Multi-Faktor-Authentifizierung (MFA) für Office 365 und weitere Produkte (neu)

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.

Das Grundprinzip der MFA

Das Grundprinzip einer MFA ist, dass man **etwas weiß und etwas hat**. Während man den Usernamen und das Kennwort als **Wissen** bezeichnet, muss man das Smartphone mit der App oder den Hardware-Token **haben**. Ein Angreifer, der die Zugangsdaten, bestehend aus Username und Kennwort, abgegriffen (Phishing) hat oder ein Dieb das Smartphone oder den Token geklaut haben kann, hat immer noch nicht beides. Somit erhöht sich die Sicherheit durch dieses Prinzip.

Was genau gilt aktuell als zweiter Faktor in Bezug auf die MFA?

Als zweiter Faktor, also neben dem Wissen, wird aktuell die Authenticator App, ein Hardwaretoken oder der Standort bzw. das Unternehmensnetzwerk bzw. der Unternehmensstandort akzeptiert.

Welche Faktoren werden aktuell unterstützt?

- Die **App auf dem Smartphone**, wird beim Login über das Internet angestoßen und fragt nach einem zweistelligen Code, den man auf der Webseite oder in der App angezeigt bekommt.
- Der **Hardware-Token** erzeugt alle 60 Sekunden einen 6-stelligen Code, den man beim Login eintippt.
- Ist man mit dem **Unternehmensnetz** physisch oder logisch bereist verbunden, gilt das auch als 2. Faktor. Das gilt immer dann, wenn man mit dem Gerät im Büro im LAN oder im WLAN ist. Aber auch wenn man bereits per VPN mit dem Unternehmen verbunden ist, gilt das als sicherer Standort. Aus diesem Grund werden wir im Laufe des 4. Quartals 2023 und des ersten Quartals 2024 nach und nach auch beim Login in das VPN-Netzwerk den zweiten Faktor App oder Hardware-Token einführen.

Auf diesem Weg wird sichergestellt, dass der Login auch wirklich vom Nutzer erfolgt und gewollt ist.

Wann greift MFA?

Damit man nicht jeden Tag bzw. alle paar Stunden sich wieder neu autorisieren muss, wird der zweite Faktor alle 14 Tage einmal je App und Gerät abgefragt. In der Zwischenzeit muss man sich, insbesondere auf den mobilen Apps, nicht immer wieder neu anmelden. Nach Ablauf der 14 Tage erfolgt eine erneute Abfrage. Ist man aber immer wieder im Unternehmensnetzwerk angemeldet, gilt das ja auch als zweiter Faktor, und damit kann bei der Anmeldung, auch erst nach mehr als 14 Tagen, der zweite Faktor wieder erforderlich sein.