



HESSISCHER LANDTAG

01. 04. 2025

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 16.12.2024**IT-Sicherheit von Landesbehörden****und**

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Die zunehmenden Cyberangriffe auf Behörden und öffentliche Einrichtungen stellen eine ernsthafte Bedrohung für das Gemeinwesen dar. Die Konsequenzen sind weitreichend: Sie führen zu erheblichen Störungen der Verwaltungsabläufe, verursachen beträchtliche finanzielle Schäden und ermöglichen den Diebstahl sensibler personenbezogener Daten. In besonders kritischen Fällen können diese Angriffe sogar Menschenleben gefährden. Angesichts dieser vielschichtigen Bedrohungslage ist die flächendeckende Implementierung präventiver Schutzmaßnahmen von höchster Dringlichkeit.

Die Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, dem Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigter 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 Welche IT-Sicherheitschecks werden in den Behörden des Landes Hessen und den Kommunen regelmäßig durchgeführt und mit welchen Methoden?

Die Dienststellen der Landesverwaltung sind verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) gemäß BSI-Standards umzusetzen. Dies umfasst unter anderem die regelmäßige Überprüfung und Bewertung der IT-Verfahren und -Systeme mit Schutzbedarfsfeststellung im Rahmen der Informationssicherheitskonzepte sowie die Anforderungen zur Durchführung von Audits, Revisionen und Penetrationstests. Derzeit befindet sich eine Pentest-Richtlinie für die gesamte Landesverwaltung in Abstimmung, welche Verfahren und Methoden für die Durchführung von Penetrationstests regeln soll.

Darüber hinaus erstellt und verteilt das Hessen CyberCompetenceCenter (Hessen3C) in Zusammenarbeit mit dem zentralen IT-Dienstleister der Landesverwaltung Schwachstellenberichte und Warnmeldungen, die in den zentralen Infrastrukturen und in den Dienststellen ausgewertet, auf Betroffenheit geprüft und durch Maßnahmen, wie beispielsweise Einspielen von Patches sowie Filtern und Blockieren von Verbindungen oder Berechtigungen, umgesetzt werden.

Weitere regelmäßige Prüfmaßnahmen und Methoden sind der Betrieb eines Security Information and Event Management (SIEM)-Systems, automatisierte Schwachstellenscans, Kontrollen auf kompromittierte Passwörter sowie Phishing-Kampagnen. Zudem finden regelmäßig Notfallübungen statt.

Die Gewährleistung der Informationssicherheit und des IT-Betriebs auf kommunaler Ebene liegt in der Organisationshoheit der Kommunen selbst.

Frage 2 Wo können Sicherheitslücken im Rahmen eines „Responsible Disclosure“-Verfahrens in hessischen Behörden und Kommunen gemeldet werden?

Ansprechstelle ist das Hessen3C.

Frage 3 Wie viele Schwachstellen wurden bisher erfolgreich behoben?

Das Beheben von Schwachstellen in der eigenen IT-Infrastruktur gehört zur täglichen Arbeit der mit Informationssicherheit befassten Beschäftigten. Die Anzahl der täglich behobenen Schwachstellen bewegt sich im zwei- bis dreistelligen Bereich.

Sollte sich die Fragestellung auf behobene Schwachstellen im Rahmen des Responsible Disclosure-Verfahrens beziehen, kann mitgeteilt werden, dass bislang keine die Landesverwaltung betreffenden Schwachstellen von Dritten gemeldet wurden.

Frage 4 Wie viele Strafanzeigen wurden von hessischen Behörden in diesem Zusammenhang gestellt? Bitte nach Jahren aufschlüsseln.

Jahr	Strafanzeigen
2015	1
2016	3
2017	7
2018	1
2019	1
2020	11
2021	10
2022	13
2023	4
2024	10

Frage 5 Wie weit ist der Umstieg von Windows 10 auf Windows 11 in der hessischen Verwaltung fortgeschritten (Anteil in Prozent der jeweils genutzten Systeme)?

In der hessischen Landesverwaltung ist der Umstieg auf Windows 11 zu über 50 Prozent umgesetzt.

Frage 6 Wie groß ist der prozentuale Anteil von Open-Source-Software in der hessischen Landesverwaltung?

Es liegen keine statistischen Daten vor.

Ergänzend wird auf die Beantwortung der Kleinen Anfrage, Drucksache 21/621, verwiesen.

Frage 7 Wie bewertet die Landesregierung die geplanten Ausnahmeregelungen für öffentliche Stellen und Dienstleister in der Umsetzung der NIS-2 Verordnung?

Die Landesregierung geht davon aus, dass der Fragesteller den Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes des Bundes meint.

Die geplante sogenannte „Öffnungsklausel“ für die internen IT-Dienstleister der Landesverwaltung wird begrüßt, da die Dienstleister, dem föderalen Prinzip gemäß, hierdurch dem Regelungsbereich und der Aufsicht des Landes Hessen unterfallen sollen.

Frage 8 Welche IT-Sicherheitsstandards müssen externe Dienstleister des Landes Hessen, insbesondere hinsichtlich ISO 27001 und IT-Grundschutz, erfüllen?

Anforderungen an den Beschaffungsgegenstand werden im Einzelfall von der auftraggebenden Stelle festgelegt und sind von einer Vielzahl von Faktoren abhängig.

Einheitliche IT-Sicherheitsstandards lassen sich nicht pauschal benennen und sind dienstleistungs-spezifisch. Abhängig von der Art der erbrachten Dienstleistung und der Sensibilität der verarbeiteten Daten im Hinblick auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit variieren die Anforderungen. Diese sind grundsätzlich vom externen Dienstleister nachzuweisen. Häufig notwendige Zertifizierungen und Testate sind ISO 27001, BSI-C5 Testat und SOC 2.

Frage 9 Wie ist das Notfallmanagement für Cyberangriffe in hessischen Behörden und Kommunen geregelt?

Das IT-bezogene Notfallmanagement ist als Teil des ISMS verpflichtend für die Dienststellen des Landes. Für schwerwiegende ressortübergreifende IT-Sicherheitsvorfälle greift das IT-Krisenmanagementkonzept gemäß Ziffer 7.11 der Informationssicherheitsleitlinie für die hessische Landesverwaltung.

Die Gewährleistung eines Notfallmanagements auf kommunaler Ebene liegt in der Organisationshoheit der Kommunen selbst.

Frage 10 Welches System des Schwachstellen-Managements wird in den Behörden und Kommunen des Landes Hessen betrieben?

In der Landesverwaltung werden technische Systeme des Schwachstellen-Managements eingesetzt, darunter marktgängige Software-Lösungen und Eigenentwicklungen. Der zentrale IT-Dienstleister der Landesverwaltung betreibt darüber hinaus ein Schwachstellenscansystem. Ergänzend wird auf die Antwort zu Frage 1 verwiesen.

Die Schaffung eines Systems im Sinne eines Schwachstellen-Managements auf kommunaler Ebene liegt in der Organisationshoheit der Kommunen selbst.

Wiesbaden, 26. März 2025

Prof. Dr. Roman Poseck