Engineer

Multifaktorautentificering

login, der kræver to eller flere forskellige slags bevis

Hvad det er

Multifaktorautentificering, i daglig tale MFA, er et login, der kun godtager en påstået identitet, når den er bakket op af mere end én slags bevis. NIST SP 800-63B-4 er den amerikanske føderale retningslinje for autentificering, og mange organisationer uden for det offentlige følger den også. Den nævner tre slags: noget, man ved, for eksempel en adgangskode; noget, man har, for eksempel en telefon eller en sikkerhedsnøgle; og noget, man er, for eksempel et fingeraftryk. Definitionen hænger på ét ord. Systemet skal kræve mere end én forskellig type faktor, så en adgangskode og svaret på et sikkerhedsspørgsmål tæller tilsammen kun som én faktor, fordi begge er noget, man ved. Tofaktorgodkendelse, eller 2FA, er det almindelige tilfælde med præcis to.

Retningslinjen godtager to veje dertil. Den første kombinerer separate autentifikatorer med hver sin faktor: en adgangskode plus en telefonapp, der viser engangskoder, eller en liste med udskrevne backupkoder. Den anden bruger én autentifikator med flere faktorer, for eksempel en sikkerhedsnøgle eller en telefon, der opbevarer en privat nøgle og kun bruger den efter en pinkode eller et fingeraftryk. Her kalder NIST pinkoden eller fingeraftrykket en aktiveringsfaktor. Den kontrolleres på selve enheden, og serveren modtager kun resultatet, en signatur, den kan verificere, så én berøring præsenterer to faktorer.

Biometri har kun en snæver plads. NIST tillader et fingeraftryk eller et ansigt udelukkende som en del af multifaktorautentificering med en fysisk autentifikator, aldrig som en faktor for sig, og kræver, at der altid tilbydes et alternativ uden biometri. Retningslinjen siger ligeud, at biometriske kendetegn ikke er hemmelige: et ansigt kan fotograferes, og et fingeraftryk kan løftes fra noget, ejeren har rørt ved.

Brug begrebet i en beslutning

Brug »Hvad er multifaktorautentificering?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Konti, adgangskoder og rettigheder sat op, så folk har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har skrevet 1.000 RBAC-regler til Linux-servere — 1,000 adgangsregler skrevet for at lukke et sikkerhedshul

Har skrevet 1.000 RBAC-regler til Linux-servere Kontakt os →

Hvorfor det betyder noget

En adgangskode kan kopieres, uden at ejeren opdager det: tastet ind på en overbevisende kopi af en loginside, gættet eller genbrugt på et websted, hvis database senere bliver stjålet. MFA gør en kopieret adgangskode utilstrækkelig alene, fordi angriberen stadig mangler noget af en anden slags.

NIST gør det til grundkravet på sit andet sikringsniveau. På AAL2 skal autentificeringen bruge en autentifikator med flere faktorer eller en kombination af to faktorer, og kombinationen skal omfatte en fysisk autentifikator sammen med en adgangskode eller en biometrisk sammenligning. En verifikator på det niveau skal tilbyde mindst én phishing-resistent mulighed, og føderale myndigheder skal kræve phishing-resistent autentificering af deres ansatte, kontraktansatte og samarbejdspartnere.

Metoderne, der sælges under de samme tre bogstaver, adskiller sig mere fra hinanden, end MFA adskiller sig fra en adgangskode alene, og retningslinjen sorterer dem tydeligt:

- **Koder sendt som sms eller taleopkald** er den eneste type autentifikator, NIST betegner som begrænset. De må stadig bruges, men verifikatoren skal tilbyde et alternativ uden den betegnelse, fortælle brugeren om risikoen og have en plan for at komme væk fra metoden. At skifte det registrerede telefonnummer tæller som at binde en ny autentifikator, med alle de kontroller, det indebærer.
- **Koder fra en app og push-beskeder på en telefon** er acceptable på AAL2, men ikke phishing-resistente: det, personen taster eller godkender, er ikke knyttet til det websted, der bad om det.
- **Kryptografiske autentifikatorer, der binder deres svar til webstedet**, for eksempel passkeys og chipkort, er phishing-resistente. AAL3 kræver en, hvis private nøgle ikke kan eksporteres fra dens hardware.

