Engineer

Multifaktorautentisering

inloggning som kräver två eller fler olika slags bevis

Vad det är

Multifaktorautentisering, ofta förkortat MFA, är en inloggning som godtar en uppgiven identitet bara när den styrks av mer än ett slags bevis. NIST SP 800-63B-4, den amerikanska federala riktlinjen för autentisering som många organisationer utanför den offentliga sektorn också följer, nämner tre slag: något du vet, till exempel ett lösenord; något du har, till exempel en telefon eller en säkerhetsnyckel; och något du är, till exempel ett fingeravtryck. Definitionen hänger på ett enda ord. Systemet måste kräva mer än en distinkt typ av faktor, så ett lösenord och svaret på en säkerhetsfråga blir tillsammans bara en faktor, eftersom båda är något du vet. Tvåfaktorsautentisering, eller 2FA, är det vanliga fallet med exakt två.

Riktlinjen godtar två vägar dit. Den första kombinerar separata autentiserare med en faktor var: ett lösenord plus en app i telefonen som visar engångskoder, eller en lista med utskrivna reservkoder. Den andra använder en autentiserare med flera faktorer, till exempel en säkerhetsnyckel eller en telefon som har en privat nyckel och bara använder den efter en PIN-kod eller ett fingeravtryck. Då kallas PIN-koden eller fingeravtrycket en aktiveringsfaktor. Den kontrolleras på själva enheten, och servern får bara resultatet, en signatur som den kan verifiera, så en enda beröring visar upp två faktorer.

Biometri har en snäv plats i det här. NIST tillåter fingeravtryck eller ansikte bara som en del av multifaktorautentisering med en fysisk autentiserare, aldrig som en faktor på egen hand, och kräver att ett alternativ utan biometri alltid erbjuds. Riktlinjen säger rakt ut att biometriska kännetecken inte är hemliga: ett ansikte kan fotograferas, och ett fingeravtryck kan säkras från något som ägaren har rört vid.

Använd begreppet i ett beslut

Använd ”Vad är multifaktorautentisering?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

Skrev 1 000 RBAC-regler som säkrar Linux-servrar Hör av er →

Varför det spelar roll

Ett lösenord kan kopieras utan att ägaren märker det: det skrivs in på en övertygande kopia av en inloggningssida, gissas eller återanvänds på en webbplats vars databas senare blir stulen. MFA gör ett kopierat lösenord otillräckligt på egen hand, eftersom angriparen fortfarande behöver något av ett annat slag.

NIST gör detta till grundkravet på sin andra tillitsnivå. På AAL2 måste autentiseringen använda en autentiserare med flera faktorer eller en kombination av två faktorer, och kombinationen måste innehålla en fysisk autentiserare tillsammans med ett lösenord eller en biometrisk jämförelse. Verifierare på den nivån måste erbjuda minst ett nätfiskeresistent alternativ, och federala myndigheter måste kräva nätfiskeresistent autentisering av sina anställda, konsulter och samarbetspartner.

Metoderna som säljs under samma tre bokstäver skiljer sig mer från varandra än MFA skiljer sig från enbart ett lösenord, och riktlinjen sorterar dem tydligt:

- **Koder som skickas via sms eller röstsamtal** är den enda typ av autentiserare som NIST märker som begränsad. De får fortfarande användas, men verifieraren måste erbjuda ett alternativ utan den märkningen, berätta för användaren om risken och ha en plan för att gå ifrån metoden. Att byta det registrerade telefonnumret räknas som att binda en ny autentiserare, med alla kontroller som det innebär.
- **Koder från en app och push-notiser i telefonen** godtas på AAL2 men är inte nätfiskeresistenta: det som personen skriver in eller godkänner är inte knutet till webbplatsen som bad om det.
- **Kryptografiska autentiserare som binder sitt svar till webbplatsen**, som passkeys och smartkort, är nätfiskeresistenta. AAL3 kräver en vars privata nyckel inte kan exporteras från hårdvaran.

