CENTRE FOR CYBERSECURITY BELGIUM

MULTIFACTORAUTHENTICATIE (MFA): EEN HANDLEIDING VOOR ORGANISATIES

MFA BEGRIJPEN EN IMPLEMENTEREN VOOR BETERE IT-BEVEILIGING

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Inhoudsopgave

Inhoudsopgave 2
1. Inleiding 3
2. Wat is multifactorauthenticatie en waarom is het belangrijk? 3
3. Multifactorauthenticatie: een kritieke beveiligingsmaatregel voor organisaties 4
4. Hoe implementeer je multifactorauthenticatie op het werk? 5
4.1 MULTIFactorauthenticatie op applicatieniveau 6
4.2 MULTIfactorauthenticatie bij toegang op afstand 7
4.3 Belangrijk bij het kiezen van een MFA-oplossing 8
4.4 MFA implementeren in Azure Cloud 8
4.5 MFA implementeren in Google Cloud 9
4.6 MFA implementeren in specifieke apps via Itsme 9
4.7 Authenticatieapps 10
5. Aandachtspunten voor de configuratie van multifactorauthenticatie en gebruikersondersteuning 10
6. Mogelijke problemen of hindernissen 11
6.1 Verbinding verbroken 11
6.2 Factoren om rekening mee te houden bij het kiezen van een MFA-methode 11
6.3 MFA en BYOD 12
7. Belangrijkste aandachtspunten voor veilig MFA-gebruik 13
8. Referenties 14
8.1 Cyberfundamentals 14
8.2 Safeonweb (@work) 14

1. Inleiding

Als het gaat om het beveiligen van je accounts, heb je waarschijnlijk wel al gehoord van tweefactorauthenticatie (2FA) of multifactorauthenticatie (MFA). Tweefactorauthenticatie is een beveiligingsmethode waarbij je twee authenticatiefactoren moet gebruiken om toegang te krijgen tot een account. Bij multifactorauthenticatie moet je twee of meer authenticatieparameters of -factoren ingeven. 2FA bestaat dus uit twee verificatiestappen, en MFA uit meerdere verificatiemethoden.

Deze eenvoudige maar doeltreffende oplossing voegt een extra beschermingslaag toe door je te vragen om twee of meer vormen van identificatie. Zelfs als iemand je wachtwoord weet, voorkomt het gebruik van MFA een ongeoorloofde toegang tot je accounts. Het is sterk aan te raden om MFA waar mogelijk te gebruiken vanwege het gebruiksgemak en de betere veiligheid. Het belang van 2FA en MFA voor publieke of private organisaties kan niet genoeg benadrukt worden. Cyberdreigingen, waaronder ransomwareaanvallen, datalekken en inbreuken, vormen een groot risico. Het is statistisch aangetoond dat een aanzienlijk percentage van de ransomware-aanvallen voorkomen zou kunnen worden door MFA te implementeren. Door meerdere beveiligingslagen toe te voegen, maakt MFA het veel moeilijker voor cybercriminelen om toegang te krijgen tot gevoelige gegevens, waardoor de kans op datalekken en andere cyberbedreigingen afneemt.

In deze gids overlopen we de basisprincipes van MFA en geven we praktisch advies over hoe je MFA kan implementeren binnen je organisatie. We halen ook voorbeelden aan uit de praktijk en geven tips om veelvoorkomende valkuilen te vermijden bij het implementeren van MFA-oplossingen. Na afloop begrijp je beter hoe MFA functioneert en hoe je het effectief kunt gebruiken om de gevoelige informatie van je organisatie te beschermen. In ons *Cyberfundamentals Framework* benadrukken we ook duidelijk de cruciale rol van sterke authenticatiemaatregelen bij het beschermen van de digitale middelen van je organisatie.

2. Wat is multifactorauthenticatie en waarom is het belangrijk?

Eenvoudig gezegd, houdt MFA in dat je naast je wachtwoord een extra code of bevestiging gebruikt om veilig toegang te krijgen tot een account of systeem. Met MFA moet je een wachtwoord en een token of biometrische gegevens opgeven om toegang te krijgen tot informatie, wat het risico op ongeoorloofde toegang sterk vermindert. Door meerdere vormen van authenticatie te vereisen, verhoogt MFA de beveiliging van je organisatie aanzienlijk en **vermindert het risico op ongeoorloofde toegang tot gevoelige informatie of systemen**.