E-mail mangler bevidst på listen: retningslinjen udelukker den som separat kanal ved såkaldt out-of-band-autentificering.

Sådan ser det ud i praksis

Koden i en autentificeringsapp er den mest udbredte anden faktor, og RFC 6238 (maj 2011) definerer den på få sider. Ved tilmeldingen genererer serveren en hemmelig nøgle og giver den til appen, som regel som en QR-kode, så begge sider nu har den samme nøgle. For at lave en kode dividerer hver side den aktuelle Unix-tid med et tidstrin, som standard 30 sekunder, og bruger heltallet som tæller. Derefter beregner den en HMAC af tælleren med nøglen og skærer resultatet ned til et kort decimaltal med metoden fra HOTP, som RFC 4226 definerede i 2005, og som kræver mindst seks cifre. I Python fylder hele beregningen få linjer:

```
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
```

RFC’ens testvektorer bruger den 20 byte lange ASCII-nøgle og otte cifre. Ved 59 sekunder efter Unix-epoken er tælleren 1, og SHA-1-varianten giver 94287082, som er det, funktionen udskriver; den sekscifrede kode, en app ville vise, er de sidste seks af de cifre, 287082. Intet i beregningen rører netværket. Derfor virker appen på en telefon i flytilstand, og derfor skal serveren også gemme sin egen kopi af hver brugers nøgle.

At kontrollere en kode er den samme beregning på serveren efterfulgt af en sammenligning. RFC 6238 anbefaler højst at godtage ét tidligere tidstrin for at dække forsinkelse på netværket og forbyder at godtage en kode igen, når den først er brugt med succes.

En passkey erstatter den fælles nøgle med et nøglepar. Under Web Authentication Level 3, en W3C-anbefaling siden 25. august 2026, opretter autentifikatoren et nøglepar til ét websted, identificeret ved dets domæne, og

giver kun serveren den offentlige nøgle. Ved login sender browseren den oprindelse med, som den faktisk er forbundet til, og autentifikatoren underskriver serverens udfordring sammen med den oprindelse, så en signatur lavet på et domæne, der ligner, er ubrugelig på det rigtige. Kræver nøglen en pinkode eller et fingeraftryk, er en passkey en autentifikator med flere faktorer i ét trin. WebAuthn kalder passkeys, der kopieres mellem en persons enheder, for multi-device credentials, og NIST godtager disse synkroniserede nøgler på AAL2, men ikke på AAL3, fordi en nøgle, der kan synkroniseres, pr. definition er en nøgle, der kan eksporteres.

At slå MFA til er den lette del. At beslutte, hvem der skal bruge det, hvilke metoder der gælder hvor, og hvad der sker, når nogen mister sin telefon, er kontoadministration og en del af den bredere tilrettelæggelse af adgang. Sidens ydelse for sikkerhed og adgangsstyring beskriver netop den tilrettelæggelse: konti, adgangskoder og rettigheder sat op, så hver person har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Hvor det går galt

En phishingside videresender koden. En engangskode er et tal, brugeren læser og taster, og intet i det registrerer, hvilket websted brugeren kiggede på. En kopiside, der sender adgangskoden og koden videre til det rigtige websted inden for tidstrinnet, logger ind som brugeren. NIST slår derfor fast, at ingen autentifikator, hvis output tastes ind manuelt, tæller som phishing-resistent, og tilføjer, at det er ligegyldigt, hvordan brugeren kom til den falske side. Løsningen er en autentifikator, der binder sit svar til verifikatoren: via domænenavnet, som WebAuthn gør, eller til selve TLS-forbindelsen, som klientcertifikater og chipkort gør. Kræv en af dem for administratorer, og tilbyd den til alle andre.

