Demnächst auch im Portal meineBLÄK

# Warum Zwei-Faktor-Authentifizierung heute notwendig ist

*Viele Menschen kennen das Gefühl: Noch ein Passwort. Noch eine Sicherheitsabfrage. Und jetzt zusätzlich auch noch eine Zwei-Faktor-Authentifizierung (2FA). Auf den ersten Blick wirkt das wie ein weiterer Schritt, der Zeit kostet und den Alltag komplizierter macht. Doch die Realität im digitalen Raum hat sich in den vergangenen Jahren stark verändert – und damit auch die Anforderungen an Sicherheit.*

Cyberangriffe treffen heute längst nicht mehr nur große Konzerne oder Banken. Auch Portale von Verbänden, Unternehmen oder öffentlichen Einrichtungen geraten zunehmend ins Visier. Der Grund ist einfach: Persönliche Daten sind wertvoll und gerade für Ärztinnen und Ärzte hat der Schutz digitaler Konten eine besondere Bedeutung. Auch wenn in einem Portal keine unmittelbaren Patientendaten gespeichert sind, können zum Beispiel berufliche Informationen oder Kontaktdaten verändert oder missbraucht werden. Zudem besteht die Gefahr, dass Angreifer im Namen der betroffenen Person auftreten. Vor dem Hintergrund der ärztlichen Verantwortung und der hohen Anforderungen an Vertraulichkeit ist ein zusätzlicher Schutzmechanismus daher besonders wichtig.

Viele Angriffe beginnen mit einem gestohlenen Passwort, beispielsweise durch ein Datenleck bei anderen Diensten oder Portalen.

Passwörter gelten seit Jahrzehnten als Standard für den Zugang zu digitalen Diensten. Doch sie haben eine entscheidende Schwäche: Menschen verwenden häufig einfache Passwörter, nutzen dasselbe Passwort mehrfach oder werden Opfer von Datenlecks. Gelangen Zugangsdaten einmal in falsche Hände, probieren Angreifer diese automatisiert auch bei anderen Plattformen aus – oft mit Erfolg.

## Genau hier setzt die Zwei-Faktor-Authentifizierung an

Das Prinzip ist einfach: Neben dem Passwort wird ein zweiter Nachweis verlangt – zum Beispiel ein Bestätigungscode per E-Mail, auf dem Smartphone oder die Freigabe über eine sogenannte Authenticator-App. Selbst wenn ein Passwort bekannt wird, reicht es allein nicht mehr aus, um Zugriff auf ein Konto zu erhalten. Der zweite Faktor funktioniert wie ein zusätzlicher Sicherheitsschlüssel. Oft wird dieses Prinzip als Kombination aus „etwas, das ich weiß" (Passwort) und „etwas, das ich besitze" (zum Beispiel Smartphone) beschrieben.

Wichtig ist dabei: Zwei-Faktor-Authentifizierung schützt nicht nur die Plattform selbst, sondern vor allem die Nutzerinnen und Nutzer. Denn kompromittierte Konten können erhebliche Folgen haben und das Vertrauen in digitale Dienste beschädigen. Häufig bleibt ein Missbrauch lange unbemerkt.

Allerdings bietet auch ein zweiter Faktor keinen vollständigen Schutz. Risiken bestehen beispielsweise, wenn Angreifer Zugriff auf das E-Mail-Postfach haben oder versuchen, Nutzer durch Täuschung zur Preisgabe eines Codes zu bewegen. Dabei geben sich die Angreifer gerne als IT-Dienstleister, Kammer oder bekannte Institution aus. Geben Sie daher Ihren zweiten Faktor niemals telefonisch weiter und achten Sie stets auf die korrekte Internetadresse in der Browserzeile. Außerdem ist eine Authenticator App – sofern möglich – einem E-Mail-Code gegenüber zu bevorzugen.

Gleichzeitig zeigen Erfahrungen vieler großer Online-Dienste, dass Zwei-Faktor-Authentifizierung hochwirksam ist. Ein Großteil automatisierter Kontoübernahmen scheitert bereits am fehlenden zweiten Faktor. Deshalb setzen inzwischen Banken, Versicherungen, E-Mail-Anbieter und zunehmend auch Behörden auf dieses Verfahren. Auch empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausdrücklich das Einrichten eines zweiten Faktors dort, wo es möglich ist.

Natürlich bedeutet die Einführung zunächst eine kleine Umstellung. Doch moderne Lösungen machen die Nutzung heute deutlich einfacher als noch vor einigen Jahren. Häufig genügt ein kurzer Blick aufs Smartphone oder eine Bestätigung per App. Der zusätzliche Aufwand beträgt meist nur wenige Sekunden – der Sicherheitsgewinn ist dagegen enorm.

Demnächst wird die Zwei-Faktor-Authentifizierung daher verbindlich im Portal *meineBLÄK* eingeführt, um ein einheitlich hohes Sicherheitsniveau Ihrer Daten zu gewährleisten. Dieser Schritt dient nicht der Erschwerung der Nutzung, sondern dem Schutz aller Beteiligten. In einer Zeit zunehmender Cyberangriffe ist Sicherheit keine optionale Zusatzfunktion mehr, sondern eine notwendige Grundlage für vertrauensvolle digitale Dienste.

Denn letztlich gilt: Das sicherste Passwort ist nur dann wirklich sicher, wenn es nicht allein über den Zugang entscheidet.

*Fabian Niggemann –*
*Experte für IT-Sicherheit (BLÄK)*