Om veilig toegang te krijgen tot je account, moet je je identiteit bewijzen. Dit kan door gebruik te maken van drie methoden of factoren:

- iets dat alleen jij weet (je wachtwoord of pincode);
- iets waar alleen jij toegang toe hebt (je telefoon of token); of
- iets dat van jou is (je vingerafdruk, gezicht, regenboogvlies etc.).

Het implementeren van MFA op organisatieniveau betekent dat werknemers en andere gebruikers meer dan één vorm van authenticatie moeten opgeven om toegang te krijgen tot bedrijfssystemen, netwerken en gevoelige informatie en applicaties. MFA kan worden geïmplementeerd in een heel aantal applicaties en systemen, zoals e-mail, VPN's, clouddiensten en interne netwerken.

MFA wordt steeds belangrijker in de hedendaagse businessomgeving, waar cyberdreigingen geavanceerder en frequenter worden. Een phishingaanval, waarbij een gebruiker wordt overgehaald om zijn wachtwoord vrij te geven, is bijvoorbeeld minder efficiënt tegen **een systeem met MFA**, omdat de aanvaller ook het token of de biometrische gegevens moet verstrekken om toegang te krijgen. Ook een brute-forceaanval, waarbij meerdere wachtwoordcombinaties worden uitgetest, zou veel minder efficiënt zijn tegen een systeem met MFA, omdat de aanvaller ook de bijkomende authenticatie moet opgeven.

Naast **het verbeteren van de beveiliging** kan het implementeren van MFA **organisaties** ook helpen om **te voldoen aan de wet- en regelgeving** voor sterke authenticatiemaatregelen (bv. AVG, NIS2). MFA kan ook helpen de continuïteit van de diensten te waarborgen door inbreuken op de beveiliging te voorkomen of de gevolgen ervan te milderen, zodat organisaties hun activiteiten na een minimale verstoring kunnen voortzetten.

3. Multifactorauthenticatie: een kritieke beveiligingsmaatregel voor organisaties

Hoewel MFA traditioneel wordt geassocieerd met grote ondernemingen, wordt het alsmaar **toegankelijker en betaalbaarder** voor alle organisaties. Bovendien zijn sommige MFA-oplossingen beschikbaar in de vorm van een **abonnement**, waardoor organisaties hun kosten efficiënter kunnen beheren door alleen te betalen voor wat ze nodig hebben. MFA-oplossingen zijn steeds **gebruiksvriendelijker** en **eenvoudiger te implementeren**. Veel leveranciers bieden eenvoudige plug-and-play opties die een minimale configuratie vereisen.

Sommige MFA-oplossingen zijn zelfs complementair met bestaande toegangsbeheersystemen, wat het voor organisaties eenvoudiger maakt om ze te implementeren **zonder grote veranderingen aan hun bestaande infrastructuur**, zoals Active Directory of LDAP. Zowel LDAP als Active Directory worden gebruikt voor authenticatie en autorisatie, waardoor organisaties de toegang van gebruikers tot systemen, applicaties en gegevens kunnen beheren. Door MFA-oplossingen te integreren met LDAP of Active Directory kunnen organisaties hun beveiliging verbeteren en zich beschermen tegen cyberdreigingen, zonder hun bestaande infrastructuur volledig te moeten aanpassen. Door MFA prioritair te gebruiken als **kritieke beveiligingsmaatregel** kunnen organisaties proactief stappen ondernemen om zichzelf en de gevoelige informatie van hun klanten te beschermen. Zo kunnen organisaties MFA implementeren om hun beveiliging te verbeteren en het risico op ongeautoriseerde toegang tot gevoelige informatie of systemen te verminderen.

Waarom een wachtwoord alleen niet meer volstaat:

- Wachtwoorden kunnen gemakkelijk achterhaald worden, vooral als ze eenvoudig en makkelijk te onthouden zijn. Daarom gebruiken veel aanvallers bruteforce- en wachtwoordspraying-aanvallen, waarbij ze een wachtwoord proberen te achterhalen door veel combinaties te testen.
- Wachtwoorden kunnen worden hergebruikt voor meerdere accounts, dus als een wachtwoord gecompromitteerd is, kunnen aanvallers het gebruiken om ook toegang te krijgen tot andere accounts. Dit staat bekend als wachtwoordhergebruik en is een veelvoorkomend probleem dat het gebruik van een wachtwoord alleen minder veilig maakt.

Wachtwoorden kunnen worden **gestolen via phishingaanvallen of malware**. Aanvallers kunnen valse e-mails of berichten sturen die lijken te komen van een legitieme bron en gebruikers ertoe aanzetten om hun inloggegevens mee te delen. Ook malware kan zo worden gebruikt om wachtwoorden rechtstreeks van het apparaat van een gebruiker te stelen.

Door deze zwakke punten **kan het gebruik van enkel een wachtwoord op verschillende manieren worden uitgebuit**. Aanvallers kunnen bijvoorbeeld gestolen of geraden wachtwoorden gebruiken om toegang te krijgen tot gevoelige gegevens of systemen van een organisatie. Ze kunnen ook tools gebruiken om zwakke wachtwoorden te kraken en vervolgens dezelfde wachtwoorden gebruiken om toegang te krijgen tot andere accounts. Kortom, de zwakke punten van wachtwoorden maken ze kwetsbaar voor uitbuiting. Daarom is het implementeren van MFA cruciaal voor een betere beveiliging.

4. Hoe implementeer je multifactorauthenticatie op het werk?

In de praktijk omvat het implementeren van MFA voor organisaties vier stappen om ervoor te zorgen dat de uitrol efficiënt en veilig gebeurt: identificeren, kiezen, plannen en implementeren.

De eerste stap is **te bepalen voor welke systemen en applicaties MFA nodig is** en welke soorten authenticatie het meest geschikt zijn. Toegang tot vertrouwelijke gegevens moet worden beveiligd via MFA.

De tweede stap is het **kiezen van een MFA-oplossing die past bij de behoeften en het budget van je organisatie**. Het is belangrijk voor organisaties om factoren zoals gebruiksgemak, schaalbaarheid en kosten in overweging te nemen bij het kiezen van een MFA-oplossing. Je moet ook een oplossing kiezen die compatibel is met de bestaande systemen en applicaties die je organisatie gebruikt, en rekening houden met de beveiligingsrisico's en bedreigingen waarmee je organisatie wordt geconfronteerd.

De derde stap is het **plannen van de uitrol van de MFA-oplossing**. Dit is belangrijk om ervoor te zorgen dat de uitrol efficiënt gebeurt en de bedrijfsactiviteiten niet verstoort. Organisaties moeten bij het plannen van de uitrol ook rekening houden met elementen zoals gebruikersopleiding, communicatie en ondersteuning. Het is belangrijk om de voordelen van MFA te communiceren naar de gebruikers en om in opleiding te voorzien over het juiste gebruik van de MFA-oplossing.

Hier zijn enkele specifieke voorbeelden die organisaties kunnen overwegen bij het kiezen van een MFA-oplossing:

- **SMS-gebaseerde MFA**: bij deze optie wordt een eenmalige code via sms naar de telefoon van de gebruiker gestuurd. De gebruiker voert dan de code in om het authenticatieproces te voltooien.
- **Softwaregebaseerde MFA**: bij deze optie wordt meestal een mobiele app of desktopsoftware gebruikt om een eenmalige code te genereren. Enkele voorbeelden van softwarematige MFA's zijn Google Authenticator en Microsoft Authenticator.
- **Hardwaregebaseerde MFA**: bij deze optie wordt meestal een fysieke token gebruikt, zoals een smartcard of USB-apparaat, om een eenmalige code te genereren. Hardwaregebaseerde MFA kan duurder en minder flexibel zijn dan andere opties, maar kan geschikt zijn voor organisaties die een hoger beveiligingsniveau vereisen.
- **Biometrische MFA**: hierbij worden biometrische gegevens, zoals vingerafdrukken of gezichtsherkenning, gebruikt om gebruikers te authenticeren. Biometrische MFA kan handiger en veiliger zijn dan andere opties, maar kan gespecialiseerde hardware of software vereisen en is soms ook duurder.

De laatste stap is het **implementeren van de MFA-oplossing**. Dit omvat het configureren van de MFA-oplossing om te werken met de systemen en applicaties die dat vereisen. Organisaties moeten ook voortdurende gebruikersondersteuning bieden om ervoor te zorgen dat de MFA-oplossing op de juiste manier wordt gebruikt en om eventuele problemen op te lossen.

Het verbeteren van de cyberbeveiliging kan vaak een ontmoedigende en complexe taak lijken, vooral met beperkte middelen en budgetten. Het implementeren van MFA kan echter een snelle en efficiënte manier zijn om je beveiliging aanzienlijk te verbeteren. Deze extra beveiligingslaag vermindert het risico op ongeautoriseerde toegang aanzienlijk, omdat het veel moeilijker wordt voor aanvallers om traditionele beveiligingsmaatregelen op basis van wachtwoorden te omzeilen. MFA kan eenvoudig worden geïmplementeerd en veel leveranciers bieden gebruiksvriendelijke oplossingen. Door het te implementeren kunnen organisaties snel hun beveiliging verbeteren, hun gevoelige gegevens beschermen en het vertrouwen van klanten vergroten, en dat alles binnen hun budget en middelen.

4.1 MULTIFACTORAUTHENTICATIE OP APPLICATIENIVEAU

MFA kan worden geïmplementeerd in een reeks applicaties en systemen, zoals e-mail, VPN, clouddiensten en interne netwerken. De meest gebruikte diensten bieden een vorm van multifactorauthenticatie en bevatten een korte instructiepagina. Hier vind je enkele voorbeelden:

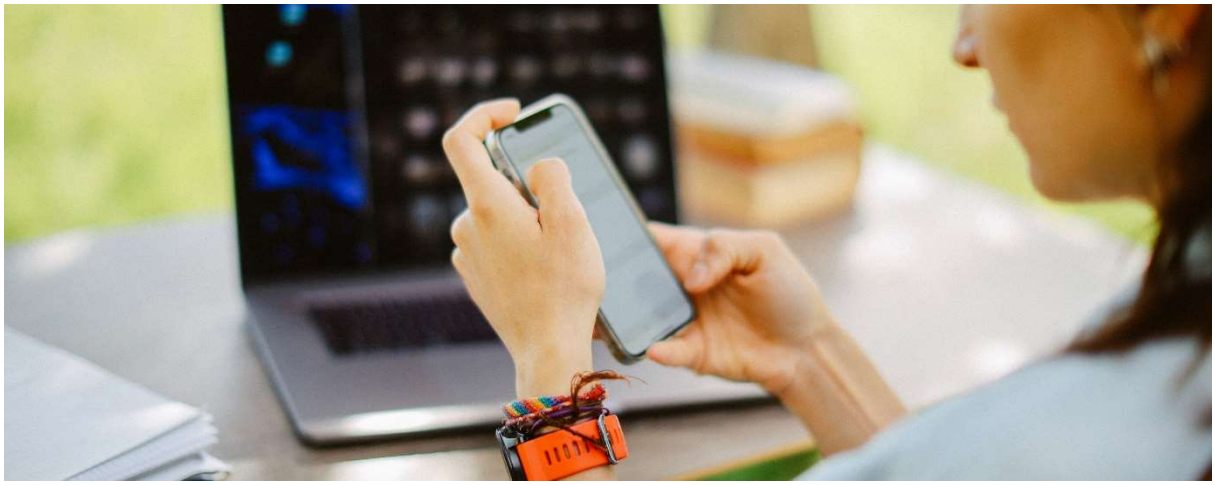
- Dropbox
- Google
- LinkedIn
- Microsoft
- Skype
- WhatsApp
- Yahoo

Voor meer concrete voorbeelden verwijzen we je naar het volgende artikel: Tweestapsverificatie toevoegen, hoe doe ik dat?

4.2 MULTIFACTORAUTHENTICATIE BIJ TOEGANG OP AFSTAND

Toegang op afstand verwijst naar de mogelijkheid voor gebruikers of processen om **verbinding te maken** met een informatiesysteem van de organisatie **via externe netwerken zoals het internet**. Het werkt meestal met technologieën zoals versleutelde Virtual Private Networks (VPN's) om de vertrouwelijkheid en integriteit van de communicatie te verzekeren. Voor het implementeren van een veilige toegang op afstand moeten strikte gebruiksbeperkingen, configuratievereisten en autorisatieprotocollen worden opgesteld. Dit zorgt ervoor dat alleen bevoegde gebruikers op afstand toegang hebben tot het systeem, waardoor het systeem beschermd wordt tegen mogelijke bedreigingen van buitenaf.

In de context van toegang op afstand kan het belang van MFA niet genoeg worden benadrukt. Een wachtwoord alleen, hoe complex ook, kan nog steeds worden gekraakt, achterhaald of gephisht door cybercriminelen. Door MFA te implementeren, kunnen organisaties **een extra beveiligingslaag toevoegen aan hun protocollen voor toegang op afstand** en ervoor zorgen dat alleen bevoegde gebruikers toegang krijgen tot hun systemen.



4.3 BELANGRIJK BIJ HET KIEZEN VAN EEN MFA-OPLOSSING

Voordat je een MFA-oplossing kiest, moet je rekening houden met het volgende:

- **Beveiliging**: kies een veilige MFA-tool die voldoet aan beveiligingsstandaarden en best practices.
- **Compatibiliteit**: zorg ervoor dat je een MFA-tool kiest die compatibel is met het bestaande systeem en de infrastructuur binnen je organisatie (bv. OS-versie) en die gemakkelijk geïntegreerd kan worden in het authenticatiekader van je organisatie (bv. Active directory).
- **Implementatie**: kies een MFA-tool die beveiliging biedt en eenvoudiger te implementeren is binnen de omgeving van je organisatie en de mate van ondersteuning die nodig is.
- **Kosten**: evalueer de kosten van de middelen die nodig zijn voor de implementatie van MFA, zoals onderhoud, licentiekosten etc.
- **Authenticatieopties**: kies voor een MFA-tool die verschillende authenticatieopties biedt om te zorgen voor de nodige flexibiliteit voor de gebruikers om de authenticatiefactoren te kiezen op basis van hun voorkeuren en behoeften.

Hieronder vind je enkele voorbeelden van het opzetten van multifactorauthenticatie binnen je organisatie met behulp van de meest gebruikte authenticatietoepassingen. Dit zijn algemene richtlijnen die mogelijk niet van toepassing zijn op de behoeften van je organisatie. De specifieke kenmerken kunnen ook verschillen naargelang je omgeving.

4.4 MFA IMPLEMENTEREN IN AZURE CLOUD

Stap 1: Azure Active Directory (vereist)

Om de Microsoft Authenticator-app te kunnen gebruiken, moet je organisatie een Azure AD (Active Directory)-account hebben.

Stap 2: MFA inschakelen

Elke versie van Azure AD bevat Azure AD Multi-Factor Authentication. Er is geen extra licentie nodig voor de registratie. Dit kan worden gedaan in het Azure-portal door te gaan naar Azure Active Directory > Security > MFA.

Stap 3: Authenticatiemethoden kiezen

Microsoft Authenticator ondersteunt een reeks authenticatiemethoden, zoals pushmeldingen en eenmalige wachtwoorden.

Stap 4: Policy's configureren

Deze stap stelt je organisatie in staat om te bepalen welke gebruikers MFA moeten gebruiken, welke authenticatiemethoden gebruikt kunnen worden en wanneer MFA vereist is (bv. specifieke applicatie).

Dit kan worden bepaald aan de hand van een van deze policyregels:

- *MFA Registration Policy*: de gebruikers moeten worden toegestaan voor meldingen via de mobiele applicatie.
- *Authentication Methods Policy*: de gebruikers moeten worden toegestaan voor de Authenticator-app en de Authenticatiemodus moet ingesteld zijn op Any of Push.

Stap 5: Microsoft Authenticator configureren

Zodra MFA is ingeschakeld en de policyregels geconfigureerd zijn, kunnen de instructies voor het instellen van Microsoft-authenticatie worden gecommuniceerd naar de gebruikers via e-mail of via de interne communicatieplatforms van je organisatie (bv. intranet).

Meer weten:

- Gebruikers aanmodigen om Microsoft Authenticator te configureren - Microsoft Entra | Microsoft Learn
- De MFA-registratiepolicy configureren - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

4.5 MFA IMPLEMENTEREN IN GOOGLE CLOUD

Stap 1: Google Cloud-account (vereist)

Om Google Authenticator te kunnen gebruiken, moet je organisatie een Google Cloud-account hebben voor de implementatie van MFA.

Stap 2: Tweestapsverificatie instellen

Schakel tweestapsverificatie in via de Google Admin Console:

Menu > Security> Authentication > 2-step verification.

Stap 3: Verificatiemethode kiezen

Google Authenticator ondersteunt een aantal tweestapsauthenticatiemethoden, zoals de Google Authenticator-app (voor Android versie 4.4 en hoger), beveiligingssleutels, Google prompt, sms of telefoonoproep en back-upcodes.

Stap 4: Policy configureren

Bepaal welke gebruikers MFA moeten gebruiken. Om de instelling op iedereen toe te passen, laat je de overkoepelende organisatieafdeling aangevinkt staan. Anders selecteer je een lagere organisatieafdeling of een configuratiegroep en vink je het vakje *Allow users to turn on 2-Step Verification* aan.

Om MFA te verplichten voor alle gebruikers of de geselecteerde groep activeer je de optie *Enforcement*.

Stap 5: Tweestapsverificatie

Bezorg de gebruikers instructies voor het instellen van Google Authenticator via e-mail of de interne communicatieplatforms van je organisatie.

Meer weten: Deploy 2-Step Verification - Google Workspace Admin Help

4.6 MFA IMPLEMENTEREN IN SPECIFIEKE APPS VIA ITSME

Stap 1: Registreer voor itsme-MFA-diensten

Je organisatie moet geregistreerd zijn voor itsme-MFA-diensten om MFA via de itsme-app mogelijk te maken en een account aan te maken op het itsme-adminportaal aan de hand waarvan je organisatie MFA-instellingen kan beheren en gebruiksstatistieken kan bekijken.

Stap 2: Kies de authenticatiemethode

De beschikbare authenticatiemethoden in itsme zijn gebaseerd op ten minste een combinatie van iets dat de gebruiker bezit, zoals zijn smartphone en de geïnstalleerde itsme-applicatie, en biometrische gegevens van de gebruiker, zoals zijn vingerafdruk of Face-ID, of iets dat de gebruiker kent (bijvoorbeeld een pincode).

Stap 3: Configureer policy's

Surf naar de policy-instelling in het adminportaal en bepaal de regels die vereisen dat itsme-MFA vereist is, alsook de uitzonderingen en het instellen van meldingen in geval van mislukte loginpogingen.

Stap 4: Implementeer itsme-MFA

Bezorg de gebruikers instructies voor het instellen van itsme via e-mail of via de interne communicatieplatforms van je organisatie.

Meer weten: General information - Documentation - Onboarding (belgianmobileid.be)

4.7 AUTHENTICATIEAPPS

Een authenticatieapp is een toepassing die wordt gebruikt om tijdelijke eenmalige wachtwoorden (*time-based one-time passwords* - TOTPS) voor multifactorauthenticatie te genereren. Zo kunnen gebruikers hun accounts beveiligen met een tweede verificatielaag:

- Authy
- Google Authenticator
- Microsoft Authenticator
- Okta Verify

5. Aandachtspunten voor de configuratie van multifactorauthenticatie en gebruikersondersteuning

Policyconfiguratie:

- Bepaal de toegestane authenticatiemethode voor de gekozen verificatietoepassing die compatibel is met je organisatieomgeving en gebruikersbehoeften.
- Het wordt aanbevolen om MFA toe te passen voor alle gebruikers en applicaties, in het bijzonder tijdens het werken op afstand. Hierbij moet de admin specificeren voor welke gebruiker, groep en apps de MFA van toepassing is, de criteria voor uitzonderingen definiëren en ervoor zorgen dat de juiste controles aanwezig zijn.
- Integreer MFA met het beschikbare systeem binnen je organisatie (zoals Active Directory) om ervoor te zorgen dat MFA wordt opgelegd voor alle apps en systemen. Zorg voor een hoog beveiligingsniveau en tegelijk voor een goede gebruikerservaring door één enkele set gebruikersgegevens te hanteren.