Telefonnummeret er faktoren. En kode sendt som sms går til den, som mobiloperatøren lige nu knytter nummeret til. NIST's egen liste over trusler omfatter en angriber, der har overtalt operatøren til at omdirigere offerets nummer og derefter modtager koden. Før en kode sendes som sms eller taleopkald, bør verifikatoren se efter tegn som et nyligt skift af SIM-kort, et nummer, der er flyttet til et andet selskab, eller en ny enhed. Behold sms som reserve frem for som hovedmetode, og kræv et fuldt login, før nummeret i systemet kan ændres.

Godkend, godkend, godkend. En push-besked med én knap, Godkend, beder om en beslutning, ikke om bevis. En angriber, der allerede har adgangskoden, kan udløse beskeder, indtil brugeren, træt af støjen, godkender en af dem. NIST kalder det autentificeringstræthed og anser ikke længere forløb, hvor man blot godkender, for acceptable: en hemmelig værdi skal overføres fra den ene kanal til den anden, for eksempel et tal på loginskærmen, som brugeren taster ind på telefonen. Det er ikke nok at vælge tallet fra en kort liste, for brugeren kan bare gætte. Begræns, hvor mange beskeder der kan sendes siden det seneste vellykkede login, som retningslinjen også anbefaler.

Gendannelsen springer den anden faktor over. Et link til »Jeg har mistet min telefon«, der kun spørger efter adgangskoden eller sender et nulstillingslink via e-mail, gør MFA til et tilvalg, som angriberen kan fravælge. For konti på AAL2 kræver NIST, at gendannelse sker med to gendannelseskoder modtaget ad forskellige veje, med én gendannelseskode plus en autentifikator med én faktor, der stadig er bundet til kontoen, eller ved at personens identitet kontrolleres forfra. Hver gendannelse skal udløse en notifikation til brugeren. Mere generelt må én faktor aldrig kunne bruges til at skaffe en autentifikator af en anden slags: en adgangskode alene må ikke være nok til at udskrive et nyt sæt backupkoder.

Koden godtages to gange eller for længe. En sekscifret kode har en million mulige værdier, så dens styrke kommer fra reglerne omkring den. En verifikator, der godtager flere tidstrin før og efter det aktuelle, eller som godtager en kode, der allerede er brugt, giver en angriber, der har set én kode, et vindue til at bruge den igen. Gem det seneste godkendte tidstrin for hver bruger, og afvis alt, der ligger på eller før det. Hold vinduet på det ene trin, RFC 6238 tillader for forsinkelse, og sæt et loft over antallet af mislykkede forsøg i træk: NIST tillader højst 100, før autentifikatoren deaktiveres.

Nøglerne ligger ved siden af adgangskoderne. Koder fra en app er symmetriske: serveren har hver brugers nøgle, og den, der kopierer de nøgler, kan lave gyldige koder til alle konti. NIST kræver, at nøglerne beskyttes stærkt, og at adgangen begrænses til de softwarekomponenter, der har brug for dem. Gem dem ikke som almindelige kolonner ved siden af hashværdierne af adgangskoderne. Kryptér dem med en nøgle, der ligger i et separat hemmelighedslager, og lad kun den tjeneste, der verificerer koder, læse dem.

Læs mere

- NIST SP 800-63B-4, Definitions and Acronyms — definitionerne af multifaktorautentificering, autentifikator med flere faktorer og phishing-resistens i den gældende retningslinje.
- NIST SP 800-63B-4 hos Computer Security Resource Center — publikationens stamdata: udgivet i juli 2025 som afløser for SP 800-63B.
- RFC 6238: TOTP — algoritmen for tidsbaserede engangskoder, dens testvektorer og reglerne for urforskydning.
- RFC 4226: HOTP — den tællerbaserede algoritme nedenunder, herunder afkortningen til seks eller flere cifre.
- Web Authentication, Level 3 — W3C's specifikation bag passkeys, med legitimationsoplysninger bundet til én oprindelse og synkroniserede passkeys.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er multifaktorautentificering?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/multi-factor-authentication/