E-post saknas i listan med flit: riktlinjen utesluter den som kanal för autentisering utanför huvudförbindelsen (out-of-band).

Så ser det ut i praktiken

Koden i en autentiseringsapp är den vanligaste andra faktorn, och RFC 6238 (maj 2011) definierar den på några få sidor. Vid registreringen genererar servern en hemlig nyckel och lämnar över den till appen, oftast som en QR-kod, så att båda sidor nu har samma nyckel. För att ta fram en kod delar varje sida aktuell Unix-tid med ett tidssteg, som standard 30 sekunder, och använder heltalet som räknare. Sedan beräknar den en HMAC av räknaren med nyckeln och kortar ned resultatet till ett kort decimaltal med metoden från HOTP, som RFC 4226 definierade 2005 och som kräver minst sex siffror. I Python får hela beräkningen plats på några rader:

```
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
```

Testvektorerna i RFC:n använder den här 20 byte långa ASCII-nyckeln och åtta siffror. 59 sekunder efter Unix-epoken är räknaren 1, och SHA-1-varianten ger 94287082, vilket är vad funktionen skriver ut; den sexsiffriga kod som en app skulle visa är de sex sista siffrorna, 287082. Beräkningen använder inte nätverket alls, och därför fungerar appen i en telefon i flygplansläge. Av samma skäl måste servern ha en egen kopia av varje användares nyckel.

Att kontrollera en kod är samma beräkning på servern, följd av en jämförelse. RFC 6238 rekommenderar att högst ett tidigare tidssteg godtas för att täcka fördröjning i nätverket, och förbjuder att en kod godtas en andra gång när den väl har använts.

En passkey ersätter den delade nyckeln med ett nyckelpar. I Web Authentication Level 3, som är en W3C-rekommendation sedan den 25 augusti 2026, skapar autentiseraren ett nyckelpar för en webbplats, identifierad genom sin domän,

och ger servern bara den publika nyckeln. Vid inloggning skickar webbläsaren med det ursprung (origin) som den faktiskt är ansluten till, och autentiseraren signerar serverns utmaning tillsammans med det ursprunget, så en signatur som skapats på en domän som liknar den äkta är värdelös hos den äkta. När en PIN-kod eller ett fingeravtryck krävs för att använda nyckeln är en passkey en autentiserare med flera faktorer i ett enda steg. WebAuthn kallar passkeys som kopieras mellan en persons enheter för multi-device credentials, och NIST godtar sådana synkroniserade nycklar på AAL2 men inte på AAL3, eftersom en nyckel som kan synkroniseras per definition är en nyckel som kan exporteras.

Att slå på MFA är den enkla delen. Att bestämma vem som måste använda den, vilka metoder som räknas var och vad som händer när någon tappar bort sin telefon är kontoadministration, en del av den bredare organisationen av åtkomst. Tjänsten för säkerhet och behörighetshantering på den här webbplatsen beskriver just den organisationen: konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

Var det går fel

En nätfiskesida vidarebefordrar koden. En engångskod är ett tal som användaren läser och skriver in, och koden bär ingen uppgift om vilken webbplats användaren tittade på. En sida som liknar den äkta, och som vidarebefordrar lösenordet och koden till den äkta webbplatsen inom tidssteget, loggar in som användaren. NIST slår därför fast att en autentiserare vars utdata skrivs in för hand aldrig räknas som nätfiskeresistent, och tillägger att det saknar betydelse hur användaren hamnade på den falska sidan. Lösningen är en autentiserare som binder sitt svar till verifieraren: via domännamnet, som WebAuthn gör, eller till själva TLS-kanalen, som klientcertifikat och smartkort gör. Kräv en sådan för administratörer och erbjud den till alla andra.

