Engineer

Flerfaktorautentisering

innlogging som krever to eller flere ulike typer bevis

Hva det er

Flerfaktorautentisering, ofte forkortet MFA, er en innlogging som godtar en påstått identitet bare når den støttes av mer enn én type bevis. NIST SP 800-63B-4, den amerikanske føderale retningslinjen for autentisering som mange virksomheter utenfor offentlig sektor også følger, nevner tre typer: noe du vet, for eksempel et passord; noe du har, for eksempel en telefon eller en sikkerhetsnøkkel; og noe du er, for eksempel et fingeravtrykk. Definisjonen henger på ett ord. Systemet må kreve mer enn én forskjellig type faktor, så et passord og svaret på et sikkerhetsspørsmål utgjør til sammen bare én faktor, fordi begge er noe du vet. Tofaktorautentisering, eller 2FA, er det vanlige tilfellet med nøyaktig to.

Retningslinjen godtar to veier dit. Den første kombinerer separate autentikatorer med én faktor hver: et passord pluss en app på telefonen som viser engangskoder, eller en liste med utskrevne reservekoder. Den andre bruker én autentikator med flere faktorer, for eksempel en sikkerhetsnøkkel eller en telefon som har en privat nøkkel og bare bruker den etter en PIN-kode eller et fingeravtrykk. Da kalles PIN-koden eller fingeravtrykket en aktiveringsfaktor. Den kontrolleres på selve enheten, og serveren mottar bare resultatet, en signatur den kan verifisere, så én berøring legger fram to faktorer.

Biometri har en smal plass her. NIST tillater fingeravtrykk eller ansikt bare som del av flerfaktorautentisering med en fysisk autentikator, aldri som en faktor alene, og krever at det alltid tilbys et alternativ uten biometri. Retningslinjen sier rett ut at biometriske kjennetegn ikke er hemmelige: et ansikt kan fotograferes, og et fingeravtrykk kan hentes fra noe eieren har tatt på.

Bruk begrepet i en beslutning

Bruk «Hva er flerfaktorautentisering?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Kontoer, passord og tilganger ordnet slik at folk har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Skrev 1 000 RBAC-regler for å sikre Linux-servere — 1,000 tilgangsregler skrevet for å tette et sikkerhetshull

Skrev 1 000 RBAC-regler for å sikre Linux-servere Ta kontakt →

Hvorfor det er viktig

Et passord kan kopieres uten at eieren merker det: det tastes inn på en overbevisende kopi av en innloggingsside, gjettes eller gjenbrukes på et nettsted der databasen senere blir stjålet. MFA gjør et kopiert passord utilstrekkelig alene, fordi angriperen fortsatt trenger noe av en annen type.

NIST gjør dette til grunnkravet på sitt andre sikkerhetsnivå. På AAL2 må autentiseringen bruke en autentikator med flere faktorer eller en kombinasjon av to faktorer, og kombinasjonen må inneholde en fysisk autentikator sammen med et passord eller en biometrisk sammenligning. Verifikatorer på dette nivået må tilby minst ett alternativ som er motstandsdyktig mot phishing, og føderale etater må kreve autentisering som er motstandsdyktig mot phishing, av sine ansatte, konsulenter og samarbeidspartnere.

Metodene som selges under de samme tre bokstavene, skiller seg mer fra hverandre enn MFA skiller seg fra et passord alene, og retningslinjen sorterer dem tydelig:

- **Koder sendt på SMS eller i taleanrop** er den eneste autentikatortypen NIST merker som begrenset. De kan fortsatt brukes, men verifikatoren må tilby et alternativ uten den merkelappen, fortelle brukeren om risikoen og ha en plan for å gå bort fra metoden. Å endre det registrerte telefonnummeret regnes som å binde en ny autentikator, med alle kontrollene det innebærer.
- **Koder fra en app og push-meldinger på telefonen** er godtatt på AAL2, men er ikke motstandsdyktige mot phishing: det personen taster inn eller godkjenner, er ikke knyttet til nettstedet som ba om det.
- **Kryptografiske autentikatorer som binder svaret til nettstedet**, som passnøkler og smartkort, er motstandsdyktige mot phishing. AAL3 krever en der den private nøkkelen ikke kan eksporteres fra maskinvaren.

