Mehr-Faktor-Authentisierung

Die Multi-Faktor-Authentifizierung (MFA), auch Multi-Faktor-Authentisierung, ist eine Verallgemeinerung der Zwei-Faktor-Authentisierung (2FA), was Sie vermutlich schon aus dem privaten Umfeld von Banking-Anwendungen oder der Steuererklärung kennen:

Statt nur ein Benutzername und Passwort zur Anmeldung an einem Dienst zu nutzen, werden weitere Faktoren oder eine Kombination aus Faktoren überprüft. Diese lassen sich grob in verschiedene Kategorien einordnen, wobei idealerweise zwei unterschiedliche Kategorien von Faktoren verwendet werden sollen:

- Wissen (z.B. Passwort, Geheimnisse)
- Besitz (z.B. Hardware-Token, Chipkarte)
- Inhärenz (z.B. Biometrie, Fingerabdruck usw.)
- Ort (z.B. über GPS oder Netzwerkadresse ermittelt)

Die Pädagogische Hochschule Freiburg strebt laut Leitlinie zur Informationssicherheit mindestens eine Standardabsicherung nach BSI Grundschutz an. Nach ORP.4 sollten „Benutzendenkennungen mit weitreichenden Berechtigungen“ über Mehr-Faktor-Authentisierung abgesichert werden. Damit sind nicht nur technische Administratoren, sondern insbesondere auch nicht-technische Funktionsträger (und damit perspektivisch alle Mitarbeitenden) gemeint.

In unser 360°-Sicherheitsanalyse wurde uns als eine der Kernbotschaften auferlegt, dass eine „Absicherung extern erreichbarer Zugänge mit einem zweiten Faktor“ unverzüglich umzusetzen ist. Zudem hat das LKA aufgrund der vermehrt auftretenden erfolgreichen Phishing-Vorfälle die Aktivierung von MFA für alle Accounts strengstens empfohlen. Das ZIK wird daher kontextuell (z.B. Ort, verdächtige Anmeldeverhalten und -uhrzeiten) und gestuft nach Dienst und Personengruppen MFA-Optionen anbieten und verpflichtend machen. Die aktuellen Vorgaben sind wie folgt:

- Für alle MFA-aktivierten Dienste muss mindestens ein zweiter Faktor hinterlegt sein.
- Ein zweiter Faktor wird in der Regel alle 20 Tage verpflichtend abgefragt.
- Je nach Dienst kann die Nutzungszeit auf maximal 30 Tage erhöht werden.
- Einzelne Dienste können ggf. häufiger oder gar immer einen zweiten Faktor anfordern, z.B. wenn sie besonders schützenswert sind oder der Account ein auffälliges Nutzungs- und/oder Anmeldeverhalten zeigt (z.B. viele Anmeldungen aus unterschiedlichen Netzen).
- Der Zugang von externen Netzen (insbesondere aus dem Ausland) ist entweder mit VPN oder unter Verwendung eines zweiten Faktors bei jeder Anmeldung möglich.
- Die Einführung verläuft gestaffelt, beginnend mit dem ZIK. Es folgen weitere Testnutzer und dann Funktionsträger sowie auffällige Accounts. Zeitnah werden wir alle Mitarbeitenden und Studierenden verpflichtend abdeckend.

Aktuell verwenden verschiedene Softwareprodukte teils konkurrierende Verfahren, der IT-Planungsrat standardisiert den Technologierahmen bzgl. MFA allerdings auf folgende Technologien: Open Authorization (OAuth), OpenID Connect (OIDC), JSON Web Token (JWT), One-Time Password (OTP) für Multi-Faktor-Authentifizierung (MFA). Das ZIK ist bestrebt basierend auf diesen Technologien eine einheitliche Lösung nachzureichen. Zeitbasierte Einmal-Passwörter (Time-Based One-Time-Passwords, kurz TOTP) sind eine durch die Initiative For Open Authentication in RFC6238 genormtes Verfahren zum Erzeugen eines zweiten Faktors. Als standardisiertes Verfahren können Sie hier verschiedene TOTP-Apps (z.B. Apple Passwords, Aegis Authenticator, Google Authenticator oder FreeOTP+) oder

Desktop-Anwendungen (z.B. KeepassXC) verwenden. Allerdings erfordern bestimmte Dienste stärkere, technisch nicht sichere Faktoren, sodass wir diese – wo bereits in Verwendung – ebenfalls dokumentieren.

Anleitungen

Anleitung für Mitarbeitende

Mitarbeitende der PH werden in der Regel sobald ein Dienst MFA-aktiviert wurde über Cisco Duo – die bestehende Lösung, die auch für VPN-MA genutzt wird – angeschlossen. Zusätzliche zweite Faktoren wie DuoPush, Hardwareschlüssel/Yubikeys oder Softwareschlüssel/Passkeys lassen sich über das myID-Portal hinterlegen. Danach können Sie Duo (und alle dort hinterlegen Faktoren) zur Einrichtung folgende Authentisierungsdienste nutzen:

Microsoft Login (Entra)

- Die Einrichtung eines zweiten Faktors für den Microsoft Account bzw. für Dienste, die über Microsofts Entra-Dienst angebunden sind wird auf der Wiki-Seite zu MS Office beschrieben.

PH Login (Keycloak)

- Derzeit verwendet noch für Studierende zugänglicher Keycloak-Dienst einen zweiten Faktor.

PH Login (Shibboleth)

- Derzeit verwendet noch kein Shibboleth-Dienst einen zweiten Faktor.

Einige Dienste, wie der EU-Login sind nicht an das IDM angeschlossen und benötigen daher eine gesonderte Einrichtung eines zweiten Faktors.