Multi-Faktor-Authentifizierung mit der Microsoft Authenticator App

Alle aus der Cloud erreichbaren Dienste sind besonders abzusichern, um einen Zugriff Dritter zu verhindern. Microsoft Produkte und Produkte, die an die Microsoft Services angebunden sind, werden über die AzureAD (den Microsoft Verzeichnisdienst) gesichert. Es reicht aber nicht aus, nur einen User und ein Passwort zu haben, denn diese Informationen können von Dritten ausgespäht werden und dann an anderer Stelle einfach verwendet werden. Liegt ein sogenannter weiterer Faktor vor, der im Moment des Logins verfügbar sein muss, kann man die Fremdnutzung verhindern. Was aber ist dieser weitere Faktor? Das kann eine App auf dem Smartphone sein, die einen mehrstelligen Code erzeugt, den man beim Login eintippt. So eine App kann auch so eingerichtet sein, dass man nur bestätigt, dass der Login gerade von mir kommt und gewollt ist. Hat man kein Smartphone, kann auch ein anderer Faktor verwendet werden. Hier wird aber zunächst nur die Einrichtung der App erläutert:

Neueinrichtung der Microsoft Authenticator App

Installation der Microsoft Authenticator App

Zunächst mal muss die App auf dem Smartphone installiert sein. Alle über das von MSP verwaltete MDM betriebenen Handys werden bereits mit der Microsoft Authenticator App ausgeliefert. Ist diese nicht vorhanden, kann die App über Apps@Work nachinstalliert werden. Ist das Smartphone nicht über das MDM verwaltet, kann die App auch manuell installiert werden. Dazu sucht man im App-Store von Apple oder Google nach der Microsoft Authenticator App. Diese hat aktuell folgendes Logo:

Die Links zu den Apps:

- iOS: https://apps.apple.com/de/app/microsoft-authenticator/id983156458
- Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=de&gl=US

Einrichtung der Microsoft Authenticator App

Ist die App installiert, ruft man den folgenden Link auf:

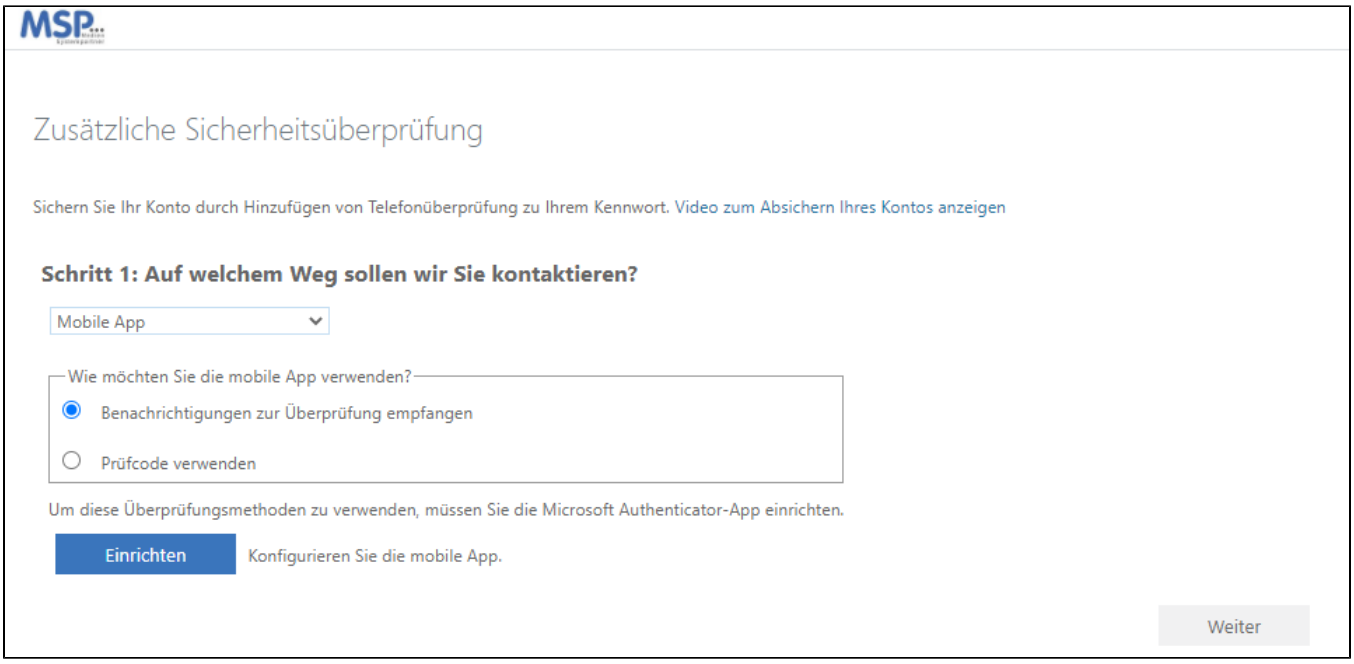
- https://aka.ms/mfasetup (Kurzlink)
- https://account.activedirectory.windowsazure.com/proofup.aspx?proofup=1