E-post mangler på listen med vilje: retningslinjen utelukker den som kanal for autentisering utenfor hovedforbindelsen (out-of-band).

Slik ser det ut i praksis

Koden i en autentiseringsapp er den vanligste andre faktoren, og RFC 6238 (mai 2011) definerer den på noen få sider. Ved registreringen genererer serveren en hemmelig nøkkel og gir den til appen, vanligvis som en QR-kode, slik at begge sider nå har den samme nøkkelen. For å lage en kode deler hver side gjeldende Unix-tid på et tidssteg, 30 sekunder som standard, og bruker heltallet som teller. Deretter beregner den en HMAC av telleren med nøkkelen og kutter resultatet ned til et kort desimaltall med metoden fra HOTP, som RFC 4226 definerte i 2005, og som krever minst seks sifre. I Python får hele beregningen plass på noen 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
```

Testvektorene i RFC-en bruker denne 20 byte lange ASCII-nøkkelen og åtte sifre. 59 sekunder etter Unix-epoken er telleren 1, og SHA-1-varianten gir 94287082, som er det funksjonen skriver ut; den sekssifrede koden en app ville vist, er de seks siste sifrene, 287082. Beregningen bruker ikke nettverket i det hele tatt, og derfor fungerer appen på en telefon i flymodus. Av samme grunn må serveren ha sin egen kopi av hver brukers nøkkel.

Å kontrollere en kode er den samme beregningen på serveren, fulgt av en sammenligning. RFC 6238 anbefaler å godta høyst ett tidligere tidssteg for å dekke forsinkelse i nettverket, og forbyr å godta en kode en gang til etter at den er brukt.

En passnøkkel erstatter den delte nøkkelen med et nøkkelpar. I Web Authentication Level 3, som har vært en W3C-anbefaling siden 25. august 2026, lager autentikatoren et nøkkelpar for ett nettsted, identifisert ved domenet, og

gir serveren bare den offentlige nøkkelen. Ved innlogging sender nettleseren med opprinnelsen (origin) den faktisk er koblet til, og autentikatoren signerer serverens utfordring sammen med den opprinnelsen, så en signatur laget på et domene som ligner, er verdiløs på det ekte. Når det kreves en PIN-kode eller et fingeravtrykk for å bruke nøkkelen, er en passnøkkel en autentikator med flere faktorer i ett enkelt steg. WebAuthn kaller passnøkler som kopieres mellom en persons enheter, multi-device credentials, og NIST godtar slike synkroniserte nøkler på AAL2, men ikke på AAL3, fordi en nøkkel som kan synkroniseres, per definisjon er en nøkkel som kan eksporteres.

Å slå på MFA er den enkle delen. Å bestemme hvem som må bruke den, hvilke metoder som gjelder hvor, og hva som skjer når noen mister telefonen, er kontoadministrasjon, en del av den bredere organiseringen av tilgang. Tjenesten for sikkerhet og tilgangsstyring på dette nettstedet beskriver nettopp den organiseringen: kontoer, passord og tilganger ordnet slik at hver person har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Hvor det går galt

En phishingside videresender koden. En engangskode er et tall som brukeren leser og taster inn, og koden bærer ingen opplysning om hvilket nettsted brukeren så på. En side som ligner, og som videresender passordet og koden til det ekte nettstedet innenfor tidssteget, logger inn som brukeren. NIST slår derfor fast at en autentikator der utdataene tastes inn for hånd, aldri regnes som motstandsdyktig mot phishing, og legger til at det er uten betydning hvordan brukeren havnet på den falske siden. Løsningen er en autentikator som binder svaret til verifikatoren: via domenenavnet, slik WebAuthn gjør, eller til selve TLS-kanalen, slik klientsertifikater og smartkort gjør. Krev en slik for administratorer, og tilby den til alle andre.

