

Sicherheitsmechanismen

Einsatz von Sicherheitsmechanismen

Bereich	Personengruppe	Benutzername und Passwort	Sicheres Gerät	2FA	PIN
Allgemeiner interner Bereich z. B. - Dashboard - Meine Daten - Interaktionen - Aktivitäten (Übungen)	alle	Pflicht	optional	optional	optional
Daten von Dritten (Feuerwehrangehörige)	Gesamtkommando o Abteilungskommando Schriftführer	Pflicht	optional	Pflicht	optional

Bedeutung und Auswirkung der Maßnahmen

Benutzername und Passwort	Wird zum allgemeinen Login benötigt. Grundsätzlich bleibt der Login aktiv, solange Cookies gespeichert bleiben und keine Abmeldung erfolgt.
----------------------------------	---

<p>Sicheres Gerät</p>	<p>Browser werden identifiziert und gespeichert. Besucht man die Seite mit einem registrierten Browser, ist man ohne erneute Eingabe von Benutzername und Passwort unmittelbar angemeldet. Diese Methode ist nur zulässig für Geräte mit eigenem Schutzmechanismus (z. B. Passwort, PIN, biometrische Erkennung).</p> <p>Das Sichere Gerät erlaubt den Zugriff auf alle Bereiche, auf denen keine Daten von Dritten enthalten sind. In Bereichen mit Daten von Dritten, ist auch weiterhin die Authentifizierung mit 2FA notwendig.</p> <div style="background-color: #fce4d6; padding: 10px; border: 1px solid #ccc;"> <p>Nur persönliche Geräte dürfen als sichere Geräte registriert werden. Geräte mit allgemeinem Zugriff (z. B. PC in der Zentrale, öffentlich zugängliche Geräte) dürfen nicht als sichere Geräte registriert werden.</p> </div>
<p>2FA</p>	<p>Die 2-Faktor-Authentifizierung ist Pflicht in allen Bereichen, in denen Daten Dritter einsehbar sind. Wo nur die eigenen Daten einsehbar sind, ist die 2-Faktor-Authentifizierung nicht Pflicht, kann aber optional aktiviert werden.</p> <p>Der zweite Faktor ist ein Link, der an die eigene E-Mail-Adresse gesendet wird. Erst nach dem Öffnen des Links wird die gewünschte Seite geöffnet. Der E-Mail-Link kann auch auf einem anderen Gerät geöffnet werden.</p> <p>Die Authentifizierung gilt 36 Stunden lang und läuft dann ab. Besucht man in diesen 36 Stunden die Seite erneut, verlängert sich der Zeitraum.</p> <p>Die Authentifizierung mit dem 2. Faktor ist auch bei aktivem sicherem Gerät durchzuführen, wenn sie aktiv ist (verpflichtend oder freiwillig).</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #ccc;"> <p>Die 2-Faktor-Authentifizierung ist an den Browser gebunden, mit dem die auslösende Seite aufgerufen wurde. Daher kann es bei späterer Verwendung eines anderen Browsers bzw. eines anderen Geräts noch einmal zur 2FA-Verifizierung kommen. Gleiches gilt, wenn Cookies nicht gespeichert bzw. gelöscht werden.</p> </div>
<p>PIN</p>	<p>An öffentlichen Geräten der Feuerwehr können sich Anwender mit einer PIN anmelden. Dadurch entfällt die Eingabe komplexer Passwörter bei Geräten, die in geschlossenen Bereichen der Feuerwehr sind (z. B. Feuerwehrhaus). Voraussetzungen für den Einsatz des PIN-Verfahrens sind:</p> <ul style="list-style-type: none"> • Der Anwender hat für sich eine PIN eingerichtet. (Website-Bereich Meine Daten -> Persönliche Einstellungen) • Das Gerät wurde von der Feuerwehrführung für die Verwendung des PIN-Verfahrens registriert.

Revision #6

Created 2025-05-01 10:23:41 UTC by Marco Morath

Updated 2025-06-09 19:22:56 UTC by Marco Morath