GIDS

De complete gids voor multi-factor authenticatie

Methoden, kosten, NIS2-verplichting, implementatie, veelgemaakte fouten en de toekomst van authenticatie. Met actuele Nederlandse marktdata.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

MFA is de meest effectieve basismaatregel tegen cyberaanvallen. De cijfers bewijzen het.

99,9%
van gecompromitteerde accounts had geen MFA ingeschakeld
Microsoft [1]

61%
van Nederlandse bedrijven (2+ pers.) gebruikt tweefactorauthenticatie (was 26% in 2017)
CBS Cybersecuritymonitor 2024 [2]

203%
ROI over 3 jaar bij inzet van FIDO2 security keys
Forrester TEI / Yubico [3]

USD 4,8M
Gemiddelde kosten per datalek via gestolen credentials
IBM Security 2024 [4]

97%
van grote bedrijven (250+ pers.) gebruikt tweefactorauthenticatie
CBS 2024 [2]

3× sneller
Inloggen met passkeys vergeleken met traditionele wachtwoorden
FIDO Alliance [5]

39%
van Nederlandse bedrijven heeft nog geen MFA -- een grote kwetsbaarheid
CBS 2024 [2]

NIS2
MFA is een expliciete wettelijke verplichting onder artikel 21.2(j) van de NIS2-richtlijn
NIS2 art. 21 [6]

1. Wat is multi-factor authenticatie?

MFA voegt extra verificatielagen toe aan het inlogproces, zodat een gestolen wachtwoord alleen niet genoeg is om toegang te krijgen.

Multi-factor authenticatie (MFA) combineert twee of meer onafhankelijke verificatiemethoden uit verschillende categorieen. Tweefactorauthenticatie (2FA) is een specifieke vorm van MFA die precies twee factoren gebruikt [7].

DE DRIE FACTORCATEGORIEEN

- **Iets dat je weet** -- Wachtwoord, pincode, beveiligingsvraag
- **Iets dat je hebt** -- Smartphone, hardware token, smart card
- **Iets dat je bent** -- Vingerafdruk, gezichtsherkenning, irisscan

Het principe is eenvoudig: als een aanvaller je wachtwoord steelt (iets dat je weet), heeft die nog steeds je telefoon (iets dat je hebt) of je vingerafdruk (iets dat je bent) nodig. Elke extra factor maakt een succesvolle aanval exponentieel moeilijker.

> **Waarom wachtwoorden alleen niet genoeg zijn**
>
> 99,9% van gecompromitteerde accounts had geen MFA [1]. Over het afgelopen decennium was 31% van alle datalekken gerelateerd aan gestolen credentials [8]. Wachtwoorden worden hergebruikt, gelekt in breaches en geraden via brute force. MFA maakt deze aanvalsroute grotendeels onbruikbaar.

2. MFA-methoden vergeleken

Niet alle MFA is gelijk. De keuze van methode bepaalt je veiligheidsniveau, gebruikservaring en kosten.

METHODE	VEILIGHEID	GEBRUIKSGEMAK	KOSTEN	PHISHING-RESISTANT
SMS OTP	Laag	Hoog	EUR 0,05--0,15/ SMS	Nee
Email OTP	Laag	Hoog	Gratis	Nee
TOTP (authenticator-app)	Gemiddeld	Gemiddeld	Gratis--EUR 3/ mnd	Nee
Push notification	Gemiddeld	Hoog	EUR 3--10/mnd	Nee
Push + number matching	Hoog	Hoog	EUR 5--15/mnd	Gedeeltelijk
FIDO2 / passkeys	Zeer hoog	Zeer hoog	EUR 20--80 eenmalig	Ja
Biometrie (device)	Hoog	Zeer hoog	Ingebouwd	Ja
Smart card / PKI	Zeer hoog	Gemiddeld	EUR 30--100 eenmalig	Ja

SMS IS NIET VEILIG GENOEG

SMS-based MFA is kwetsbaar voor SIM-swapping, onderschepping en SS7-aanvallen. Het is beter dan niets, maar niet geschikt als enige MFA-methode voor gevoelige systemen. Het NCSC adviseert om over te stappen naar authenticator-apps of FIDO2 [9].

