WilroffReitsma

Haarlemmerstraatweg 111
1165 MK Halfweg

Satelliet 7
3824 MT Amersfoort

Tel: +31 20 40 77 700
www.wilroffreitsma.nl

Kvk: 34067050
BTW: NL 8035 25 928.B01
IBAN: NL 39 ABNA 0643 248 277

WilroffReitsma
Configuratie Multi Factor Authentication (MFA)

WilroffReitsma B.V.
8-12-2023
P. de Boer
Versie 1.0

1 Inhoudsopgave

2 MFA instellingen uitleg

MFA is momenteel volgens Microsoft een ‘must’ om geconfigureerd te hebben binnen Microsoft Azure. Niet gebruik maken van MFA wordt gezien als een beveiligingsrisico.

Het aanzetten van MFA niet veilig genoeg, dus zullen er bepaalde instellingen strakker moeten worden geconfigureerd. Denk hierbij aan de tijd van een sessie na goedkeuring van MFA. Waarom is dit een extra functie waaraan gedacht moet worden? Omdat na aanzetten van MFA de standaard door Microsoft op 90 dagen worden gezet, met andere woorden, dan hebben hackers de mogelijkheid om 90 dagen jouw sessie te hacken om dan alsnog alles te kunnen doen met het account wat mogelijk is.

MFA wordt ingesteld via Conditional Access (Voorwaardelijke Toegang), wat betekent dat er een algemene policy wordt gemaakt die geldt voor het hele bedrijf. Dit zijn 2 policies, 1 voor Windows apparaten en 1 voor mobiele apparaten (iOS en Android). Deze policies omschrijven een aantal zaken:

- Welke groep met gebruikers maakt gebruik van deze policy
- Welke groep met bijvoorbeeld ‘Rooms’ maakt geen gebruik van deze policy
- Welke applicaties maken gebruik van MFA (standaard zijn dit de applicaties van Microsoft)
- Welke applicaties worden uitgezonderd voor MFA (dit kunnen alleen door Microsoft goedgekeurde applicaties zijn)
- Welke locaties (Named Locations) zijn ‘vertrouwd’ (denk hierbij aan de kantoor locatie)
- Na hoeveel tijd dient een apparaat weer MFA versleuteling te vragen? Die tijd is afhankelijk zijn van welke apparaat (Windows of Mobiel)

3 MFA requirements

Om MFA via Conditional Access aan te kunnen zetten, zijn de volgende licenties minimaal nodig:

- Users: Microsoft 365 Business Premium
- Tenant: Azure AD Premium P1

Iedere medeweker dient in het bezit te zijn van een smartphone met iOS of Android zodat de Microsoft Authenticator App kan worden gedownload in de App Store of via Google Play.

android Android Download Link	
iOS iOS Download Link	

4 WR Standaarden

De ingesteld standaard door WR is hierbij als volgt:

- Vertrouwde locaties: Kantoor locatie(s)
    - Hiervoor hebben wij de IP Adressen van iedere locatie nodig om in te stellen. Thuis IP adressen worden niet gezien als vertrouwde locaties.

- MFA Sessies frequentie Windows apparaten: 16 uur
    - Ieder Windows apparaat zal na 16 uur de sessie vernieuwen via de Microsoft Authenticator App

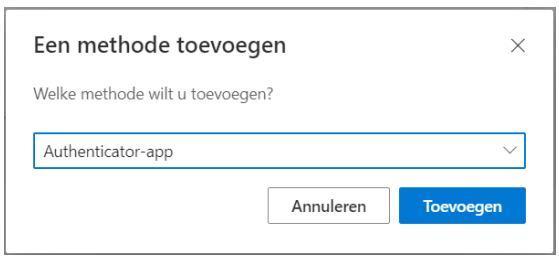
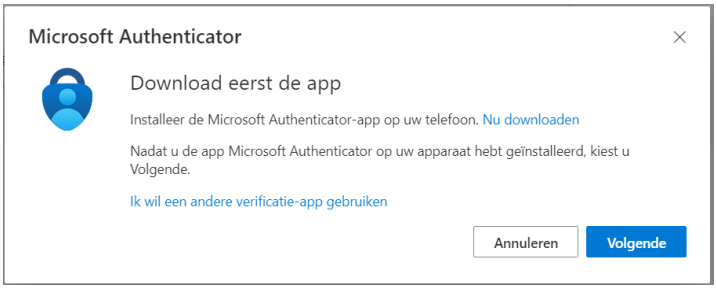
- MFA Sessies frequentie Mobiele apparaten: 7 dagen
    - Ieder Mobiel apparaat draaiend op iOS of Android zal na 7 dagen de sessie vernieuwen via de Microsoft Authenticator App

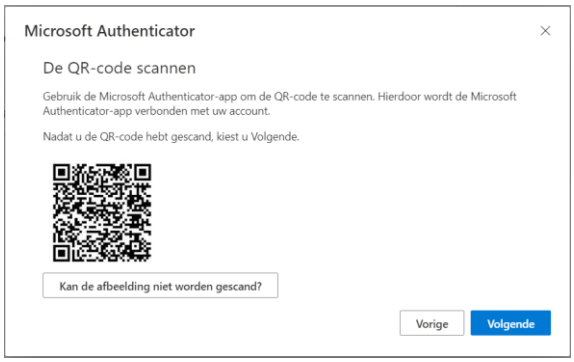
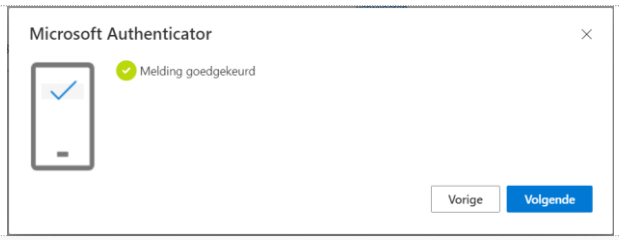
- MFA methode is alleen via de Microsoft Authenticator App (te downloaden in de App Store en Google Play Store)
    - Voormalige methodes zoals SMS of bellen zijn niet meer veilig genoeg

5 Hoe kunnen gebruikers verder als MFA is ingesteld?

Wanneer alle policies aan zijn gezet en functioneel zijn, zal dit direct van toepassing zijn bij de gebruikers.

Gebruikers dienen te gaan naar https://portal.office.com

Rechtsbovenin klikken op je eigen naar en kies voor ‘Account weergeven’	
Kies daarna voor ‘Beveiligingsgegevens’ aan de rechterkant.	
Daarna op ‘+ Aanmeldmethode toevoegen’ en kies voor ‘Authenticator-app’.	
1e venster is alleen van toepassing als de App nog niet is gedownload op een mobiel apparaat:	

2e venster geeft aan dat het account ingesteld dient te worden in de Authenticator App:	
Open ondertussen de Authenticator App voor de eerste keer op je mobiele apparaat en kies na akkoord te zijn gegaan voor ‘Een QR-code scannen’	
Scan de code die in beeld staat op je scherm en klik daarna op volgende:	
Keur na het scanner van de QR-code de melding op je mobiele apparaat goed door te klikken op ‘Goedkeuren’:	
Druk op ‘volgende’:	
Daarna staat de methode configureert in je account en is MFA goed ingesteld: