



HESSISCHER LANDTAG

28. 11. 2025

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 06.10.2025**Cybersecurity und NIS-2-Richtlinie Umsetzung****und****Antwort****Minister des Innern, für Sicherheit und Heimatschutz**

Vorbemerkung Fragesteller:

Die Cybersicherheitslage in Deutschland und Europa verschärft sich dramatisch. Während Deutschland wegen verspäteter NIS-2-Umsetzung im EU-Vertragsverletzungsverfahren steht, steigen die Kosten für Cybersicherheit explosionsartig. Für Hessen als Wirtschaftsstandort mit wichtiger Infrastruktur sind diese Entwicklungen von größter Bedeutung. Die NIS-2-Richtlinie ist eine EU-weite Cybersicherheitsvorgabe, die ab Ende 2024 beziehungsweise 2025 deutlich mehr Unternehmen und auch öffentliche Einrichtungen als bisher betrifft. Ziel ist es, ein einheitlich hohes Schutzniveau für Netz- und Informationssysteme kritischer Branchen (zum Beispiel Energie, Verkehr, Gesundheit, öffentliche Verwaltung, IT-Dienste) zu gewährleisten. Alle betroffenen Organisationen müssen strenge technische und organisatorische IT-Sicherheitsmaßnahmen umsetzen, sich beim BSI registrieren, Sicherheitsvorfälle schnell melden und ihre Lieferketten absichern. Bei Verstößen drohen empfindliche Geldbußen. Die Anforderungen betreffen in Deutschland etwa 30.000 Unternehmen, auch viele Mittelständler.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister der Finanzen, dem Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum und dem Minister für Wissenschaft und Forschung, Kunst und Kultur und wie folgt:

Frage 1 Wie viele hessische Unternehmen sind von der NIS-2-Richtlinie betroffen?

Frage 2 Mit welchen Gesamtkosten rechnet die Landesregierung für die hessische Wirtschaft bei der Umsetzung?

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

Die Gesetzgebungskompetenz für die Umsetzung der NIS-2-Richtlinie in Bezug auf Unternehmen liegt beim Bund, das Gesetzgebungsverfahren ist noch nicht abgeschlossen. Der Landesregierung liegen keine gesicherten Erkenntnisse zur Anzahl der von der NIS-2-Richtlinie betroffenen Unternehmen vor; schätzungsweise sind rund 2.000 hessische Unternehmen betroffen. Der Stellungnahme des Nationalen Normenkontrollrates zum Gesetz zur Umsetzung der NIS-2-Richtlinie ist zu entnehmen, dass mit Kosten für die Wirtschaft in Höhe von 2,3 Milliarden Euro gerechnet wird; gesonderte Zahlen für Hessen liegen nicht vor.

Im Übrigen wird auf die Beantwortung der Frage 5 der Kleinen Anfrage, Drucksache 21/748, verwiesen.

Frage 3 Welche konkreten Maßnahmen plant die Landesregierung zur Unterstützung hessischer Unternehmen bei der NIS-2-Compliance?

Frage 6 Wie unterstützt die Landesregierung kleine und mittlere Unternehmen in Hessen bei der Verbesserung ihrer IT-Sicherheit?

Die Fragen 3 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet kostenlose Informationen, Webinare, Veranstaltungen und Schulungen an. Flankierend dazu bietet das im Ministerium des Innern, für Sicherheit und Heimatschutz (HMdI) eingerichtete Hessen Cyber-CompetenceCenter (Hessen3C) hessischen Unternehmen zur Verbesserung ihrer

Informationssicherheit umfassende Unterstützung durch den Einsatz des Computer Emergency Response Teams (CERT) beziehungsweise des Mobile Incident Response Teams (MIRT) an. Hierzu gehören:

- Anlassbezogene und regelmäßige Lageberichte,
- Kostenlose, hersteller- und produktunabhängige Beratung zur IT-Sicherheitsarchitektur sowie den dazugehörigen Prozessen,
- Präventions- und Sensibilisierungsveranstaltungen für Beschäftigte und Führungskräfte sowie
- Unterstützung bei der Analyse von schwerwiegenden IT-Sicherheitsvorfällen und Beratung zum IT-Krisenmanagement sowie zur Wiederherstellung der IT-Infrastruktur.