Gebruikersondersteuning:

Na het configureren van de policy en het verplichten van MFA kunnen de gebruikers zich niet meer authenticeren op het systeem zonder MFA in te schakelen. Je organisatie moet ervoor zorgen dat de gebruikers de juiste ondersteuning krijgen door:

- duidelijk te communiceren over het MFA-registratieproces en gebruikers richtlijnen te geven voor het instellen van de verificatie-app op hun mobiele apparaten via de communicatiemiddelen van je organisatie, zoals e-mail en intranet;
- opleidingen voor gebruikers te organiseren om meer vertrouwd te geraken met MFA, het doel ervan en hoe het kan worden gebruikt;
- permanente ondersteuning te bieden, onder meer via contactpersonen bij wie de gebruikers terecht kunnen voor ondersteuning bij de implementatie;
- de gebruikers op de hoogte te houden van wijzigingen of updates van de MFA-policy en -toepasbaarheid.

6. Mogelijke problemen of hindernissen

6.1 VERBINDING VERBROKEN

Het is belangrijk om een back-up plan te hebben voor het geval dat de gebruikers zich niet kunnen authenticeren met MFA door problemen met de verbinding, verlies van het MFA-compatibele apparaat of via de primaire methode (bv. geblokkeerd GSM-nummer, gewijzigde e-mail). Dit kan het volgende omvatten:

- **Een back-up-authenticatiemethode** bieden, zoals een tweede telefoonnummer of e-mailadres.
- **Alternatieve authenticatiemethoden** gebruiken, die niet afhankelijk zijn van connectiviteit (bv. fysieke tokens, smartcards).
- MFA **tijdelijk uitschakelen** voor een specifieke gebruiker of groep gebruikers. Dit is echter een laatste redmiddel. De MFA moet weer geactiveerd worden zodra het probleem is opgelost.

Daarnaast moet er een operationele ondersteuningsgids worden opgesteld met stapsgewijze instructies voor het oplossen van problemen, de contactpersonen voor ondersteuning en de manieren om ervoor te zorgen dat de gegevens van je organisatie veilig blijven tijdens de storing.

6.2 FACTOREN OM REKENING MEE TE HOUDEN BIJ HET KIEZEN VAN EEN MFA-METHODE

Bij het kiezen van een multifactorauthenticatiemethode is het belangrijk om te overwegen welk type MFA het beste past bij de behoeften van je organisatie. Een veelgebruikte MFA-methode is een authenticatie-app. Hoewel deze methode handig en veilig is, is het belangrijk om in gedachten te houden dat alle gebruikers een smartphone nodig hebben om deze te gebruiken. Dit kan een potentieel probleem zijn voor **organisaties die hun werknemers geen smartphone van de organisatie ter beschikking stellen** of voor **werknemers die geen smartphone hebben**, de applicatie niet op hun persoonlijke smartphone **willen installeren** of er slechts beperkte toegang toe hebben. In dergelijke gevallen kan het nodig zijn om alternatieve MFA-methoden te overwegen, zoals via een fysiek beveiligingstoken of een sms, om ervoor te zorgen dat alle gebruikers veilig toegang kunnen krijgen tot de systemen. Daarom is het cruciaal om **de voor- en nadelen** van verschillende MFA-methoden **tegen elkaar af te wegen** voordat je een beslissing neemt, en ervoor te zorgen dat de gekozen methode toegankelijk is voor alle gebruikers.

6.3 MFA EN BYOD

Persoonlijke apparaten zoals smartphones die voor werkdoeleinden worden gebruikt, zijn mogelijk niet compatibel met de gekozen MFA-methode van je organisatie, waardoor het moeilijk is om **MFA te verplichten in een *Bring Your Own Device* (BYOD)-omgeving** en te zorgen voor een consistente MFA-implementatie op alle apparaten op een formele en correcte manier.

Overweeg daarom het gebruik van MDM (*Mobile Device Management*) om persoonlijke apparaten van gebruikers die voor werkdoeleinden worden gebruikt, te beheren en zorg ervoor dat deze apparaten goed beveiligd zijn en voldoen aan het beveiligingsbeleid van je organisatie.

