ADVIESPLAN VOOR PHISHING-RESISTANT MFA IN AZURE

15 november 2024

versie 0.1

Inhoudsopgave

1 Inleiding 3

2 Voordelen van YubiKeys 4

3 Doelstelling: 5

4 Beoordeling van de Huidige Omgeving 6

5 Advies voor Implementatie van YubiKeys 7

5.1 1. Selectie van YubiKey-modellen: 7

5.2 2. Configuratie van Azure AD voor YubiKeys: 7

5.3 3. Uitgifte en distributie van YubiKeys: 7

5.4 4. Training en bewustwording: 7

5.5 5. Pilot en testing: 7

 **Beheer en Onderhoud van YubiKeys** 7

5.6 Verlies of diefstal: 8

5.7 Audit en rapportage: 8

5.8 Rotatie van sleutels: 8

6 Risico's en Beperkingen 9

7 Conclusie en Advies 10

# Inleiding

Dit adviesplan is gericht op de implementatie van YubiKeys binnen een organisatie als middel voor sterke en phishing-resistente multi-factor authenticatie (MFA). YubiKeys zijn hardware-gebaseerde authenticatieapparaten die meerdere beveiligingsprotocollen ondersteunen, waaronder **FIDO2**, **WebAuthn**, en **OTP** (One-Time Password). Ze bieden een hogere mate van beveiliging in vergelijking met traditionele MFA-methoden zoals SMS en e-mail, die vatbaar zijn voor phishing-aanvallen.

# Voordelen van YubiKeys

* **Phishing-resistent:** De sleutel werkt alleen op de juiste websites en kan niet worden gerepliceerd via phishing.
* **Gebruiksvriendelijk:** Een simpele aanraking op de sleutel vervangt complexe inlogmethoden, wat zorgt voor snelle en eenvoudige authenticatie.
* **Multi-protocol ondersteuning:** Ondersteunt FIDO2, WebAuthn, OTP, en meer, waardoor het veelzijdig is voor verschillende use-cases.
* **Offline bescherming:** Kan ook worden gebruikt voor offline toepassingen zoals lokale inlog op werkstations.

# Doelstelling:

De doelstelling is om YubiKeys te implementeren als primair middel voor MFA binnen de organisatie om de beveiliging te verbeteren en het risico op phishingaanvallen aanzienlijk te verminderen.

# Beoordeling van de Huidige Omgeving

1. **Licentievereisten:**
   * Controleer of de organisatie beschikt over **Azure AD Premium P1 of P2** licenties voor Conditional Access en geavanceerde authenticatiemethoden.
2. **Ondersteunde hardware en software:**
   * Inventariseer welke werkstations, laptops, en mobiele apparaten YubiKeys ondersteunen. Let op de aanwezigheid van USB-A, USB-C, NFC, en Bluetooth voor compatibiliteit.
3. **Gebruikersinventaris:**
   * Maak een lijst van gebruikers die toegang hebben tot gevoelige applicaties en systemen, en bepaal voor welke gebruikers YubiKeys verplicht worden gesteld.

# Advies voor Implementatie van YubiKeys

## 1. Selectie van YubiKey-modellen:

| **Model** | **Beschrijving** | **Aanbevolen Gebruik** |
| --- | --- | --- |
| **YubiKey 5 NFC** | Ondersteunt USB-A en NFC | Laptops, smartphones |
| **YubiKey 5C** | Ondersteunt USB-C | Moderne laptops, tablets |
| **YubiKey Bio** | Ondersteunt vingerafdrukauthenticatie | Extra beveiliging |

**Advies:** Kies een mix van YubiKey 5 NFC en YubiKey 5C om een breed scala aan apparaten te ondersteunen.

## 2. Configuratie van Azure AD voor YubiKeys:

* Ga naar **Azure AD** > **Security** > **Authentication methods**.
* Schakel **FIDO2 Security Key** in als authenticatiemethode.
* Voeg de groepen gebruikers toe die gebruik gaan maken van YubiKeys.
* Stel het beleid in om YubiKeys te vereisen voor toegang tot kritieke applicaties via **Conditional Access**.

## 3. Uitgifte en distributie van YubiKeys:

* Zorg voor de aanschaf van voldoende YubiKeys (minimaal 2 per gebruiker: één primair en één reserve).
* Plan een uitgiftesessie waarbij medewerkers hun YubiKey ontvangen en direct registreren via **[https://myprofile.microsoft.com](https://myprofile.microsoft.com" \t "_new)**.
* Geef duidelijke instructies voor het opslaan van de reserve YubiKey op een veilige plek (bijvoorbeeld een kluis).

## 4. Training en bewustwording:

* Organiseer trainingssessies voor eindgebruikers om hen te begeleiden bij het gebruik van de YubiKey.
* Verspreid een gebruikershandleiding met stappen voor het instellen van de YubiKey, inclusief screenshots.

## 5. Pilot en testing:

* Voer een pilot uit met een kleine groep gebruikers (bijvoorbeeld IT en beveiligingsteams).
* Monitor de prestaties en verzamel feedback om eventuele problemen op te lossen voordat de uitrol naar de hele organisatie plaatsvindt.
* **Beheer en Onderhoud van YubiKeys**

## Verlies of diefstal:

* Zorg dat er een proces is voor het melden van verloren of gestolen YubiKeys.
* Laat gebruikers inloggen met hun reserve YubiKey of fallback-MFA-methode (bijv. Microsoft Authenticator-app).
* Blokkeer de verloren YubiKey in Azure AD via **Security Info**.

## Audit en rapportage:

* Monitor het gebruik van YubiKeys via Azure AD **Sign-in logs**.
* Controleer regelmatig of gebruikers de YubiKey blijven gebruiken en of er geen fallback-opties misbruikt worden.
* Gebruik **Conditional Access rapportages** om inzicht te krijgen in het gebruik van sterke authenticatiemethoden.

## Rotatie van sleutels:

* Adviseer om YubiKeys iedere 3 jaar te vervangen, of eerder indien deze beschadigd zijn.

# Risico's en Beperkingen

| **Risico** | **Maatregel** |
| --- | --- |
| **Verlies van YubiKey** | Gebruik van reserve YubiKey en fallback-MFA-opties. |
| **Hardware-incompatibiliteit** | Vooraf testen op verschillende apparaten. |
| **Gebrek aan gebruikersacceptatie** | Zorg voor uitgebreide training en communicatie. |

# Conclusie en Advies

Het implementeren van YubiKeys binnen de organisatie biedt een significante verbetering in beveiliging door phishing-resistente MFA. Wij adviseren om te starten met een pilotfase en vervolgens gefaseerd uit te rollen naar alle gebruikers. Door het combineren van sterke authenticatiemethoden en gebruikersbewustzijn zal de algehele beveiliging tegen inlogfraude aanzienlijk toenemen.