



HESSISCHER LANDTAG

25. 02. 2025

Kleine Anfrage

Sascha Herr (fraktionslos) vom 28.01.2026

Steuerungsdefizite und Risikotransparenz bei der kommunalen Cybersicherheit in Hessen

und Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

In der Antwort der Landesregierung auf die Kleine Anfrage, Drucksache 21/3143, wird dargestellt, dass das Land Hessen Kommunen im Bereich der Cybersicherheit durch Beratungs- und Unterstützungsangebote begleitet. Zugleich wird jedoch ausgeführt, dass zu zentralen Fragen der tatsächlichen IT-Sicherheitslage – etwa zu vorhandenen Notfallkonzepten, getesteten Backups, Funktionsausfällen oder entstandenen Schäden infolge von Cyberangriffen – keine landesweiten Erkenntnisse vorliegen und entsprechende Daten nicht erhoben werden. Damit bleibt offen, wie die Landesregierung die Wirksamkeit ihrer Maßnahmen bewertet, wie sie Risiken für die kommunale Daseinsvorsorge einschätzt und auf welcher Grundlage sie ihre Steuerungs- und Schutzverantwortung wahrnimmt. Aus diesen offengelegten Defiziten ergibt sich weiterer parlamentarischer Klärungsbedarf.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

- Frage 1 Wie bewertet die Landesregierung die Cybersicherheitslage der hessischen Kommunen insgesamt, wenn ihr nach eigener Darstellung keine belastbaren Erkenntnisse zu Notfallvorsorge, Wiederanlaufplänen und tatsächlichen Schadensfolgen von Cyberangriffen vorliegen?
- Frage 2 Warum verzichtet die Landesregierung trotz der sicherheitsrelevanten Bedeutung kommunaler IT-Systeme bewusst auf landesweite Mindeststandards oder verbindliche Melde- und Berichtspflichten im Bereich der kommunalen Cybersicherheit?

Die Fragen 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Ausgestaltung der IT-Sicherheit, die Notfallvorsorge sowie die Bewertung bestehender Risiken gehören zu den inneren Angelegenheiten der Kommunen (Organisationshoheit) und fallen damit in den Schutzbereich der verfassungsrechtlich garantierten kommunalen Selbstverwaltung gemäß Art. 28 Abs. 2 des Grundgesetzes sowie Art. 137 der Hessischen Verfassung.

Vor diesem Hintergrund ist weder eine landesweite Bewertung der kommunalen Cybersicherheitslage noch die Einführung verbindlicher Mindeststandards oder Melde- und Berichtspflichten ohne ausdrückliche gesetzliche Grundlage vorgesehen. Entsprechende Maßnahmen würden einen Eingriff in die Organisationshoheit der Kommunen darstellen.

Unabhängig hiervon werden Fragen der kommunalen Cybersicherheit fortlaufend im Rahmen des etablierten Austauschs zwischen Land und kommunaler Ebene, insbesondere unter Einbindung der kommunalen Spitzenverbände, behandelt.

- Frage 3 Auf welcher Grundlage entscheidet die Landesregierung über die Ausgestaltung und Fortentwicklung ihrer Förder- und Unterstützungsprogramme, wenn deren Nutzung und Wirksamkeit nicht systematisch ausgewertet werden?

Das Innenministerium gestaltet und entwickelt die Förder- und Unterstützungsprogramme auf Grundlage fachlicher Bewertungen, der praktischen Erfahrungen aus der Umsetzung sowie des kontinuierlichen Austauschs mit den beteiligten Akteuren. Beispielsweise wurde das Aktionsprogramm Kommunale Cybersicherheit (AKC) in mehreren Workshops zusammen mit Vertretern der kommunalen Spitzenverbände sowie IT-Sicherheitsexperten aus Landkreisen, Städten und

Gemeinden verschiedener Größenordnungen entwickelt und dabei am tatsächlichen Bedarf ausgerichtet.

Frage 4 Wie stellt die Landesregierung sicher, dass kritische kommunale Dienstleistungen für Bürgerinnen und Bürger (zum Beispiel Meldewesen, Sozialleistungen, Schulen, Verwaltungen) im Falle schwerer Cybervorfälle landesweit handlungsfähig bleiben?

Kommunale Dienstleistungen werden eigenverantwortlich durch die jeweiligen Kommunen erbracht. Aufgrund der dezentralen Organisation kommunaler IT-Systeme wirken sich Cyber-vorfälle gegen einzelne Kommunen grundsätzlich nicht landesweit, sondern ausschließlich auf die jeweils betroffene Kommune aus.

Das Land unterstützt Kommunen im Ereignisfall im Rahmen seiner Zuständigkeiten durch beratende und koordinierende Maßnahmen, insbesondere durch das Hessen CyberCompetence-Center (Hessen3C). Im Falle eines schweren Cyberangriffs stehen für die betroffene Kommune ein mobiles Soforthilfe-Paket-Kommunikation und – abhängig vom Einzelfall – ein Incident-Response-Service durch externe IT-Sicherheitsexperten zur Verfügung.

Frage 5 Welche politischen Schlussfolgerungen zieht die Landesregierung aus der Tatsache, dass nur ein sehr geringer Teil der Kommunen bislang vertiefte IT-Audits oder Notfallmanagementmaßnahmen in Anspruch genommen hat?

287 und damit über die Hälfte der hessischen Kommunen haben die Schulung wahrgenommen. Die Entscheidung darüber liegt jedoch im Rahmen der kommunalen Selbstverwaltung in der Verantwortung der jeweiligen Kommune. Die Inanspruchnahme landesseitiger Unterstützungsangebote ist freiwillig und orientiert sich an den individuellen Strukturen, Risikobewertungen und bereits vorhandenen Maßnahmen vor Ort. Aus der unterschiedlichen Nutzung der Angebote lassen sich daher keine politischen Schlussfolgerungen im Sinne zusätzlicher landesseitiger Vorgaben oder Steuerungsmaßnahmen ableiten.

Wiesbaden, 20. Februar 2026

Prof. Dr. Roman Poseck