Daarnaast moet het beveiligingsbeleid van de organisatie worden toegepast om:

- ervoor te zorgen dat **minimale beveiligingseisen** worden geïmplementeerd op de apparaten van gebruikers (bv. type besturingssysteem, vereisten voor het up-to-date houden van het apparaat met beveiligingspatches, configuraties etc.);
- het belang van MFA en **de risico's van het gebruik van persoonlijke apparaten** voor werkdoeleinden te benadrukken. Ze moeten worden gecommuniceerd aan alle werknemers van de organisatie om hen bewust te maken van de manier waarop persoonlijke apparaten die voor werkdoeleinden worden gebruikt, kunnen worden beschermd;
- ondersteuning te bieden met **duidelijke richtlijnen** voor gebruikers om hun apparaten goed te configureren voor gebruik met MFA en procedures op te stellen voor hoe en waar ze een beveiligingsincident met betrekking tot BYOD moeten melden;
- de toegang op afstand te beperken. Je organisatie zou ook moeten overwegen **om de toegang** tot haar gegevens en applicaties **te segmenteren** op basis van het risiconiveau en MFA verplicht te stellen wanneer dat haalbaar is en in het bijzonder voor gegevens en applicaties met een hoog risico en toegang op afstand.

Tot slot moet het implementeren van **MFA in BYOD-omgevingen** worden beschouwd als een essentiële beveiligingsmaatregel, omdat apparaten van werknemers mogelijk niet voldoen aan dezelfde beveiligingsstandaarden als apparaten die eigendom zijn van de organisatie.

7. Belangrijkste aandachtspunten voor veilig MFA-gebruik

Bij het gebruik van MFA om een extra beschermingslaag toe te voegen en de beveiliging te verbeteren, is het belangrijk om waakzaam te zijn en rekening te houden met bepaalde aandachtspunten:

- **Beveilig je apparaten**: implementeer beveiligingsupdates en patches voor je MFA-applicatie, besturingssystemen en softwareversies die op je apparaten zijn geïnstalleerd zodra ze beschikbaar zijn, om mogelijke kwetsbaarheden te verhelpen.
- **Aandachtige interactie**: als je push-upmeldingen kiest als tweede authenticatiefactor is het belangrijk om waakzaam te blijven en te voorkomen dat je niet achteloos meldingen accepteert zonder de inhoud te bekijken. Neem altijd de tijd om de melding te lezen voordat je actie onderneemt.
- **Gebruik een sterk(e) wachtwoord/wachtzin:** gebruik naast MFA een sterk en lang wachtwoord of een verzameling van ten minste drie willekeurige algemene woorden gecombineerd tot een zin die een zeer goede combinatie van onthoudbaarheid en beveiliging bieden, met kleine letters en hoofdletters, eventueel ook cijfers en speciale tekens en vermijd voor de hand liggende paswoorden, zoals "wachtwoord", “ABCDEF”, “123456” en persoonlijke informatie.
- **Gebruik officiële platforms:** gebruik bij het downloaden van MFA-applicaties vertrouwde officiële appstores zoals Google Play Store voor Android of de Apple App Store voor IOS-apparaten om de authenticiteit en integriteit van de applicatie te garanderen en zo het risico op het downloaden van kwaadaardige software te verkleinen.

8. Referenties

8.1 CYBERFUNDAMENTALS

Deze bijlage bevat links naar de relevante basisvereisten voor cyberfundamentals in verband met multifactorauthenticatie (MFA) en biedt gedetailleerde referenties ter ondersteuning van de implementatie en het beheer van MFA in het cyberbeveiligingskader.

- **PR.AC-3: De toegang op afstand wordt beheerd.**

  Belangrijkste maatregel: de netwerken van de organisatie die op afstand worden gebruikt, moeten worden beveiligd, **onder andere door middel van multifactorauthenticatie (MFA)**.

8.2 SAFEONWEB (@WORK)

Bescherm accounts met multifactorauthenticatie | Safeonweb@work

Een sterk wachtwoord om waardevolle informatie te beschermen | Safeonweb@work

Policy templates | Safeonweb@work

Gebruik tweestapsverificatie | Safeonweb

Tweestapsverificatie toevoegen, hoe doe ik dat? | Safeonweb