Engineer

Mehrfaktor-Authentifizierung

Anmeldung mit mindestens zwei verschiedenen Nachweisarten

Was es ist

Mehrfaktor-Authentifizierung, meist MFA genannt, ist eine Anmeldung, die eine behauptete Identität nur mit mehr als einer Art von Nachweis akzeptiert. NIST SP 800-63B-4, die US-Bundesrichtlinie zur Authentifizierung, der auch viele Organisationen außerhalb des Staatssektors folgen, nennt drei Arten: etwas, das man weiß, etwa ein Passwort; etwas, das man hat, etwa ein Telefon oder einen Sicherheitsschlüssel; und etwas, das man ist, etwa ein Fingerabdruck. Ihre Definition hängt an einem Wort. Das System muss mehr als eine unterschiedliche Faktorart verlangen. Ein Passwort und die Antwort auf eine Sicherheitsfrage ergeben deshalb nur einen Faktor: Beides ist Wissen. Zwei-Faktor-Authentifizierung, kurz 2FA, ist der häufige Fall mit genau zwei Faktoren.

Die Richtlinie akzeptiert zwei Wege dorthin. Der erste kombiniert getrennte Ein-Faktor-Authentifikatoren: ein Passwort und zusätzlich eine Telefon-App mit Einmalcodes oder eine Liste ausgedruckter Sicherungscodes. Der zweite verwendet einen einzigen Mehrfaktor-Authentifikator, etwa einen Sicherheitsschlüssel oder ein Telefon, das einen privaten Schlüssel hält und ihn erst nach einer PIN oder einem Fingerabdruck verwendet. PIN oder Fingerabdruck heißen dann Aktivierungsfaktor. Dieser wird auf dem Gerät selbst geprüft. Der Server erhält nur das Ergebnis, eine überprüfbare Signatur. Eine einzige Berührung liefert damit zwei Faktoren.

Biometrie hat dabei einen eng begrenzten Platz. NIST erlaubt Fingerabdruck oder Gesicht nur, wenn zugleich ein physischer Authentifikator an der Authentifizierung beteiligt ist, nie als eigenständigen Faktor. Außerdem muss immer eine nicht biometrische Alternative angeboten werden. Die Richtlinie sagt ausdrücklich, dass biometrische Merkmale nicht geheim sind: Ein Gesicht lässt sich fotografieren und ein Fingerabdruck von einem Gegenstand abnehmen, den die betreffende Person berührt hat.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Mehrfaktor-Authentifizierung?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Ein Passwort kann unbemerkt kopiert werden: durch Eingabe auf einer überzeugenden Kopie der Anmeldeseite, durch Erraten oder durch Wiederverwendung auf einer Website, deren Datenbank später gestohlen wird. MFA sorgt dafür, dass ein kopiertes Passwort allein nicht genügt. Dem Angreifer fehlt weiterhin etwas von anderer Art.

NIST macht das zur Grundlage seiner zweiten Vertrauensstufe. Auf AAL2 muss sich der Nutzer mit zwei Faktoren authentifizieren, entweder in einem Authentifikator kombiniert oder getrennt geliefert. Die Kombination muss einen physischen Authentifikator zusammen mit einem Passwort oder einem biometrischen Vergleich enthalten. Prüfende Systeme müssen auf dieser Stufe mindestens eine phishingresistente Option anbieten. Bundesbehörden müssen für ihre Beschäftigten, Auftragnehmer und Partner phishingresistente Authentifizierung vorschreiben.

Die unter denselben drei Buchstaben verkauften Verfahren unterscheiden sich untereinander stärker als MFA von einem Passwort allein. Die Richtlinie ordnet sie klar:

- **Codes per SMS oder Sprachanruf** sind die einzige Authentifikatorart, die NIST als eingeschränkt einstuft. Sie dürfen weiter verwendet werden, doch das prüfende System muss eine Alternative ohne diese Einstufung anbieten, den Nutzer über das Risiko informieren und einen Plan für die Ablösung haben. Eine Änderung der hinterlegten Telefonnummer gilt als Bindung eines neuen Authentifikators samt allen damit verbundenen Prüfungen.
- **Codes aus einer App und Push-Aufforderungen auf einem Telefon** sind auf AAL2 zulässig, aber nicht phishingresistent: Was die Person eingibt oder bestätigt, ist nicht an die anfragende Website gebunden.

- **Kryptografische Authentifikatoren, die ihre Antwort an die Website binden**, etwa Passkeys und Smartcards, sind phishingresistent. AAL3 verlangt einen, dessen privater Schlüssel sich nicht aus seiner Hardware exportieren lässt.

E-Mail fehlt absichtlich in der Liste: Die Richtlinie schließt sie als Kanal für die Authentifizierung über einen getrennten Übertragungsweg aus.