AANBEVELING PER RISICOPROFIEL

RISICOPROFIEL	AANBEVOLEN MFA	TOELICHTING
Basis (laag risico)	Authenticator-app (TOTP)	Gratis, redelijke beveiliging, breed ondersteund

RISICOPROFIEL	AANBEVOLEN MFA	TOELICHTING
Standaard (gemiddeld risico)	Push + number matching	Goede balans tussen veiligheid en gebruiksgemak
Hoog risico / NIS2	FIDO2 passkeys / security keys	Phishing-resistant, voldoet aan strengste eisen
Zeer hoog / financieel	FIDO2 + biometrie + continuous auth	Maximale bescherming voor kritieke systemen

3. MFA in Nederland: de stand van zaken

Het gebruik van tweefactorauthenticatie is verdubbeld sinds 2017, maar 39% van de bedrijven heeft nog steeds geen MFA.

ADOPTIE PER BEDRIJFSGROOTTE

BEDRIJFSGROOTTE	2017	2024	GROEI
Alle bedrijven (2+ pers.)	26%	61%	+135%
Micro (2–10 pers.)	~20%	57%	+185%
Klein (10–50 pers.)	29%	76%	+162%
Middelgroot (50–250 pers.)	~50%	~88%	+76%
Groot (250+ pers.)	71%	97%	+37%

ADOPTIE PER SECTOR

SECTOR	2FA-GEBRUIK (2024)
Informatie en communicatie	88%
Financiele dienstverlening	83%
Gezondheids- en welzijnszorg	80%
Industrie	~65%
Bouwnijverheid	~55%
Horeca	44% (sterkste groei: van 16% in 2017)

TIP

Check of MFA is ingeschakeld voor alle accounts in je organisatie, niet alleen voor email. Cloudapplicaties, VPN, remote desktop en beheerderstoegang zijn minstens zo belangrijk -- en worden vaker vergeten.

4. Wat kost MFA?

MFA hoeft bijna niets te kosten. Een gratis authenticator-app beschermt al 99,9% van de aanvallen. Maar er zijn ook geavanceerdere opties.

OPLOSSING	KOSTEN PER GEBRUIKER/MAAND	JAARLIJKS (50 GEBRUIKERS)
Authenticator-app (gratis)	EUR 0	EUR 0 (alleen implementatietijd)
Authenticator-app (managed)	EUR 1--3	EUR 600--1.800
Cloud MFA (standaard)	EUR 3--10	EUR 1.800--6.000
Cloud MFA (geavanceerd)	EUR 10--25	EUR 6.000--15.000
Hardware tokens (FIDO2)	EUR 20--80 eenmalig + EUR 2--5/mnd	EUR 2.200--5.000 eenmalig
Enterprise MFA-platform	EUR 25--50+	EUR 15.000--30.000+

VERBORGEN KOSTEN OM REKENING MEE TE HOUDEN

- **Implementatie:** EUR 1.000--15.000 afhankelijk van complexiteit en integraties
- **Training:** EUR 500--3.000 voor gebruikers en helpdesk
- **SMS-kosten:** EUR 0,05--0,15 per OTP als je SMS-based MFA gebruikt
- **Helpdesk-belasting:** 20--30% meer tickets in de eerste maand na uitrol
- **Token-vervanging:** EUR 20--80 per verloren of defect hardware token

> **MKB-rekenvoorbeeld**
>
> 50 medewerkers met managed authenticator-app (EUR 3/user/maand): EUR 1.800/jaar. Implementatie eenmalig EUR 2.000, training EUR 500. Totaal jaar 1: EUR 4.300. Vanaf jaar 2: EUR 1.800. Dat is EUR 3 per medewerker per maand voor bescherming die 99,9% van credential-aanvallen blokkeert.

