Multi-Faktor-Authentifizierung (MFA)

Publiziert it-support@fhnw.ch Übersichtseite Benutzerdokumentation

Diese Übersichtsseite weist auf alle notwendigen Informationen rund um die Multi-Faktor-Authentifizierung des FHNW-Accounts hin.

Was bedeutet Multi-Faktor Authentifizierung?

Die **M**ulti-**F**aktor-**A**uthentifizierung (MFA) ist ein Authentifizierungsverfahren, bei dem die Benutzenden zwei oder mehr Identitätsnachweise (Faktoren) zur Verifizierung liefern müssen, bevor sie Zugriff auf die gewünschte Ressource erlangen, beispielsweise auf eine Anwendung, ein Benutzerkonto oder ein VPN. Statt nur einen Benutzernamen und ein Kennwort abzufragen, erfordert die MFA zusätzliche Identitätsnachweise, so dass das Risiko eines erfolgreichen Cyberangriffes massiv reduziert werden kann.

Warum ist die MFA wichtig?

Da Benutzende beim Zugriff auf Anwendungen neben ihrem Benutzernamen und Kennwort weitere Identitätsnachweise erbringen müssen, steigt die Sicherheit für das Unternehmen der FHNW – ein wesentlicher Vorteil der MFA. Cyberkriminelle haben es somit deutlich schwerer, auf vertrauliche Daten und Anwendungen zuzugreifen.

Welche Faktoren können verwendet werden?

- Microsoft Authenticator-App (im Apple Store oder Google Play erhältlich) (empfohlen von der FHNW)
- alternative Authenticator Apps wie Google Authenticator, Authy, LastPass Authenticator
- Windows Hello for Business
- FIDO2 Security Key oder OATH-Hardwaretoken (Token2 oder Yubikey) (kostenpflichtig)

Folgende Faktoren werden für Neuregistrierungen nicht unterstützt:

- Anruf
- SMS

Einrichtung von Multi-Faktor-Authentifizierung für den FHNW-Account

Es wird empfohlen die einmalige Registration von MFA in einem separaten Browserfenster (Inkognito / privates Browser Fenster) zu machen und nicht in einer Office 365 App wie Teams.

Öffnen Sie den Browser und melden Sie sich auf https://office.com mit Ihrer FHNW E-Mail-Adresse an und befolgen die Anweisungen des Assistenten, um das Konto zu schützen.

Eine detaillierte Anleitung ist in folgendem Help-Artikel zu finden: FHNW Account mit Multi-Faktor-Authentifizierung (MFA) verbinden | FHNW Help

Verwalten von (registrierten) Multi-Faktoren

Die Verwaltung erfolgt über folgende Webseite: https://myaccount.microsoft.com/ oder https://aka.ms/mysecurityinfo

Darin können Sie unter «Sicherheitsinformationen» die erfassten Faktoren von Ihrem Account verwalten. So können Sie beispielsweise bei einem neuen Smartphone das Microsoft Authenticator App neu registrieren lassen.

Eine detaillierte Anleitung ist in folgendem Help-Artikel zu finden: Aktualisierung von Multi-Faktor-Authentifizierungsinformationen des FHNW-Accounts | FHNW Help

FAQ rund um Multi-Faktor-Authentifizierung

Das FAQ beantwortet die meist gestellten Fragen rund um MFA.

FAQ: Multi-Faktor-Authentifizierung FHNW-Account | FHNW Help

Weiter zu Einrichten von Multi-Faktor-Authentifizierung -->

Nützliche Links

MFA Dokumentation von Microsoft: Übersicht über die Microsoft Entra-Multi-Faktor-Authentifizierung - Microsoft Entra ID | Microsoft Learn

Videoanleitung von Microsoft (Englisch): Set up multi-factor authentication (MFA)

Verwandte Artikel

- FAQ: Multi-Faktor-Authentifizierung FHNW-Account
- Authentifizierungsfaktor bei MFA wechseln
- FHNW Account, MFA Multi-Faktor-Authentifizierung - Ersteinrichtung

publiziert: 28. Februar 2024 22:25 Service: S1309 - IT Infrastruktur Basisdienste (AD | Entra ID | SCEP | Entra Application Proxy)