Wie es in der Praxis aussieht

Der Code in einer Authentifikator-App ist der häufigste zweite Faktor. RFC 6238 vom Mai 2011 definiert ihn auf wenigen Seiten. Bei der Einrichtung erzeugt der Server einen geheimen Schlüssel und übergibt ihn der App, meist als QR-Code. Beide Seiten halten dann denselben Schlüssel. Für einen Code teilt jede Seite die aktuelle Unix-Zeit durch einen Zeitschritt, standardmäßig 30 Sekunden, und verwendet den ganzzahligen Anteil des Ergebnisses als Zähler. Sie berechnet mit dem Schlüssel einen HMAC dieses Zählers und kürzt das Ergebnis auf eine kurze Dezimalzahl. Dafür verwendet sie das HOTP-Verfahren, das RFC 4226 2005 definierte und das mindestens sechs Ziffern verlangt. In Python passt die gesamte Rechnung in wenige Zeilen:

```
import hashlib, hmac, struct

def totp(key: bytes, unix_time: int, digits: int = 6, step: int = 30) -> str:
    counter = struct.pack(">Q", unix_time // step)
    mac = hmac.new(key, counter, hashlib.sha1).digest()
    offset = mac[-1] & 0x0F
    code = struct.unpack(">I", mac[offset:offset + 4])[0] & 0x7FFFFFFF
    return str(code % 10**digits).zfill(digits)

print(totp(b"12345678901234567890", 59, digits=8))  # 94287082
```

Die Testvektoren im RFC verwenden diesen 20-Byte-ASCII-Schlüssel und acht Ziffern. 59 Sekunden nach der Epoche steht der Zähler auf 1, und die SHA-1-Variante liefert 94287082, genau die Ausgabe der Funktion. Der sechsstellige Code einer App besteht aus den letzten sechs Ziffern dieser Ausgabe: 287082. Nichts an der Berechnung greift auf das Netzwerk zu. Deshalb funktioniert die App auch im Flugmodus, und deshalb muss der Server seine eigene Kopie des Schlüssels jedes Nutzers aufbewahren.

Die Prüfung eines Codes ist dieselbe Berechnung auf dem Server mit anschließendem Vergleich. RFC 6238 empfiehlt, wegen Netzwerkverzögerungen höchstens den unmittelbar vorhergehenden Zeitschritt zusätzlich zu akzeptieren. Einen bereits erfolgreich verwendeten Code ein zweites Mal anzunehmen, verbietet er.

Ein Passkey ersetzt das gemeinsame Geheimnis durch ein Schlüsselpaar. Nach Web Authentication Level 3, seit dem 25. August 2026 eine W3C-Empfehlung, erzeugt der Authentifikator ein Schlüsselpaar für eine durch ihre Domain bezeichnete Website und gibt dem Server nur den öffentlichen Schlüssel. Bei der Anmeldung übermittelt der Browser den Origin, mit dem er tatsächlich verbunden ist. Der Authentifikator signiert die Challenge des Servers zusammen mit diesem Origin. Eine auf einer ähnlich aussehenden Domain erzeugte Signatur ist deshalb auf der echten unbrauchbar. Erfordert die Verwendung des Schlüssels eine PIN oder einen Fingerabdruck, ist ein Passkey ein Mehrfaktor-Authentifikator in einem Schritt. WebAuthn nennt Passkeys, die zwischen den Geräten einer Person kopiert werden, geräteübergreifende Zugangsdaten. NIST akzeptiert diese synchronisierten Schlüssel auf AAL2, aber nicht auf AAL3: Ein synchronisierbarer Schlüssel ist definitionsgemäß exportierbar.

MFA einzuschalten ist der einfache Teil. Festzulegen, wer sie verwenden muss, welche Verfahren wo zählen und was bei einem verlorenen Telefon geschieht, ist Kontoverwaltung als Teil der umfassenderen Zugriffsorganisation. Die Leistung für Sicherheits- und Zugriffsverwaltung dieser Website beschreibt diese Organisation: Konten, Passwörter und Berechtigungen so einrichten, dass jede Person genau den Zugang für ihre Arbeit hat und Ausscheidende ihn am Tag ihres Ausscheidens verlieren.

Wo es schiefgeht

Eine Phishing-Seite leitet den Code weiter. Ein Einmalcode ist eine Zahl, die ein Nutzer abliest und eintippt. Nichts darin hält fest, welche Website er angesehen hat. Leitet eine täuschend ähnliche Seite Passwort und Code innerhalb des Zeitschritts an die echte Website weiter, meldet sie sich als Nutzer an. NIST stellt deshalb fest, dass kein Authentifikator mit manuell eingegebener Ausgabe als phishingresistent gilt. Wie der Nutzer auf die gefälschte Seite gelangte, ist dabei unerheblich. Die Lösung ist ein Authentifikator, der seine Antwort an die prüfende Gegenstelle bindet: an deren Domain wie bei WebAuthn oder an den TLS-Kanal selbst wie bei Client-Zertifikaten und Smartcards. Schreiben Sie einen solchen für Administratoren vor und bieten Sie ihn allen anderen an.