Im Rahmen des Programms „Existenz- und Betriebsberatung sowie Coaching“ fördert das Ministerium für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum (HMWVW) Digitalisierungsberatungen, die über die RKW Hessen GmbH angeboten werden. Inhalt dieser Beratungen können auch die Themen IT-Sicherheit und Cybersicherheit sein sowie speziell Fragen zur NIS-2-Richtlinie. Zudem fließen in die Beratung auch Hinweise auf anderweitige Unterstützungsangebote beispielsweise des Bundes ein. Dieser bietet entsprechende Tools sowohl im Bereich der allgemeinen Cybersicherheit als auch spezielle NIS-2-Tools an wie etwa den sogenannten FitNIS2-Navigator, der Unternehmen bei der Umsetzung der NIS-2-Richtlinie unterstützt. Mit diesem Werkzeug ist die Prüfung der eigenen Betroffenheit eines Unternehmens über die Erhebung des eigenen Status quo und den daraus resultierenden Handlungsbedarfen bis hin zur Erstellung individueller Aktionspläne möglich.

Das RKW Hessen hat zusätzlich im Rahmen seiner – ebenfalls vom HMWVW geförderten – Erstberatung im Februar 2025 eine Informationsveranstaltung zusammen mit dem LKA zum Thema Cybersicherheit durchgeführt. Diese Kooperation zwischen RKW und LKA soll fortgeführt werden.

Weiterhin unterstützt der DIGI-Zuschuss KMU der gewerblichen Wirtschaft und der Freien Berufe bei der konkreten Einführung neuer digitaler Systeme der Informations- und Kommunikationstechnik sowie der Verbesserung der IT-Sicherheit mit bis zu 10.000 Euro. Besonders im Handwerk, das rund ein Viertel der Förderungen erhält, trägt der DIGI-Zuschuss dazu bei, den digitalen Wandel voranzutreiben. Mit dem DIGI-Zuschuss wurden bis 2024 jährlich rund 1.000 Unternehmen gefördert. Für 2025 sind rund 600 Bewilligungen geplant. Seit dem 01.09.2025 läuft die diesjährige zweite große Bewerbungsrunde für den DIGI-Zuschuss.

Frage 4 Wie ist der aktuelle Stand der Cybersicherheitsstrategie des Landes Hessen?

Die am 04.09.2023 vom Kabinett verabschiedete hessische Cybersicherheitsstrategie wird derzeit, wie vorgesehen, evaluiert.

Frage 5 Welche Cybersicherheitsvorfälle hat es in hessischen Behörden und Kommunen sowie kommunalen Unternehmen in 2025 gegeben?

Für Dienststellen der Landesverwaltung besteht eine Meldepflicht für Sicherheitsvorfälle nach § 18 Abs. 1 des Hessischen IT-Sicherheitsgesetzes (HITSiG). Sie haben 2025 bislang 293 Sicherheitsvorfälle gemeldet. Von hessischen Kommunen wurden sechs und von hessischen kommunalen Unternehmen sieben Vorfälle gemeldet; eine Pflicht zur Meldung besteht hier nicht.

Frage 7 Wie plant die Landesregierung die Aus- und Weiterbildung von Cybersicherheitsexperten in Hessen?

Die Ausgestaltung von Studium und Lehre an den Hochschulen obliegt diesen selbst. An den Hochschulen sowie an den außeruniversitären Forschungseinrichtungen existiert ein breites Portfolio zum Thema Cybersicherheit, das auch den Themenbereich Aus- und Weiterbildung umfasst. In den Fachbereichen Informatik ist Cybersicherheit fester Bestandteil der Lehre. Einige Hochschulen bieten darüber hinaus Kurse zu Cybersicherheit an, zum Beispiel die Hochschule Fulda. Exemplarisch zu erwähnen sind der an der Technischen Universität Darmstadt (TUD) angebotene Masterstudiengang IT-Sicherheit und der Kooperative Studiengang IT-Sicherheit (B.Sc.) an der Hochschule Darmstadt (h_da). Ergänzend hierzu bestehen zwischen der TUD sowie der h_da Kooperationen im Bereich der Lehre. Durch die räumliche Nähe zum Cybersicherheitsforschungszentrum ATHENE und die personelle Beteiligung der beiden Hochschulen an diesem können die Studierenden unter anderem von den aktuellen wissenschaftlichen Erkenntnissen profitieren. Je nach Schwerpunktsetzung der Hochschule existieren weitere Angebote. So wird beispielsweise an allen Universitäten mindestens ein Modul mit Schwerpunkt

Cybersicherheit im Rahmen des Studiums angeboten. Insbesondere bei Studiengängen mit technischem Schwerpunkt, wie zum Beispiel Technische Informatik (B.Sc.) an der Hochschule Rhein-Main oder Organisations- und IT-Sicherheit (B.Sc.) der Technischen Hochschule Mittelhessen, sind ebenfalls Module oder ganze Semester dem Schwerpunkt Cybersicherheit gewidmet. Das Fraunhofer-Institut für Sichere Informationstechnologie bietet ebenfalls Weiterbildungsmöglichkeiten an, zum Beispiel das Lernlabor Cybersicherheit mit Angeboten zu AI Security und IT-Forensik sowie eine Cyber-Range zur realistischen Angriffssimulation. Der duale Studiengang Informatik/IT-Sicherheit, der von der Finanzverwaltung in Kooperation mit der hda angeboten wird, bietet auch in der Landesverwaltung Ausbildungsmöglichkeiten im Bereich Cybersicherheit. Darüber hinaus unterstützt das Land Hochschulen und Forschungseinrichtungen bei Forschungsvorhaben im Bereich der Cybersicherheit, die der Entwicklung innovativer Schutzmaßnahmen und verlässlicher Lösungen für Informations- und Kommunikationstechnologien dienen.