5. MFA en NIS2: wettelijke verplichting

MFA is een expliciete verplichting onder NIS2. Niet "nice to have" maar "must have" -- met boetes tot EUR 10 miljoen bij niet-naleving.

Artikel 21, sectie 2(j) van de NIS2-richtlijn schrijft voor [6]:

> **NIS2 ARTIKEL 21.2(J)**
>
> "Het gebruik van multi-factor authenticatie of continue authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit, waar passend."

De clausule "waar passend" betekent niet dat MFA optioneel is. Je moet aantonen dat je je identiteitsaanvalsoppervlak grondig hebt beoordeeld. MFA is vereist overal waar gebrek aan MFA-bescherming zou kunnen resulteren in een cyberaanval. In de praktijk betekent dit: overal [10].

MFA IN HET BREDERE NIS2-KADER

NIS2-MAATREGEL	MFA-ROL
Toegangsbeleid (art. 21.2.i)	MFA als verplicht onderdeel van toegangscontrole
Cyberhygiene (art. 21.2.g)	MFA als basispraktijk voor alle medewerkers
Ketenbescherming (art. 21.2.d)	MFA voor externe toegang van leveranciers
Incidentpreventie	MFA voorkomt 99,9% van credential-based aanvallen
Compliance-bewijs	MFA-logboeken als aantoonbare maatregel bij audit

6. Het implementatietraject

MFA uitrollen kost 2--6 weken voor een gemiddeld MKB-bedrijf. Zo doe je het goed.

1

Inventarisatie

WEEK 1

Breng alle applicaties en systemen in kaart die MFA nodig hebben: email, cloud-apps, VPN, remote desktop, beheerderstoegang, CRM, ERP.

2

Methode kiezen

WEEK 1--2

Kies de MFA-methode die past bij je risicoprofiel en gebruikers. Bied altijd een backup-methode aan voor als de primaire niet werkt.

3

Pilot met IT-team

WEEK 2--3

Begin met je IT-beheerders en powerusers. Los problemen op voordat je breder uitrolt. Test alle applicaties en scenario's.

4

Communicatie en training

WEEK 3--4

Informeer alle medewerkers: waarom MFA, hoe het werkt, wat ze moeten doen. Maak korte instructievideo's en een FAQ. Zet ambassadeurs in per afdeling.

5

Gefaseerde uitrol

WEEK 4--6

Rol uit per afdeling of per applicatie. Begin met de meest kritieke systemen. Bied extra helpdesk-ondersteuning in de eerste week.

6

Monitoring en bijsturing

DOORLOPEND

Monitor adoptie, verzamel feedback, los problemen op. Check of alle accounts daadwerkelijk MFA hebben -- niet alleen de accounts die het makkelijk was.

7. Veelgemaakte fouten

MFA-implementatie gaat vaker fout op menselijke dan op technische aspecten. Deze fouten kun je vermijden.

#	FOUT	WAAROM HET FOUT GAAT
1	**SMS als enige factor**	Kwetsbaar voor SIM-swap en onderschepping. Gebruik authenticator-apps of FIDO2 [9]
2	**Niet alle accounts beschermd**	Admin-accounts zonder MFA zijn de eerste die worden aangevallen. Begin juist daar
3	**Gebruikersweerstand negeren**	Zonder communicatie en training omzeilen medewerkers MFA of zetten het uit
4	**Geen backup-methoden**	Telefoon kwijt = uitgesloten van alle systemen. Altijd backup-codes of alternatieve methoden
5	**Legacy applicaties overslaan**	Oudere systemen die geen MFA ondersteunen worden de zwakste schakel
6	**MFA fatigue negeren**	Gebruikers die push-notificaties blind accepteren. Gebruik number matching
7	**Geen monitoring**	Aanvallen op MFA (brute force, fatigue) blijven onopgemerkt zonder logging
8	**Alleen bij inloggen**	MFA bij login maar niet bij gevoelige acties (data-export, configuratiewijziging) is onvolledig
9	**Persoonlijke devices verplichten**	Privacy-bezwaren en niet iedereen heeft een smartphone. Bied alternatieven
10	**Denken dat MFA genoeg is**	MFA is een basislaag, geen complete beveiliging. Combineer met andere maatregelen

8. Aanvallen op MFA en verdediging

MFA is niet onkraakbaar. Aanvallers ontwikkelen steeds slimmere methoden om MFA te omzeilen. Ken de risico's.