Die Telefonnummer ist der Faktor. Ein SMS-Code geht an die Person, an die der Mobilfunkanbieter die Nummer gerade weiterleitet. NISTs eigene Bedrohungsliste nennt einen Angreifer, der den Anbieter zur Umleitung der Nummer des Opfers überredet hat und dann den Code erhält. Vor einem Codeversand per SMS oder Sprachanruf sollten prüfende Systeme auf Hinweise wie einen kürzlichen SIM-Wechsel, eine Rufnummernportierung oder einen Gerätewechsel achten. Behalten Sie SMS als Rückfalloption statt als Hauptverfahren und verlangen Sie vor jeder Änderung der hinterlegten Nummer eine vollständige Anmeldung.

Bestätigen, bestätigen, bestätigen. Eine Push-Aufforderung mit einem einzigen Button zum Bestätigen verlangt eine Entscheidung, keinen Nachweis. Wer das Passwort bereits besitzt, kann Aufforderungen auslösen, bis der vom Lärm ermüdete Nutzer eine akzeptiert. NIST nennt das Authentifizierungsermüdung und hält Abläufe mit bloßer Bestätigung nicht mehr für zulässig: Ein Geheimnis muss von einem Kanal in den anderen übertragen werden, etwa eine Zahl auf dem Anmeldebildschirm, die der Nutzer ins Telefon eintippt. Die Auswahl aus einer kurzen Liste reicht nicht, weil der Nutzer einfach raten könnte. Begrenzen Sie auch, wie viele Aufforderungen seit der letzten erfolgreichen Anmeldung gesendet werden dürfen, wie es die Richtlinie empfiehlt.

Die Wiederherstellung überspringt den zweiten Faktor. Ein Link „Telefon verloren“, der nur das Passwort verlangt oder einen Rücksetzlink per E-Mail sendet, macht MFA zu einer Option, die der Angreifer ablehnen kann. Für Konten auf AAL2 verlangt NIST zur Wiederherstellung zwei über unterschiedliche Verfahren erhaltene Wiederherstellungscodes, einen Wiederherstellungscode plus einen weiterhin ans Konto gebundenen Ein-Faktor-Authentifikator oder eine erneute Identitätsprüfung. Bei jeder Wiederherstellung muss eine Benachrichtigung an den Nutzer gesendet werden. Allgemeiner darf ein Faktor nie ausreichen, um einen Authentifikator einer anderen Art zu erhalten: Ein Passwort allein darf nicht genügen, um einen neuen Satz Sicherungscodes auszudrucken.

Der Code wird zweimal oder zu lange akzeptiert. Ein sechsstelliger Code hat eine Million mögliche Werte. Seine Stärke liegt deshalb in den Regeln darum herum. Akzeptiert ein prüfendes System mehrere Zeitschritte vor oder nach dem aktuellen oder einen bereits verwendeten Code, gibt es einem Angreifer, der einen Code gesehen hat, ein Zeitfenster zur erneuten Verwendung. Speichern Sie pro Nutzer den zuletzt akzeptierten Zeitschritt und weisen Sie alles zu diesem oder einem früheren Schritt zurück. Begrenzen Sie das Fenster auf den einen

Schritt, den RFC 6238 für Verzögerungen erlaubt, und begrenzen Sie aufeinanderfolgende Fehlversuche: NIST erlaubt höchstens 100, bevor der Authentifikator deaktiviert wird.

Die geheimen Schlüssel liegen neben den Passwörtern. App-Codes sind symmetrisch: Der Server hält den Schlüssel jedes Nutzers, und wer diese Schlüssel kopiert, kann gültige Codes für jedes Konto erzeugen. NIST verlangt einen starken Schutz der Schlüssel, mit Zugriff nur für die Softwarekomponenten, die sie benötigen. Speichern Sie sie nicht als unverschlüsselte Spalten neben den Passwort-Hashes. Verschlüsseln Sie sie mit einem Schlüssel aus einem separaten Geheimnisspeicher und lassen Sie nur den Dienst, der Codes prüft, darauf zugreifen.

Weiterführende Lektüre

- NIST SP 800-63B-4, Definitionen und Abkürzungen — die Definitionen von Mehrfaktor-Authentifizierung, Mehrfaktor-Authentifikator und Phishingresistenz in der aktuellen Richtlinie.
- NIST SP 800-63B-4 beim Computer Security Resource Center — der Veröffentlichungsnachweis: erschienen im Juli 2025, ersetzt SP 800-63B.
- RFC 6238: TOTP — der zeitbasierte Einmalpasswort-Algorithmus, seine Testvektoren und die Regeln für abweichende Uhren.
- RFC 4226: HOTP — der darunterliegende zählerbasierte Algorithmus einschließlich der Kürzung auf sechs oder mehr Ziffern.
- Web Authentication, Level 3 — die W3C-Spezifikation hinter Passkeys mit Origin-gebundenen Zugangsdaten und synchronisierten Passkeys.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist Mehrfaktor-Authentifizierung?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/multi-factor-authentication/