IMPLEMENTATIEPLAN VOOR PHISHING-RESISTANT MFA IN AZURE

15 november 2024

versie 0.1

Inhoudsopgave

1 Inleiding 3

2 Doelstelling: 4

2.1 Voorbereidingen: 4

3 Advies voor Phishing-Resistente MFA-methoden: 5

4 Stappenplan voor Implementatie 6

4.1 Stap 1: Voorbereiding in Azure Entra 6

4.2 Stap 2: Implementatie van FIDO2 Security Keys 6

4.3 Stap 3: Implementatie van Windows Hello for Business 6

4.4 Stap 4: Certificate-based Authentication (CBA) 7

5 Stap 5: Monitoring en Rapportage 8

6 Advies voor Beheer en Onderhoud 9

7 Conclusie: 10

# Inleiding

Met de toename van phishingaanvallen is het belangrijk om robuuste multi-factor authenticatie (MFA) te implementeren die phishingbestendig is. Traditionele MFA-methoden, zoals SMS en e-mail, zijn kwetsbaar voor phishingaanvallen en sim-swapping. In dit document geven we een advies en stapsgewijs implementatieplan voor het invoeren van phishing-resistente MFA in Azure.

# Doelstelling:

Het doel van dit plan is om Azure Entra-omgevingen van klanten te beveiligen door middel van sterke, phishingbestendige MFA-methoden zoals **FIDO2**, **Windows Hello for Business**, en **Certificate-based Authentication (CBA)**.

## Voorbereidingen:

1. **Vereistenanalyse:**
   * Inventariseer de huidige omgeving en identificeer bestaande authenticatiemethoden.
   * Controleer of alle gebruikers Azure Entra Premium P1 of hoger hebben (vereist voor geavanceerde MFA-opties).
   * Zorg dat gebruikers beschikken over ondersteunde hardware voor FIDO2 (zoals YubiKey) en apparaten met TPM 2.0 voor Windows Hello for Business.
2. **Communicatie en Change Management:**
   * Informeer stakeholders en eindgebruikers over de geplande wijzigingen.
   * Stel een communicatieplan op om gebruikers te informeren over de voordelen en de nieuwe inlogmethoden.
   * Plan trainingssessies voor gebruikers om hen te begeleiden bij de configuratie van nieuwe MFA-methoden.

# Advies voor Phishing-Resistente MFA-methoden:

| **Methode** | **Beschrijving** | **Voor- en nadelen** |
| --- | --- | --- |
| **FIDO2 Security Keys** | Hardware tokens die phishingbestendig zijn. | + Zeer veilig, + Geen wachtwoord nodig, - Extra kosten |
| **Windows Hello for Business** | Biometrische of PIN-gebaseerde authenticatie | + Gebruiksvriendelijk, - Vereist TPM 2.0-apparaten |
| **Certificate-based Authentication (CBA)** | Certificaatgebaseerde verificatie | + Veilig, - Complexere implementatie |

# Stappenplan voor Implementatie

## Stap 1: Voorbereiding in Azure Entra

1. **Controleer licenties:**
   * Zorg dat de omgeving is voorzien van Azure Entra Premium P1 of hoger.
2. **Controleer gebruikersinventaris:**
   * Gebruik Microsoft Graph API om alle gebruikers op te halen die momenteel geen MFA geconfigureerd hebben:

**powershell**

Get-MgUser -Filter "strongAuthenticationMethods/any()" | Select-Object UserPrincipalName

1. **Configureer MFA-beleid:**
   * Schakel **Conditional Access** in voor het afdwingen van MFA:
     + Ga naar **Entra** > **Security** > **Conditional Access**.
     + Maak een nieuw beleid aan: "Phishing-resistente MFA".
     + Selecteer de gebruikers en apparaten waarop dit beleid van toepassing is.
     + Kies als controle "Require multifactor authentication".

## Stap 2: Implementatie van FIDO2 Security Keys

1. **Activeer FIDO2-authenticatie:**
   * Ga naar **Entra** > **Security** > **Authentication methods**.
   * Klik op **FIDO2 Security Key** en zet de status op **Enabled**.
   * Selecteer de gebruikers of groepen waarvoor dit ingeschakeld moet worden.
2. **Uitgifte van FIDO2-sleutels:**
   * Verdeel FIDO2-sleutels onder de gebruikers.
   * Geef een handleiding voor het registreren van de sleutel:
     + Gebruikers navigeren naar [**https://myprofile.microsoft.com**](https://myprofile.microsoft.com).
     + Klik op **Security info** en voeg een **FIDO2 Security Key** toe.
3. **Test de configuratie:**
   * Laat een groep gebruikers testen met de nieuwe inlogmethode.
   * Verzamel feedback en los eventuele problemen op.

## Stap 3: Implementatie van Windows Hello for Business

1. **Activeer Windows Hello for Business:**
   * Ga naar **Entra** > **Devices** > **Windows Hello for Business**.
   * Kies de implementatiemodus: "Cloud trust" of "Key trust".
   * Zet de status op **Enabled** en selecteer de doelgroepen.
2. **Configureer Intune-profilen:**
   * Ga naar **Intune** > **Configuration profiles** en maak een profiel voor **Windows Hello for Business** aan.
   * Configureer de PIN- en biometrie-opties:
     + Min. lengte PIN: 6 cijfers
     + Gebruik biometrische verificatie: Ingeschakeld
3. **Test en implementatie:**
   * Voer een pilot uit met een kleine groep gebruikers.
   * Monitor de prestaties en verzamel feedback.

## Stap 4: Certificate-based Authentication (CBA)

1. **Voorbereiding van certificaten:**
   * Zorg dat er een Public Key Infrastructure (PKI) beschikbaar is.
   * Maak clientcertificaten aan voor gebruikers.
2. **Configureer Entra voor CBA:**
   * Ga naar **Azure AD** > **Security** > **Certificate-based Authentication**.
   * Schakel CBA in en voeg de rootcertificaten toe.
3. **Test en controle:**
   * Laat gebruikers hun certificaat importeren in hun apparaat.
   * Test de authenticatie en controleer of deze phishingbestendig is.

# Stap 5: Monitoring en Rapportage

1. **Conditional Access rapporten:**
   * Ga naar **Entra** > **Security** > **Conditional Access** > **Insights and reporting**.
   * Controleer of gebruikers de phishingbestendige MFA-methoden gebruiken.
2. **Audit logs:**
   * Controleer de audit logs op mislukte aanmeldpogingen:

**powershell**

Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -RecordType AzureActiveDirectory

1. **Gebruikersfeedback en aanpassingen:**
   * Verzamel feedback van gebruikers.
   * Pas het beleid aan indien nodig op basis van problemen en uitdagingen.

# Advies voor Beheer en Onderhoud

* **Training en ondersteuning:** Zorg voor doorlopende training van gebruikers.
* **Periodieke audits:** Voer regelmatige audits uit op MFA-gebruik en -effectiviteit.
* **Incident response:** Stel een incidentresponsplan op voor gebruikers die problemen ondervinden met MFA.

# Conclusie:

Door het implementeren van phishing-resistente MFA-methoden zoals FIDO2, Windows Hello for Business, en Certificate-based Authentication, vergroot je de beveiliging van Azure aanzienlijk. Het stappenplan biedt een gestructureerde aanpak om de implementatie soepel te laten verlopen en gebruikers te beschermen tegen phishingaanvallen.