AANVALSTECHNIEK	HOE HET WERKT	KWETSBARE METHODEN	VERDEDIGING
Phishing (AitM)	Adversary-in-the-middle vangt sessie-token na MFA	SMS, TOTP, push	FIDO2 passkeys
SIM-swapping	Telefoonnummer overnemen bij provider	SMS-based MFA	App of hardware token
MFA fatigue	Massale push-verzoeken tot gebruiker accepteert	Push notifications	Number matching, rate limiting
Helpdesk social engineering	Helpdesk overtuigen om MFA te resetten	Alle methoden	Strikte verificatieprocedures
Session hijacking	Na succesvolle MFA sessie-cookie stelen	Alle methoden	Token binding, continuous auth

In Q1 2024 betrof 50% van alle incident responses van Cisco Talos een MFA-bypass aanval [11]. Dit onderstreept dat MFA-methoden niet allemaal gelijk zijn: phishing-resistant MFA (FIDO2, passkeys) is de standaard waar je naartoe moet werken.

TIP

Elke MFA is beter dan geen MFA. Start met wat haalbaar is (authenticator-app) en werk toe naar phishing-resistant methoden (FIDO2/passkeys) voor je meest kritieke accounts en gebruikers.

9. ROI en business case

MFA is een van de weinige security-investeringen die zich binnen maanden terugverdient. De cijfers spreken voor zich.

EFFECTIVITEIT

INDICATOR	WAARDE
Gecompromitteerde accounts zonder MFA	99,9%
Phishing/credential theft reductie (FIDO2)	99,9%
Helpdesk-tickets reductie (passkeys)	-75%
ROI over 3 jaar (FIDO2 keys)	203%
Password reset tickets reductie	-32%

KOSTENVERMIJDING

SCENARIO	VERMEDEN KOSTEN
Voorkomen credential breach	USD 4,8 miljoen gemiddeld
Voorkomen ransomware (MKB)	EUR 270.000 gemiddeld
NIS2-boetevermijding	Tot EUR 10.000.000
Lagere cyberverzekeringspremie	5--15% korting
Helpdesk-kostenreductie	EUR 5.000--15.000/jaar

De eenvoudigste rekensom in cybersecurity

MFA kost EUR 0--3 per medewerker per maand. Het voorkomt 99,9% van credential-based aanvallen. De gemiddelde schade van zo'n aanval is EUR 270.000 voor MKB. De terugverdientijd is minder dan 4 maanden. Er is geen security-investering met een betere verhouding tussen kosten en effect.

10. Trends 2025--2026: passkeys en passwordless

De toekomst van authenticatie is zonder wachtwoorden. Passkeys zijn de grootste verschuiving in jaren.

PASSKEYS: DE NIEUWE STANDAARD

Passkeys zijn gebaseerd op FIDO2 en WebAuthn standaarden. Ze gebruiken cryptografische sleutels op je device in plaats van wachtwoorden. Ze kunnen niet gephisht, gestolen of hergebruikt worden [5].

