



HESSISCHER LANDTAG

25. 04. 2025

Kleine Anfrage

Markus Fuchs (AfD), Karsten Bletzer (AfD) und Christian Rohde (AfD)
vom 19.02.2025

Nachfrage zur Anfrage 21/1201 – Softwarezertifizierung und digitale Resilienz **und** **Antwort**

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Seit 2015 widmet sich der Gesetzgeber in verstärktem Maß dem Schutz der kritischen Infrastruktur (KRITIS). Ausdruck findet dies z. B. im BSI-Gesetz, der BSI-KritisV und der NIS 2-Richtlinie. Das BSI definiert Kritische Infrastrukturen (KRITIS) als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Dementsprechend werden vom BSI auch „Staat und Verwaltung“ als Teil der KRITIS betrachtet. Diese Einschätzung wird vom Land Hessen anscheinend geteilt, wie sich aus themenbezogenen Veröffentlichungen im Internet entnehmen lässt (→ <https://hessen.de/handeln/kritische-infrastruktur/bereiche-kritischer-infrastruktur>). Dementsprechend kann als Arbeitshypothese davon ausgegangen werden, dass die Landesregierung, zumindest über die den Staat im Allgemeinen und die (Landes-)Verwaltung im Besonderen, betreffende Informationen verfügt bzw. sich diese unschwer beschaffen kann. Dabei ist in Bezug auf das Interpellationsrecht zu beachten, dass „sich die Regierung allgemein bemühen muss, eine möglichst vollständige und präzise Antwort zu geben. Falls dies nicht möglich ist, hat die Regierung die Gründe hierfür gegenüber dem Parlament detailliert und einzelfallbezogen darzulegen.“ (BeckOK Verfassung Hessen/Ogorek/Poseck/Langner HessVerf Art. 77 Rn. 56-60). Die in Beantwortung der Anfrage 21/1201 gegebenen Aussagen erreichen zum Teil nicht den in der Kommentierung geforderten Grad der Vollständigkeit und Präzision. Aus diesem Grund ist eine Nachfrage notwendig.

Diese Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, dem Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigten des Landes Hessen beim Bund, dem Minister der Finanzen, dem Minister der Justiz und für den Rechtsstaat, dem Minister für Kultus, Bildung und Chancen, dem Minister für Wissenschaft und Forschung, Kunst und Kultur, dem Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum, der Ministerin für Digitalisierung und Innovation, dem Minister für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat, der Ministerin für Familie, Senioren, Sport, Gesundheit und Pflege und der Ministerin für Arbeit, Integration, Jugend und Soziales wie folgt:

Frage 1 Geht die Landesregierung davon aus, dass „Staat und Verwaltung“ Teil der KRITIS sind?
Die Antwort bitte normativ begründen.

Am 16. Januar 2023 sind zwei EU-Richtlinien für besseren Schutz Kritischer Infrastrukturen in Kraft getreten: Die EU-Richtlinie über die Resilienz Kritischer Einrichtungen (Critical Entities Resilience /CER-Richtlinie) sowie die EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie). Beide Richtlinien führen unter anderem den Sektor „Öffentliche Verwaltung“ als Kritische Infrastruktur auf. Die Umsetzung dieser Richtlinien in nationales Recht steht bundesseitig noch aus.

Die Landesregierung hat per Kabinettsbeschluss die Kritische Infrastruktur in elf Sektoren eingeteilt. Hierzu gehört auch der Sektor „Staat und Verwaltung“. Überdies hat die Bund-Länder-Arbeitsgruppe KRITIS unter Beteiligung der Länder, des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) und des Bundesministeriums des Innern und für Heimat (BMI) eine Übersicht der KRITIS-Sektoren erstellt, die ebenfalls den Sektor „Staat und Verwaltung“ umfasst.

Zum Bereich „Staat und Verwaltung“ und damit zu den Sektoren der Kritischen Infrastruktur zählen in Hessen der Landtag, alle Ressorts sowie die Justizeinrichtungen.

Frage 2 Welche Notfall-Szenarien werden durch die für die Cybersicherheit der KRITIS-Verantwortlichen in Staat und Verwaltung in Hessen geübt?

Die Antwort bitte begründen und dabei nach Szenario, der Übungsart (im Sinne von BSI-Standard 100-4 (Version 1 (2004) S. 85 Tabelle 18.)), der Anzahl der Übungen pro Zeiteinheit und der übenden Stelle differenzieren.

Wie in der Beantwortung der Fragen 1 und 2 der Kleinen Anfrage Drucksache 21/1201 ausgeführt, sind die KRITIS-Betreiber für die Cybersicherheit verantwortlich.

