nur bei Anomalien (neues Gerät, neue IP, unüblicher Tag). Aktuell gibt es Anomalie-Erkennung mit Mail-Alert, aber kein automatisches Step-up. Auf der Roadmap.

Diese Lücken werden offen kommuniziert, weil das Thema Authentifizierung keine Marketing-Bühne verträgt. Wer mehr verspricht als implementiert ist, baut Sicherheits-Theater statt Sicherheit.

Wo wir stehen — produktiv

Die in diesem Artikel beschriebenen Funktionen — TOTP-Setup, Backup-Codes mit Single-Use, abgestuftes Recovery, Kopplung an RBAC und Audit-Trail, Invalidierung beim Offboarding — sind in ImmoGenio produktiv. Sie laufen ohne Zusatzkosten in jedem Tenant, der 2FA aktiviert. Tenant-Admins können in der Sicherheits-Konfiguration entscheiden, welche Rollen 2FA als Pflicht haben. Wer eine Verwaltung mit Banking-Zugriff betreibt und noch ohne 2FA arbeitet, sollte heute den nächsten Wartungstermin nutzen, um den Standard zu setzen, bevor es eine Mail tut, die niemand öffnen wollte.

Wenn Sie wissen möchten, wie 2FA mit den restlichen Sicherheitsbausteinen zusammenspielt — von SEPA-Lastschrift-Sammelläufen bis zum Open-Banking-Mieteingang über fin-API — schreiben Sie uns. Wir zeigen Ihnen die Konfiguration in Ihrem Tenant und gehen den Recovery-Pfad mit Ihnen durch, damit der erste Lockout nicht der erste Härtetest wird.

Erreichbar unter kontakt@immogenio.de.