LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/6179**
8. Wahlperiode **14.01.2026**

ANTRAG

der Gruppe der FDP

Funktionsfähigkeit und Sicherheit der Landespolizei wiederherstellen

Der Landtag möge beschließen:

I. Der Landtag stellt fest:

1. Die Landespolizei Mecklenburg-Vorpommern sieht sich seit dem Cyberangriff auf die Infrastruktur der dienstlichen mobilen Endgeräte mit erheblichen Funktionseinschränkungen konfrontiert.

2. Die Unbrauchbarkeit moderner mobiler Dienstgeräte beeinträchtigt die polizeiliche Effizienz bei Routineaufgaben wie Identitäts- und Fahrzeugabfragen, den Informationsfluss im Einsatz sowie die digitale Dokumentation, was die innere Sicherheit und das Sicherheitsgefühl der Bevölkerung negativ beeinflusst.

3. Die Digitalisierung der Polizei ist nicht nur eine technische Modernisierung, sondern auch zentraler Bestandteil einer bürgernahen, effektiven Sicherheitsbehörde. Langandauernde Ausfälle von digitalen Diensten untergraben das Vertrauen der Bevölkerung in die Fähigkeit des Staates, digitale Anwendungen sicher und robust zu betreiben.

4. IT-Sicherheit, Resilienz gegen Cyberangriffe und transparente Kommunikation gegenüber den Einsatzkräften und der Öffentlichkeit sind notwendige Voraussetzungen, um Vertrauen in moderne Technologien und die Leistungsfähigkeit der Polizei zu erhalten.

II. Die Landesregierung wird aufgefordert,

1. die vollständige Wiederherstellung der Funktionsfähigkeit der dienstlichen mobilen Polizeigeräte zeitnah zu gewährleisten und dabei sicherzustellen, dass alle Geräte und Server höchsten Sicherheitsanforderungen genügen.
2. einen umfassenden Bericht über den IT-Sicherheitsvorfall, Identität und Umfang möglicher Datenabflüsse, die Ursachen der Schwachstellen und die laufenden Maßnahmen zur Behebung dem Landtag vorzulegen.
3. verbindliche und regelmäßige Schulungs- und Sensibilisierungsprogramme für Polizeibedienstete zur Cyber- und IT-Sicherheit einzuführen, um sowohl technische als auch organisatorische Schwachstellen zu minimieren.
4. dem Landtag bis zur nächsten Sitzungsperiode einen Zwischenbericht über die Fortschritte der hier aufgelisteten Maßnahmen vorzulegen.

René Domke und Gruppe

Begründung:

Der Cyberangriff auf die IT-Infrastruktur der Landespolizei Mecklenburg-Vorpommern hat gravierende und nachhaltige Auswirkungen auf die Funktionsfähigkeit dienstlicher mobiler Endgeräte sowie auf zentrale digitale Prozesse im polizeilichen Alltag. Die infolgedessen eingetretenen Einschränkungen betreffen nicht lediglich Komfortfunktionen, sondern elementare Arbeitsgrundlagen der Polizei, darunter Echtzeitabfragen, Einsatzkommunikation und digitale Dokumentation. Damit ist die effektive Wahrnehmung des staatlichen Sicherheitsauftrages unmittelbar beeinträchtigt.

Die nun erforderlichen Maßnahmen zur Wiederherstellung der Funktionsfähigkeit und zur Absicherung der Systeme stellen keine regulären Investitionen in die Fortentwicklung der Polizeidigitalisierung dar. Vielmehr handelt es sich eindeutig um Kosten der Schadensbeseitigung und Schadensregulierung, die unmittelbar durch den erfolgten Hackerangriff verursacht wurden. Ziel dieser Maßnahmen ist es, den Zustand vor dem Angriff wiederherzustellen, Sicherheitslücken zu schließen und erneute Angriffe wirksam zu verhindern.

Aus diesem Grund dürfen die entstehenden Kosten nicht der Landespolizei selbst angelastet oder durch Umschichtungen innerhalb laufender Budgets kompensiert werden. Die Verantwortung für die Bewältigung der Folgen eines derart schwerwiegenden IT-Sicherheitsvorfalls liegt beim Land Mecklenburg-Vorpommern insgesamt. Entsprechend sind die erforderlichen Mittel durch das Land bereitzustellen, um eine schnelle, vollständige und nachhaltige Wiederherstellung der Einsatzfähigkeit der Polizei sicherzustellen.

Darüber hinaus ist eine transparente Aufarbeitung des Vorfalls zwingend erforderlich. Nur durch eine umfassende Analyse der Ursachen, der entstandenen Schäden und der ergriffenen Gegenmaßnahmen kann das Vertrauen der Einsatzkräfte und der Öffentlichkeit in die digitale Handlungsfähigkeit des Staates wiederhergestellt werden. Die im Antrag geforderten Berichte, Schulungen und Zwischenergebnisse sind daher notwendige Bestandteile einer verantwortungsvollen Schadensregulierung und einer zukunftsfesten IT-Sicherheitsstrategie.

Der Antrag ist somit erforderlich, um die unmittelbaren Folgen des Cyberangriffes zu bewältigen, die innere Sicherheit des Landes zu gewährleisten und die staatliche Verantwortung für die durch externe Angriffe verursachten Schäden klar wahrzunehmen.