

12.12.2024

Multi-Faktor-Authentifizierung und Passkeys

Im digitalen Umfeld ist der Schutz von Benutzerkonten entscheidend. Multi-Faktor-Authentifizierung (MFA) bietet hier mehr Sicherheit als herkömmliche Passwörter, indem sie mehrere Sicherheitsfaktoren kombiniert.

Multi-Faktor-Authentifizierung (MFA) ist eine Sicherheitsmethode, die aktuell am ehesten unter dem Unterbegriff Zwei-Faktor-Authentifizierung (2FA) bekannt ist. MFA ist umfassender und beschreibt alle Authentifizierungsmethoden, die zwei oder mehr Sicherheitsfaktoren benötigen. Dabei werden Authentifizierungsfaktoren wie Wissen (z. B. Passwort), Besitz (z. B. Smartphone) und Zugehörigkeit (z. B. Fingerabdruck) kombiniert. Das Ziel ist, eine mehrschichtige Verteidigung zu schaffen und damit Benutzerkonten vor den häufigsten Bedrohungen wie Phishing und Passwortdiebstahl besser zu schützen.

MFA löst dabei zentrale Sicherheitsprobleme: Selbst, wenn ein Passwort, also ein Faktor, gestohlen oder kompromittiert wird, bleibt der Zugang für Angreifende gesperrt, da die weiteren Faktoren fehlen. Die Kombination verschiedener Sicherheitsfaktoren erhöht das Schutzniveau deutlich und ist heutzutage unverzichtbar.

Ein neuer Ansatz für eine einfachere, benutzerfreundlichere Authentifizierungstechnologie ist der [Passkey](https://www.ebas.ch/passkeys/) (<https://www.ebas.ch/passkeys/>). Passkeys sollen traditionelle Passwörter vollständig ersetzen und beruhen auf sicheren Authentifizierungsmethoden wie biometrischen Merkmalen. In der Passkey-Technologie ist MFA bereits integriert. Anstelle eines Passworts verwendet der Nutzer ein biometrisches Merkmal oder eine PIN auf seinem Gerät, wobei der private Schlüssel sicher auf dem Gerät bleibt und niemals übertragen wird. Passkey stärkt den Passwortaspekt des Logins an sich und fügt nicht eine weitere Sicherheitsschicht durch einen weiteren Authentifikationsfaktor hinzu.

Lesen Sie mehr dazu in unserem Artikel zu [Passkeys](https://www.ebas.ch/passkeys/) (<https://www.ebas.ch/passkeys/>).