Telefonnumret blir faktorn. En kod som skickas via sms går till den som mobiloperatören för tillfället kopplar numret till. NIST:s egen lista över hot tar upp en angripare som har övertalat operatören att styra om offrets nummer och sedan tar emot koden. Innan en kod skickas via sms eller röstsamtal bör verifieraren leta efter tecken som ett nyligen bytt SIM-kort, flytt av numret till en annan operatör eller byte av enhet. Behåll sms som reservlösning och inte som huvudmetod, och kräv en fullständig inloggning innan numret på kontot kan ändras.

Godkänn, godkänn, godkänn. En push-notis med en enda godkännandeknapp ber om ett beslut, inte om bevis. En angripare som redan har lösenordet kan skicka notiser tills användaren, trött på bruset, godkänner en av dem. NIST kallar detta autentiseringströtthet och godtar inte längre lösningar där det räcker att trycka på godkänn: ett hemligt värde måste gå från den ena kanalen till den andra, till exempel ett tal på inloggningsskärmen som användaren skriver in i telefonen. Att välja talet ur en kort lista räcker inte, eftersom användaren kan gissa. Begränsa hur många notiser som kan skickas efter den senaste lyckade inloggningen, som riktlinjen också rekommenderar.

Återställningen hoppar över den andra faktorn. En länk av typen ”Har du tappat bort telefonen?” som bara ber om lösenordet, eller som skickar en återställningslänk via e-post, gör MFA till ett val som angriparen kan tacka nej till. För konton på AAL2 kräver NIST att återställningen använder två återställningskoder som tagits emot på olika sätt, en återställningskod plus en autentiserare med en faktor som fortfarande är bunden till kontot, eller en ny kontroll av identiteten. Varje återställning ska leda till ett meddelande till användaren. Mer allmänt får en faktor aldrig kunna användas för att skaffa en autentiserare av ett annat slag: enbart ett lösenord får inte räcka för att skriva ut en ny uppsättning reservkoder.

Koden godtas två gånger, eller för länge. En sexsiffrig kod har en miljon möjliga värden, så dess styrka kommer från reglerna runt den. En verifierare som godtar flera tidssteg före och efter det aktuella, eller som godtar en kod som redan har använts, ger en angripare som har sett en kod ett fönster för att använda den igen. Spara det senast godtagna tidssteget för varje användare och avvisa allt som infaller på eller före det. Håll fönstret till det enda steg som RFC 6238 tillåter för fördröjning, och begränsa antalet misslyckade försök i rad: NIST tillåter högst 100 innan autentiseraren inaktiveras.

Nycklarna ligger bredvid lösenorden. Koder från en app är symmetriska: servern har varje användares nyckel, och den som kopierar de nycklarna kan skapa giltiga koder för vilket konto som helst. NIST kräver att nycklarna skyddas väl och att åtkomsten begränsas till de programkomponenter som behöver dem. Lagra dem inte som vanliga kolumner bredvid lösenordens hashvärden. Kryptera dem med en nyckel som förvaras i ett separat hemlighetslager, och låt bara tjänsten som verifierar koderna läsa dem.

Läs mer

- NIST SP 800-63B-4, Definitions and Acronyms — definitionerna av multifaktorautentisering, autentiserare med flera faktorer och nätfiskeresistens i den gällande riktlinjen.
- NIST SP 800-63B-4 hos Computer Security Resource Center — publikationsposten: utgiven i juli 2025 och ersätter SP 800-63B.
- RFC 6238: TOTP — algoritmen för tidsbaserade engångslösenord, testvektorerna och reglerna för klockavvikelse.
- RFC 4226: HOTP — den räknarbaserade algoritmen som TOTP bygger på, inklusive avkortningen till sex eller fler siffror.
- Web Authentication, Level 3 — W3C-specifikationen bakom passkeys, med nycklar knutna till ursprunget och synkroniserade passkeys.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är multifaktorautentisering?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/multi-factor-authentication/