Unabhängig davon besteht eine Zuständigkeit des Ministeriums des Innern, für Sicherheit und Heimatschutz für die Cybersicherheit in der Landesverwaltung, das in den letzten vier Jahren folgende Übungen durchgeführt hat:

- eintägige Planbesprechung zum Szenario Stromausfall
- eintägige Stabsübung ohne spezifisches Szenario zur praktischen Beübung der Stabsarbeit
- eintägige Stabsübung mit dem Szenario Cyberangriff und Priorisierung von IT-Verfahren
- mehrtägige Stabsrahmenübung mit Alarmierungsübung mit dem Szenario Cyberangriff auf ein wichtiges IT-Verfahren der Landesverwaltung
- mehrtätige ressort- und länderübergreifende Stabsrahmenübung mit dem Szenario Cyberangriff auf das Regierungshandeln (LÜKEX 23)
- zwei eigenständige Alarmierungsübungen ohne spezifisches Szenario

Die Staatskanzlei und die Ressorts haben sich an den ressortübergreifenden landesweiten Übungen unter Federführung des HMdI beteiligt. Das Ministerium für Arbeit, Integration, Jugend und Soziales (HMSI) hat überdies eine Stabsrahmenübung anlässlich der KLIMPRAX Krisenvorbereitung und eine Alarmierungsübung ohne spezifisches Szenario durchgeführt.

Der BSI-Standard 100-4 wurde durch die Veröffentlichung des BSI-Standards 200-4 im Jahr 2023 abgelöst. Die Beantwortung bezieht sich daher auf die Übungsarten des BSI-Standards 200-4 (S. 254 f.).

Frage 3 Wird bei den gegebenen IT-Systemen in Staat und Verwaltung real überprüft, ob innerhalb der vorgesehenen Zeit auf ein Notfallsystem umgeschaltet wird?

Die Antwort bitte begründen.

Ja, das Ausweichen auf Notfallsysteme war teilweise Bestandteil o. g. Übungen.

Frage 4 Für welche IT-Produkte ist in Hessen eine erfolgreiche ITSEC- oder CC-Zertifizierung Voraussetzung für den Einsatz in Staat und Verwaltung?

Die Antwort bitte unter Angabe der Produkte begründen.

In den Ressorts der Landesverwaltung sind keine der genannten Zertifizierungen Voraussetzung für den Einsatz von IT-Produkten; vor dem Einsatz der IT-Produkte erfolgt verwaltungsseitig eine umfassende Prüfung, ob das Produkt für den Einsatzbereich geeignet ist.

Frage 5

- a) In Frage 4 c) der Anfrage 21/1201 wurde auf die Ausführungen ab Minute 00:55:56 ff. des in der Anfrage benannten Vortrags gezielt: „Vorbildfunktion von Politikern“ und „Politik muss vorbeugend weiter voranschreiten“. Frau E. trifft bei Minute 1:00:52 als Quintessenz der genannten Abschnitte die Feststellung, dass die Politik „Teil des Problems“ ist. Ist diese Feststellung nach Auffassung der Landesregierung zutreffend?
Die Antwort bitte ausführlich begründen.
- b) Hat der die Anfrage 21/1201 zeichnende Staatsminister des Inneren selbst eigene Kenntnis vom Inhalt des Vortrags von Frau Professor E. erlangt?
- c) Welche der mit der Beantwortung der Anfrage 21/1201 befassten Personen haben den Vortrag von Frau E. selbst angeschaut?
- d) Kann die fehlende Identifikation der nun benannten Videoabschnitte bei Beantwortung der Anfrage 21/1201 als Beispiel für ein „Teil des Problems sein“ angesehen werden?
Die Antwort bitte begründen.

Die Fragen 5 a) bis d) werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Landesregierung wird auch weiterhin im Rahmen ihrer Zuständigkeit das notwendige veranlassen, um die Resilienz des Landes vor Angriffen weiter zu verbessern. Die von der Vortragenden benannten Defizite beziehen sich im Kern auf Erfordernisse und Maßnahmen der Bundesebene (Gesetzgebung, Cybersicherheitsstrategie des Bundes), für welche die Landesregierung nicht zuständig ist und diese dementsprechend nicht kommentiert.

Die Beantwortung der Kleinen Anfrage Drucksache 21/1201 erfolgte durch den Minister des Innern, für Sicherheit und Heimatschutz.

Frage 6

- a) In welchem Umfang machen Staat und Verwaltung in Hessen von der Möglichkeit Gebrauch, die Beschaffung von IT-Produkten von der Erfüllung von Sicherheitsanforderungen abhängig zu machen?
Die Antwort bitte unter Angabe von Beispielen begründen.
- b) Um welche Art der Sicherheitsanforderungen handelt es sich dabei?
Die Antwort bitte unter Angabe von Beispielen begründen.

Die Fragen 6 a) und b) werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das Land macht umfangreich von dieser Möglichkeit Gebrauch. Die Sicherheitsanforderungen beziehen sich dabei regelmäßig auf anerkannte Standards wie der ISO 27001 bzw. den BSI-Standards nach dem aktuellen Stand der Technik. Dabei werden u. a. IT-Sicherheitskonzepte mit Risikoanalysen, Möglichkeit zu externen Pentests, regelmäßige Audits, Testate (bspw. nach C5) und der Einsatz eines zertifizierten Informationssicherheitsmanagementsystems beim Auftragnehmer vorausgesetzt.

Die Ausschreibungen und Beschaffungen sind mit Leistungsbeschreibungen auf der Hessischen Ausschreibungsdatenbank (HAD) öffentlich einsehbar. Beispielhaft wird auf die HAD-Referenznummern 5/1187 und 8/38659 verwiesen.

Wiesbaden, 14. April 2025

Prof. Dr. Roman Poseck