INDICATOR	WAARDE
Consumenten met passkey-awareness (2025)	74%
Consumenten met minstens 1 passkey	69%
Top-100 websites met passkey-support	48%
Login-snelheid vs wachtwoord	3x sneller
Login-snelheid vs wachtwoord + legacy MFA	8x sneller

REGULERINGSDRUK

- **NIS2:** MFA verplicht onder artikel 21.2(j) -- inwerkingtreding Q2 2026
- **DORA:** Sterke authenticatie verplicht voor financiele sector -- van kracht januari 2025
- **NIST SP 800-63-4:** Phishing-resistant optie verplicht bij AAL2 -- juli 2025
- **EU Digital Identity Wallet:** Digitale identiteit met sterke authenticatie -- eind 2026

WAT DIT VOOR JOU BETEKENT

ACTIEPLAN VOOR 2026

- Als je nog geen MFA hebt: begin vandaag met authenticator-apps. Het kost niets
- Als je SMS-based MFA hebt: plan migratie naar app-based of FIDO2
- Als je app-based MFA hebt: evalueer passkeys/FIDO2 voor je meest kritieke accounts
- Val je onder NIS2? MFA is verplicht. Documenteer je implementatie als compliance-bewijs
- Vraag je cyberverzekering: MFA is steeds vaker een acceptatie-eis

Onafhankelijk vergelijken?

Op ibgids.nl/word-gematcht vind je een gratis matchingtool die je koppelt aan MFA-specialisten die passen bij jouw situatie, omgeving en budget. Onafhankelijk, zonder verplichtingen.

Bronnenlijst

[1] **Microsoft** -- Security at your organization: MFA statistics. https://learn.microsoft.com/en-us/partner-center/security/security-at-your-organization

[2] **CBS** -- Gebruik van tweestapsverificatie verdubbeld sinds 2017. https://www.cbs.nl/nl-nl/nieuws/2025/25/gebruik-van-tweestapsverificatie-verdubbeld-sinds-2017

[3] **Forrester TEI / Yubico** -- Total Economic Impact of YubiKeys. https://www.yubico.com/solutions/multi-factor-authentication/

[4] **IBM Security** -- Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

[5] **FIDO Alliance** -- World Passkey Day 2025. https://fidoalliance.org/fido-alliance-champions-widespread-passkey-adoption-and-a-passwordless-future-on-world-passkey-day-2025/

[6] **Digital Trust Center** -- Gebruik MFA en andere beveiligde communicatie (NIS2). https://www.digitaltrustcenter.nl/nis2/mfa

[7] **CertificeringsAdvies Nederland** -- 2-factor en multifactor authenticatie en NIS2. https://certificeringsadvies.nl/2-factor-en-multifactor-authenticatie/

[8] **Verizon** -- 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[9] **NCSC** -- Hoe kies je een MFA methode? https://www.ncsc.nl/multifactor-authenticatie/hoe-kies-je-een-mfa-methode

[10] **Silverfort** -- How to Comply with NIS2 Directive MFA Requirements. https://www.silverfort.com/blog/comply-with-nis2-directive-mfa-requirements-with-silverfort/

[11] **NoorStream** -- Real-world MFA bypass techniques in recent breaches 2024--2025. https://noorstream.com/2025/09/10/real-world-mfa-bypass-techniques-in-recent-breaches-2024-2025/

[12] **CBS** -- Cybersecuritymonitor 2024. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[13] **Eftsure** -- Two-Factor Authentication Statistics. https://www.eftsure.com/statistics/two-factor-authentication-statistics/

[14] **CISA** -- Implementing Phishing-Resistant MFA. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[15] **NTNT** -- Hoe implementeer ik MFA in mijn bedrijf? https://www.ntnt.nl/hoe-implementeer-ik-mfa-in-mijn-bedrijf/

[16] **DesktopToWork** -- MFA implementatie in 5 stappen. https://desktoptowork.com/hoe-multi-factor-authenticatie-in-5-stappen-te-implementeren/

[17] **Descope** -- 2025 FIDO Report: The Passwordless Future. https://www.descope.com/blog/post/2025-fido-report

[18] **AdminByRequest** -- SIM Swapping and MFA Bombing. https://www.adminbyrequest.com/en/blogs/sim-swapping-and-mfa-bombing-how-attackers-beat-two-factor-authentication