Bezogen auf die hessische Landesverwaltung besteht ebenfalls ein umfassendes Aus- und Weiterbildungsprogramm für Beschäftigte. Mit speziellen Schulungsangeboten für IT-Fachkräfte können besondere Qualifikationen im Bereich der Cybersicherheit erworben werden (beispielsweise in der IT-Forensik oder durch sogenannte Cyber-Range-Trainings). Darüber hinaus schult das Land Hessen im Hessischen Cyberabwehrausbildungszentrum Beschäftigte der Landes- und der Kommunalverwaltungen im Bereich des Business-Continuity-Managements. Die Hessische Zentrale für Datenverarbeitung (HZD) bietet zur Gewinnung und Entwicklung von Fachkräften weitere Aus- und Weiterbildungen an. Die HZD ist Kooperationspartner der Hochschule Darmstadt mit dem dualen Studiengang IT-Sicherheit (KITS) und bildet jährlich dual Studierende aus. Thematisch liegt der Studienschwerpunkt auf Verschlüsselung, Datensicherung und IT-Forensik. Nach dem erfolgreichen Bachelorabschluss erfolgt ein Einsatz in Aufgabengebieten der HZD, die sich mit cybersicherheitsrelevanten Themen und Technologien beschäftigen. Darüber hinaus fördert ein im Jahr 2024 aufgesetztes Qualifizierungsprogramm für Beschäftigte der HZD ein berufsintegriertes Masterstudium mit Schwerpunkt auf Informationssicherheit. Die IT-Fortbildung der HZD ist eine der wenigen von der Bundesakademie für öffentliche Verwaltung (BAköV) akkreditierten Qualifizierungs- und Zertifizierungsstellen für den Lehrgang „Informationssicherheitsbeauftragte in der öffentlichen Verwaltung (BAköV)“. Durch dieses vom BSI und der BAKöV entwickelte Fortbildungsprogramm werden Expertinnen und Experten auf hohem Niveau in allen Fragen der Informationssicherheit weitergebildet und zertifiziert. Ziel ist die Sicherstellung der Informationssicherheit in allen Dienststellen des Landes. Die Informations-sicherheitsbeauftragten sind mit bestehenden Compliance-Vorgaben vertraut, unterstützen direkt bei allen cybersicherheitsrelevanten Aufgaben und stärken zugleich die Awareness.

Die Hessische Hochschule für öffentliches Management und Sicherheit (HöMS) bietet überdies seit dem Sommersemester 2021 am Fachbereich Polizei das Bachelorstudium „Kriminalpolizei“ mit einer Vertiefungsrichtung „Cyberkriminalistik“ am Standort Mühlheim an. Hierdurch soll den immer schneller wachsenden Herausforderungen durch Cyberkriminalität und den Herausforderungen im Umgang mit digitalen Spuren in allen polizeilichen Kontexten in angemessener Weise begegnet werden. Ziel des Vertiefungsstudiengangs Cyberkriminalistik ist es, Kriminalbeamtinnen und -beamte auszubilden, die neben den klassischen Kompetenzen während des Studiums zusätzliches Wissen aus dem Bereich der Computer-, Netzwerk- und Kommunikationstechnik sowie anderen Teildisziplinen der Informatik und Informationstechnik erwerben, welches sie sowohl zum kompetenten Umgang mit digitalen Spuren – von deren Sicherstellung bis zur forensischen Auswertung – als auch zu moderner digitaler Ermittlungsarbeit im Zusammenhang mit dem Internet befähigt.

Zudem befindet sich derzeit ein Wahlpflichtmodul zur Informations- und Cybersicherheit im Studiengang Digitale Verwaltung an der HöMS in Erarbeitung.

Frage 8 Welche Rolle spielt Künstliche Intelligenz in der hessischen Cybersicherheitsstrategie?

Künstliche Intelligenz ist eine Schlüsseltechnologie, die für die Cybersicherheit von grundlegender Bedeutung ist. Ihre besondere Bedeutung wird im Abschnitt 5.3.1 Angewandte Forschung der CSS hervorgehoben. Das Themenfeld KI wird im Rahmen der Evaluierung der CSS mitberücksichtigt.

Wiesbaden, 21. November 2025

Prof. Dr. Roman Poseck