Nun meldet man sich mit den Windows Zugangsdaten (primäre E-Mail-Adresse und Windows Kennwort) an dem Portal an und klickt einmal auf Weiter:

Nun fragt der Einrichtungs-Dialog nach der Methode und den Daten. Vom Prinzip her ist jedes Verfahren, das hier angeboten wird, ausreichend sicher. Wir empfehlen aber folgendes Verfahren, da es am einfachsten im täglichen Betrieb ist:

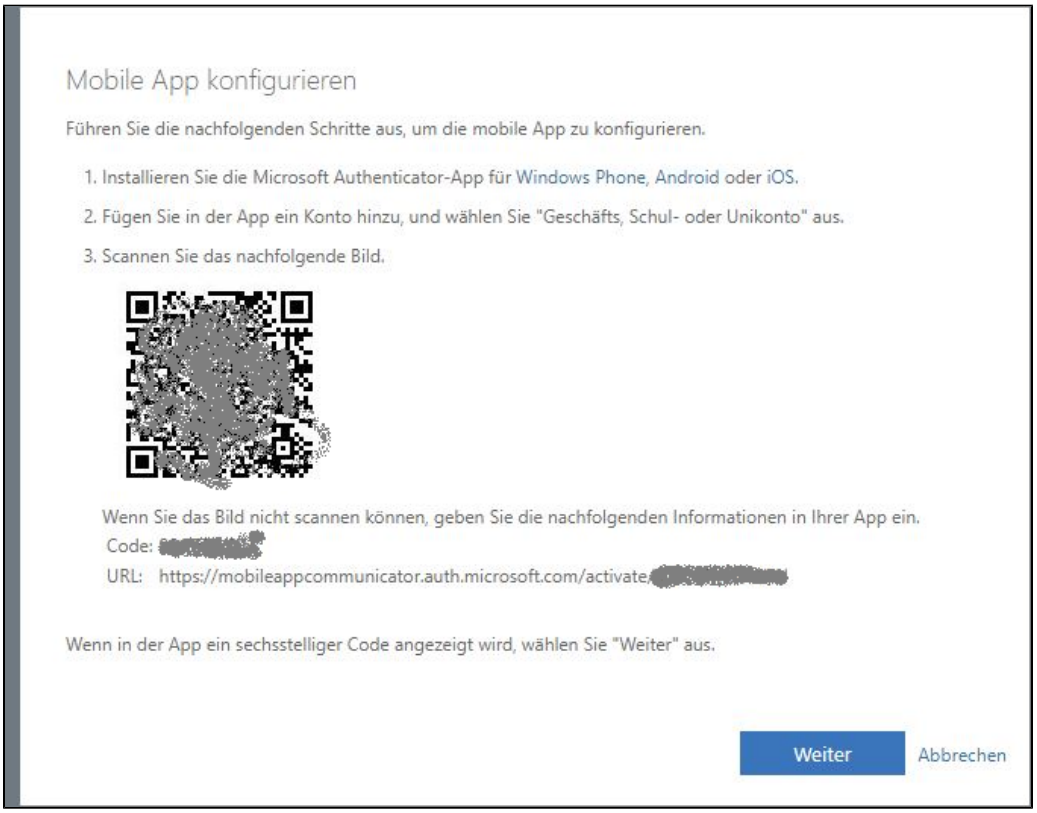
Schritt 1: Der Weg, auf dem die Autorisierung erfolgen soll

Die Mobile App soll eingerichtet werden und diese über eine Benachrichtigung aktiviert werden. Danach ein Klick auf Einrichten