Telefonnummeret blir faktoren. En kode sendt på SMS går til den mobiloperatøren for øyeblikket ruter nummeret til. NISTs egen liste over trusler omfatter en angriper som har overtalt operatøren til å omdirigere offerets nummer og deretter mottar koden. Før en kode sendes på SMS eller i taleanrop, bør verifikatoren se etter tegn som et nylig bytte av SIM-kort, portering av nummeret eller bytte av enhet. Behold SMS som reserveløsning, ikke som hovedmetode, og krev full innlogging før nummeret på kontoen kan endres.

Godkjenn, godkjenn, godkjenn. En push-melding med én godkjenningsknapp ber om en avgjørelse, ikke om bevis. En angriper som allerede har passordet, kan sende meldinger helt til brukeren, lei av støyen, godtar én av dem. NIST kaller dette autentiseringstretthet og godtar ikke lenger løsninger der det er nok å trykke på godkjenn: en hemmelig verdi må gå fra den ene kanalen til den andre, for eksempel et tall på innloggingsskjermen som brukeren taster inn på telefonen. Å velge tallet fra en kort liste er ikke nok, siden brukeren kan gjette. Begrens hvor mange meldinger som kan sendes etter siste vellykkede innlogging, slik retningslinjen også anbefaler.

Gjenopprettingen hopper over den andre faktoren. En lenke av typen «Mistet telefonen?» som bare ber om passordet, eller som sender en tilbakestillingslenke på e-post, gjør MFA til et valg angriperen kan takke nei til. For kontoer på AAL2 krever NIST at gjenoppretting bruker to gjenopprettingskoder mottatt på forskjellige måter, én gjenopprettingskode pluss en autentikator med én faktor som fortsatt er bundet til kontoen, eller en ny kontroll av identiteten. Hver gjenoppretting skal utløse en melding til brukeren. Mer generelt skal én faktor aldri kunne brukes til å skaffe en autentikator av en annen type: et passord alene skal ikke være nok til å skrive ut et nytt sett reservekoder.

Koden godtas to ganger, eller for lenge. En sekssifret kode har en million mulige verdier, så styrken kommer fra reglene rundt den. En verifikator som godtar flere tidssteg før og etter det gjeldende, eller som godtar en kode som allerede er brukt, gir en angriper som har sett én kode, et vindu der den kan brukes igjen. Lagre det siste godtatte tidssteget for hver bruker, og avvis alt som faller på eller før det. Hold vinduet til det ene steget RFC 6238 tillater for forsinkelse, og begrens antall mislykkede forsøk på rad: NIST tillater høyst 100 før autentikatoren deaktiveres.

Nøklene ligger ved siden av passordene. Koder fra en app er symmetriske: serveren har hver brukers nøkkel, og den som kopierer disse nøklene, kan lage gyldige koder for hver eneste konto. NIST krever at nøklene beskyttes godt, og at tilgangen begrenses til programvarekomponentene som trenger dem. Ikke lagre dem som vanlige kolonner ved siden av passordhashene. Krypter dem med en nøkkel som ligger i et eget hemmelighetslager, og la bare tjenesten som verifiserer kodene, lese dem.

Les mer

- NIST SP 800-63B-4, Definitions and Acronyms — definisjonene av flerfaktorautentisering, autentikator med flere faktorer og motstandsdyktighet mot phishing i den gjeldende retningslinjen.
- NIST SP 800-63B-4 hos Computer Security Resource Center — publikasjonsoppføringen: utgitt i juli 2025 og erstatter SP 800-63B.
- RFC 6238: TOTP — algoritmen for tidsbaserte engangspassord, testvektorene og reglene for klokkeavvik.
- RFC 4226: HOTP — den tellerbaserte algoritmen som TOTP bygger på, inkludert avkortingen til seks eller flere sifre.
- Web Authentication, Level 3 — W3C-spesifikasjonen bak passnøkler, med nøkler knyttet til opprinnelsen og synkroniserte passnøkler.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er flerfaktorautentisering?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/multi-factor-authentication/