Abgeordnetenhaus BERLIN

Drucksache 19 / 25 618
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 20. März 2026 (Eingang beim Abgeordnetenhaus am 23. März 2026)

zum Thema:

Multi-Faktor-Authentifizierung (MFA) in Berlin: Mehr als nur Passwort12345?

und **Antwort** vom 9. April 2026 (Eingang beim Abgeordnetenhaus am 13. Apr. 2026)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Stefan Ziller (GRÜNE)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/25618
vom 20. März 2026
über Multi-Faktor-Authentifizierung (MFA) in Berlin: Mehr als nur Passwort12345?

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche sicheren Authentifizierungsmethoden (z.B. SMS-TAN, Hardware-Token, App-basierte TAN, biometrische Verfahren) stehen den Mitarbeiter*innen der Berliner Verwaltung und nachgeordneten Behörden zur Verfügung, um sich in die IT-Systeme der Berliner Verwaltung einzuloggen?

2. Wie verbreitet ist die Verwendung von Multi-Faktor-Authentifizierung (MFA) in der Berliner Verwaltung und den nachgeordneten Behörden, um sich sicher für IT-Systeme zu authentifizieren?

Zu 1. und 2.: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt für eine sichere Authentifizierung mehrere Faktoren zu kombinieren, um potentiellen Angreifern den Zugriff in Systeme zu erschweren. Diese Multi-Faktor-Authentifizierung gibt es in zahlreichen Varianten. Dabei bieten vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit. Im Land Berlin ist flächendeckend mindestens die Zwei-Faktor-Authentifizierung im Einsatz. Für Behörden und Einrichtungen der Berliner Verwaltung, die an das Berliner Landesnetz angeschlossen sind, gelten die Vorgaben des BSI-Standards 200-x einschließlich des IT-Grundschutz-Kompendiums in der jeweils gültigen Fassung. Um

Angreifern keine potentiellen Angriffsvektoren zu bieten, wird auf eine detaillierte Aufstellung mit verwendeten Authentifizierungsmethoden in der Berliner Verwaltung und den nachgeordneten Behörden verzichtet.

3. Nach welchen Kriterien wird in der Berliner Verwaltung und in nachgeordneten Behörden entschieden, welche Authentifizierungsmethode für die jeweiligen IT-Systeme, Software oder Fachverfahren eingesetzt werden?

Zu 3.: Gemäß EU-NIS-2-Richtlinie sind besonders wichtige und wichtige Einrichtungen zur Verwendung einer Multi-Faktor-Authentisierung oder einer kontinuierlichen Authentifizierung sowie zur Absicherung der Kommunikationswege von Sprache, Video und Text verpflichtet. Zudem gelten für Behörden und Einrichtungen der Berliner Verwaltung, die an das Berliner Landesnetz angeschlossen sind, die Vorgaben gem. BSI IT-Grundschutz. Des Weiteren werden internationale Standards und hardware-basierte Standards für MFA herangezogen. Die dargestellten Optionen für Einmalpasswörter (OTP-/TAN-Methoden) weisen normalerweise keine Widerstandsfähigkeit gegen (Echtzeit-)Phishing auf. Daher ist ihre Empfehlung nur eingeschränkt möglich.

4. Welche Voraussetzungen in Sachen Authentifizierungsmethoden müssen zur Einführung des National-Once-Only-Technical-System (NOOTS) als Architektur zur Registermodernisierung erfüllt werden?

Zu 4.: Der Entwurf der NOOTS-NetzV setzt die sicherheitstechnischen Anforderungen sowie die Anschlussklassen fest, welche sich aus den jeweils geltenden Fassungen der Technischen Richtlinien TR-03176 und TR-03190 des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergeben.

5. Gibt es (IT-Sicherheits-)Ziele für die Berliner Verwaltung in Sachen Multi-Faktor-Authentifizierung (MFA)?

Zu 5.: Mittels einer sorgfältig konzipierten und umgesetzten MFA werden die Angriffsmöglichkeiten von Angreifern und Cyberkriminellen stark eingeschränkt und das Risiko für eine erfolgreiche Kompromittierung der Zugänge stark reduziert. Ziel ist, eine Phishing-Resistenz durch technische Lösungen und ein sachgerechtes Awareness-Niveau bei den Beschäftigten herzustellen. Weitere Unterstützungsleistungen sind die in 2026 geplante Einführung einer landesweiten PKI und verbindlicher Richtlinien hinsichtlich Authentifizierungsverfahren, Passwörtern usw., die die stetige Weiterentwicklung des Informationssicherheitsniveaus des Landes Berlin umsetzen.
Die (IT-Sicherheits-)Ziele werden stetig evaluiert und weiterentwickelt.

Berlin, den 09. April 2026

Der Regierende Bürgermeister von Berlin
In Vertretung

Matthias Hundt
Staatssekretär für Digitalisierung
und Verwaltungsmodernisierung / CDO