Weiterbildung in Baden-Württemberg

Kurzanleitung

Einrichtung und Nutzung der Zwei-Faktor-Authentifizierung (2FA) für Teilnehmer des Weiterbildungsportals.

1. Einleitung

Ab sofort bietet das Weiterbildungsportal Baden-Württemberg für alle Logins eine erhöhte Sicherheit durch eine Zwei-Faktor-Authentifizierung (2FA) an. Dies betrifft den Login aller Weiterbildungsträger, Referenten, organisatorisch eingebundene Personen und Besucher.

Mit der Aktivierung von 2FA benötigt der Nutzer zum Login zusätzlich zu seinem Kennwort noch ein weiteres Sicherheitsmerkmal in Form einer sechsstelligen Nummer, ähnlich wie die aus dem Online-Banking bekannten Transaktionsnummern (TAN). Diese Nummer, auch TOTP (*Time Based One-Time Pad*) genannt, erhält der Nutzer wahlweise per E-Mail an seine Login-Adresse oder über eine App auf seinem Smartphone. Diese Authenticator-App existiert bereits von mehreren Anbietern und kann kostenlos aus dem jeweiligen App-Store heruntergeladen und auf dem Smartphone installiert werden. Voraussetzung für die Nutzung der 2FA ist im letzteren Fall also ein Smartphone.

Es gibt zahlreiche Authenticator-Apps von verschiedenen Anbietern. Eine Empfehlung wird nicht abgegeben, wir haben das Verfahren mit folgenden Apps erfolgreich getestet: Google Authenticator, Microsoft Authenticator, 2Fa Authenticator (2FAS) und Twilio Authy Authenticator. Generell ist jede TOTP-kompatible Authenticator App geeignet.

2. Einrichtung des 2FA-Login

Standardmäßig ist 2FA für ein Benutzerkonto deaktiviert. Ein entsprechender Hinweis in dem persönlichen Dashboard weist auf die Möglichkeit der Nutzung von 2FA hin. Zur Einrichtung klicken Sie bitte auf diesen Hinweis, alternativ gelangen Sie auch über das Menü „Benutzerkonto => „Anmeldedaten“.

Auf der Seite „Anmeldedaten“ scrollen Sie bitte runter bis zu dem Abschnitt „Zwei-Faktor-Authentisierung (2FA)“. Aktivieren Sie die Option 2FA.

Nun können Sie das gewünschte Verfahren für Ihren zweiten Faktor auswählen.

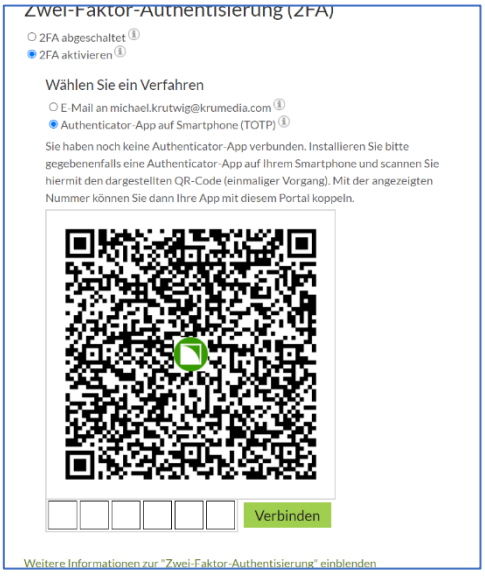
2.1. Verfahren: E-Mail

Sowohl beim Einrichten als auch zukünftig beim Login wird Ihnen eine 6-stellige „TAN“ per E-Mail an Ihre Adresse gesendet. Eine von Ihrem Login abweichende E-Mail kann nicht gewählt werden.

Bitte wählen Sie dieses Verfahren, wenn Sie jederzeit Zugriff auf Ihr Postfach haben und wenn Sie kein weiteres Gerät benutzen wollen.

2.2. Verfahren: Authenticator-App (mit dem Smartphone)

Als Voraussetzung installieren Sie bitte eine TOTP-kompatible App auf Ihrem Smartphone (siehe Anleitung). Die Aktivierung des Verfahrens ist relativ einfach:



Starten Sie die App auf Ihrem Smartphone und scannen Sie den QR-Code. Die App wird Sie durch diesen Prozess durchführen.

Laden Sie die „Recovery Codes“ herunter und legen Sie diese in einem gesicherten Verzeichnis auf Ihrem Rechner ab. Dieser Code wird nur benötigt, falls Sie keinen Zugang mehr zu Ihrem Smartphone haben sollten.

Geben Sie dann den 6-stelligen, von Ihrer App erzeugten Code in das entsprechende Feld ein und klicken Sie auf „Activate“.

Dieses Verfahren ist, zumindest längerfristig, die bessere Wahl, da Ihre Authenticator-App nicht nur für das Weiterbildungsportal, sondern für alle Logins mit 2FA und TOTP genutzt werden kann.

Nun haben Sie Ihren Login mit einem zweiten Faktor abgesichert. Die Nutzung von 2FA kann jederzeit wieder deaktiviert werden.

3. Nutzung des 2FA-Login

Die Nutzung von 2Fa ist denkbar einfach, halten Sie bitte – je nach gewähltem Verfahren - Ihr E-Mail-Programm oder Ihr Smartphone griffbereit:

Loggen Sie sich mit Ihrer Nutzerkennung und Ihrem Kennwort wie gewohnt ein. Nach Eingabe dieser Daten müssen Sie nun den 6-stelligen Zahlencode eingeben, den Sie über Ihre Authenticator App oder per E-Mail zeitgleich erhalten haben.