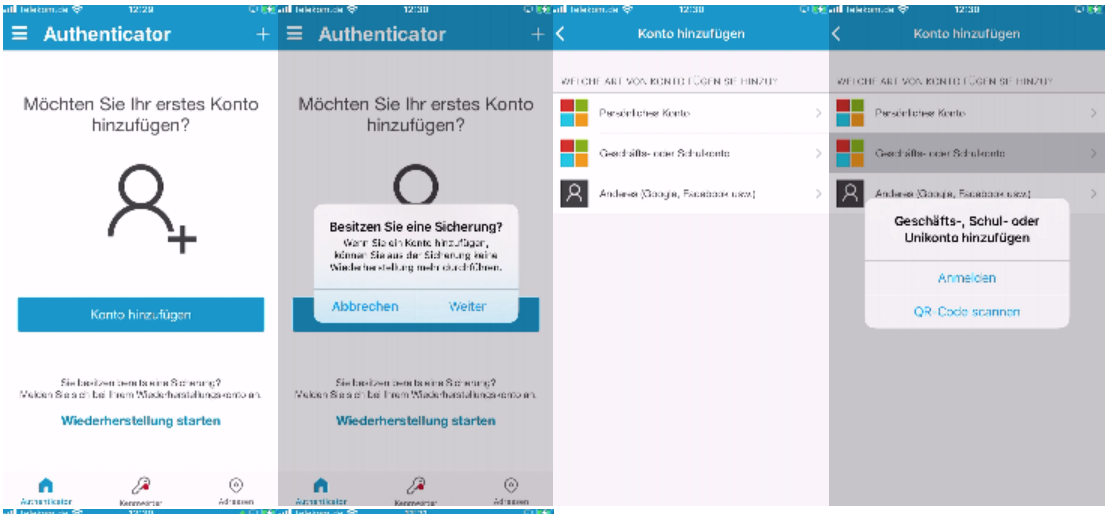
Schritt 2: App einrichten

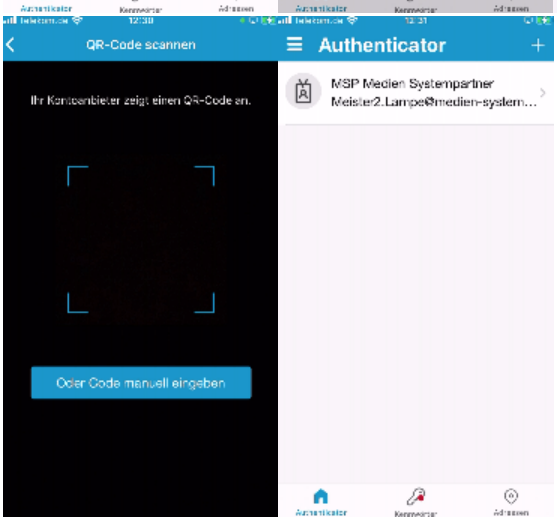
Es folgt ein Bildschirm wie dieser:



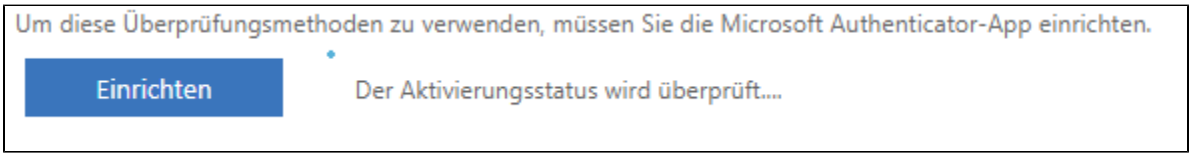
Nun wird die gerade installierte App aufgerufen,

- auf **Hinzufügen** (oder wenn schon ein Eintrag vorhanden ist, auf das Plus ⊕) geklickt
- ggf. noch bestätigt, dass keine Sicherung erfolgen muss
- die Verwendung eines Geschäfts- oder Schulkontos ausgewählt
- und der QR-Code eingescannt





Danach muss zügig in der Einrichtung auf dem PC auf Weiter geklickt werden:

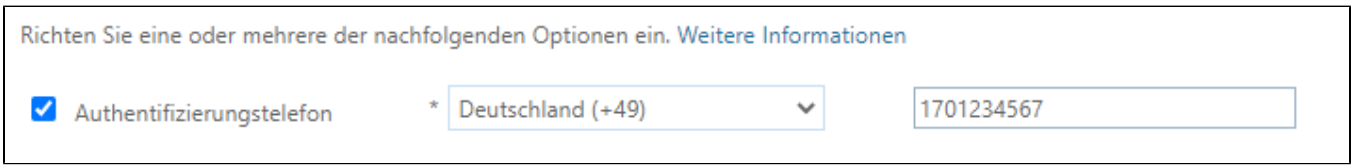


Und die Einrichtung ist abgeschlossen.

Es wird noch einmal geprüft, ob die Kommunikation mit der App funktioniert. Dazu muss einmal in der App bestätigt werden:

Schritt 3: Absicherung des Login

Es folgt eine Aufforderung noch die mobile Rufnummer zu hinterlegen um im Falle einer App Störung per SMS einen Code zu erhalten. Dieses ist wie folgt einzurichten:



Abschluss

Die Anmeldung an den AzureAD Diensten kann nun mit der Microsoft Authenticator App validiert werden. Sobald der Administrator die Anmeldung per MFA erzwingt, wird diese über die App abgefragt.

Empfehlung für die einfache Nutzung der App

Damit in der App nicht immer wieder der Gerätepin eingetippt werden muss, sollte aus Sicherheitsgründen ein biometrisches Verfahren zur Erkennung des Anwenders aktiviert sein (Einstellung im Gerätesetup).

Wiedereinrichtung der Microsoft Authenticator App

Sollte das Smartphone zusammen mit der Authenticator App verloren gegangen sein oder das Handy getauscht werden, kann man mit diesen Links die App neu einrichten:

- https://aka.ms/mfasetup (Kurzlink)
- https://account.activedirectory.windowsazure.com/proofup.aspx?proofup=1