LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/5072**
8. Wahlperiode **25.06.2025**

ANTRAG

der Fraktion der CDU

Nach Hackerangriff auf Smartphones der Polizei – Mecklenburg-Vorpommern braucht eine IT- und Cybersicherheitsstrategie

Der Landtag möge beschließen:

I. Der Landtag stellt fest:

1. Der jüngste Angriff auf dienstliche Mobiltelefone der Landespolizei Mecklenburg-Vorpommern, bei dem offenbar auch private Daten der Beamtinnen und Beamten betroffen waren, offenbart in aller Deutlichkeit erhebliche Defizite in der IT-Sicherheitsarchitektur des Landes. Der Vorfall wirft schwerwiegende Fragen hinsichtlich des Schutzes personenbezogener und sicherheitsrelevanter Daten, der Trennung dienstlicher und privater Nutzung sowie der organisatorischen und technischen Zuständigkeiten auf.

2. Der Landtag hat sich in der laufenden Wahlperiode bereits mehrfach mit Fragen der IT- und Cybersicherheit befasst:

   - Mit dem Antrag auf Drucksache 8/244 „IT-Sicherheit unserer Wirtschaft verbessern – kleine und mittlere Unternehmen schützen“ wurde frühzeitig gefordert, grundlegende Handlungsempfehlungen zur Verbesserung der IT-Sicherheit sowie zum Umgang bei Cyberangriffen zu entwickeln und dafür das Know-how des Computer Emergency Response Team (CERT) zu nutzen.
   - In Drucksache 8/249 „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen“ wurde gefordert, mehr gut ausgebildetes Personal für den Bereich IT-Sicherheit und Infrastruktur bereitzustellen, Strategien zu entwickeln, um Angriffe besser vereiteln zu können, und die Cybercrimedienststellen in den Behörden des Landes besser auszustatten.
   - Mit dem Antrag „IT-Sicherheit der Kommunen verbessern“ auf Drucksache 8/663 wurde auf die besondere Verwundbarkeit kommunaler IT-Infrastrukturen hingewiesen und die Landesregierung aufgefordert, Kommunen stärker bei der Absicherung ihrer Systeme zu unterstützen sowie das CERT personell und finanziell dauerhaft besser auszustatten.

- Mit dem Antrag auf Drucksache 8/2346 „Digitalisierungsbestrebungen unterstützen und Cybersicherheit stärken – DigiTrans-Förderung für Unternehmen fortführen“ wurde gefordert, die Förderung von Unternehmensinvestitionen im Bereich Digitalisierung fortzusetzen und die Hälfte der zur Verfügung stehenden Mittel für IT-Sicherheit und Datenschutz aufzuwenden.
- In dem Antrag „Innere Sicherheit – Äußere Stärke: Politikwechsel jetzt“ auf Drucksache 8/4513 wurde abermals auf die Notwendigkeit hingewiesen, die Cybersicherheit als strukturelle Querschnittsaufgabe zu begreifen, sie gezielt zu fördern und institutionell sowie technisch und personell angemessen auszustatten sowie die spezialisierten Einheiten gegen Cyberkriminalität innerhalb der Landespolizei zu stärken.
- Der Sonderbericht des Landesrechnungshofes „Herausforderungen bei der Digitalisierung der Landesverwaltung“ auf Drucksache 8/4703 wie auch verschiedene frühere Landesfinanzberichte stellen kritische Schwachstellen in der Informationssicherheit des Landes fest und fordern die unverzügliche Beseitigung der erkannten Schwachstellen sowie die Verbesserung der personellen Ausstattung in der Informationssicherheitsorganisation.

3. Trotz dieser wiederholten parlamentarischen Initiativen liegt bis heute keine konsistente, ressortübergreifende Gesamtstrategie zur IT- und Cybersicherheit in Mecklenburg-Vorpommern vor, obwohl in Expertenanhörungen der einschlägigen Ausschüsse aus den verschiedenen Landtagsinitiativen eindeutige Empfehlungen der angehörten Sachverständigen abgegeben wurden.

4. Die Landesregierung hat es versäumt, die bekannten Schwachstellen systematisch zu analysieren und konkrete, wirksame Maßnahmen umzusetzen. Das wiederholte Nichthandeln angesichts steigender Bedrohungslagen untergräbt das Vertrauen in die digitale Handlungsfähigkeit des Staates.

5. Vor diesem Hintergrund und angesichts der jüngst erneut offenbarten Lücken in der IT-Sicherheitsarchitektur des Landes bedarf es dringend der Erarbeitung und Umsetzung einer Gesamtstrategie zur Cybersicherheit in Mecklenburg-Vorpommern.

II. Die Landesregierung wird aufgefordert,

1. eine Task-Force zu bilden, welche Ad-hoc-Maßnahmen zur Verbesserung der IT-Sicherheit entwickelt und koordiniert, um kurzfristig weitere Cyberangriffe zu verhindern.
2. einen IT-Sicherheitsrat zu bilden, in dem die kommunale Ebene, die IT-Wirtschaft des Landes sowie weitere Experten eingebunden werden.
3. unverzüglich mit Unterstützung des IT-Sicherheitsrates eine umfassende, ressortübergreifende und mit der kommunalen Ebene, dem Bundesamt für Sicherheit in der Informationstechnik und dem Landtag abgestimmte verbindliche Gesamtstrategie zur Cybersicherheit in Mecklenburg-Vorpommern zu erarbeiten und umzusetzen.

Diese Gesamtstrategie muss
- klare Zuständigkeiten und Verantwortlichkeiten auf allen Ebenen verbindlich regeln,
- modernste technische Sicherheitsstandards verpflichtend einführen und kontinuierlich an aktuelle Bedrohungslagen anpassen,
- eine angemessene technische und personelle Ausstattung der IT-Sicherheitsorgane des Landes, vom CERT über die Landespolizei bis hin zu den IT-Sicherheitsbeauftragten der Kommunen und Kritischer Infrastruktur, verbindlich sicherstellen,
- ein regelmäßiges und verpflichtendes Schulungsprogramm für alle Beschäftigten im öffentlichen Dienst etablieren,
- die strenge Trennung dienstlicher und privater IT-Nutzung vorschreiben und technisch sicherstellen,
- die kommunalen Verwaltungen systematisch und nachhaltig bei der Absicherung ihrer IT-Infrastrukturen unterstützen sowie
- ein wirksames Monitoring- und Frühwarnsystem zur Erkennung und Abwehr von Cyberangriffen beinhalten.

4. den federführenden Ausschuss für Inneres, Bau und Digitalisierung sowie weitere relevante Ausschüsse unverzüglich und fortlaufend über jede Maßnahme zu unterrichten.

Daniel Peters und Fraktion