Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT
mit Antwort der Landesregierung

Anfrage der Abgeordneten Omid Najafi und Dennis Jahn (AfD)

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

Cybersicherheit und kritische Infrastrukturen: Welche Auswirkungen hat die EU-NIS2-Richtlinie und das NIS2-Umsetzungsgesetz für Niedersachsen?

Anfrage der Abgeordneten Omid Najafi und Dennis Jahn (AfD), eingegangen am 12.01.2024 - Drs. 19/3267,
an die Staatskanzlei übersandt am 15.01.2024

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 14.02.2024

Vorbemerkung der Abgeordneten

Die EU-Richtlinie 2022/2555 vom 14. Dezember 2022 über „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“[1] wird seit April 2023 und mit Zieldatum 17. Oktober 2024 in nationales deutsches Recht übertragen (Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit, NIS2UmsuCG). Bisher liegen seitens des Bundes aus April, Juli und September 2023 drei Referentenentwürfe vor, die parallel zum Dachgesetz zur Sicherung kritischer Infrastrukturen (KRITIS) fortgeschrieben wurden. Der Geltungsbereich des NIS2-Umsetzungsgesetzes geht über die KRITIS-Kriterien hinaus.

Neben Institutionen von Bund, Ländern und Kommunen werden bundesweit rund 30 000 Unternehmen die vorgeschriebenen Anforderungen von NIS2 erfüllen müssen. Betroffen sind Unternehmen ab 50 Mitarbeitern und einem Jahresumsatz von 10 Millionen Euro, die in ihren Geschäftsfeldern 18 Wirtschaftssektoren zugeordnet werden können. Als „wesentliche“ Sektoren (elf) gelten Energie, Transport, Bankwesen und Finanzinfrastruktur, Gesundheitsdienstleistung und -forschung, Trink- und Abwasserversorgung, Digitale Infrastruktur und ITK-Servicemanagement (B2B), Öffentliche Verwaltung und Weltraum. Als „wichtige“ Sektoren (sieben) gelten Post, Abfallentsorgung, Chemie und produzierendes Gewerbe, Lebensmittelindustrie, Digitale Dienste und Forschungsinstitute.

Das gemeinsame Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen, der IT-Planungsrat, hat gefordert, „von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen“[2].Hingegen hat der DIHK in einer Stellungnahme deutlich gemacht, dass eine Ausnahme der öffentlichen Hand von den NIS2-Verpflichtungen von der Wirtschaft kritisch gesehen werde, weil gerade die Wirtschaft auf sichere IT-Strukturen in den Verwaltungen angewiesen sei. Der Wirtschaft fehle ein staatliches Gesamtkonzept zur Cybersicherheit; es bestehe die Gefahr von Doppelregulierungen, unklaren Behördenzuständigkeiten, fehlender Fachkräfte-Ressourcen sowie einer schwer zu realisierenden Einbeziehung der Lieferkette in die Risikomanagementmaßnahmen in Verbindung mit den vorgesehenen Haftungsansprüchen[3].

---

1 Zur Änderung der EU-Verordnung Nr. 910/2014, der EU-Richtlinie 2018/1972 sowie zur Aufhebung der EU-Richtlinie 2016/1148

2 www.it-planungsrat.de/beschluss/beschluss-2023-39

3 https://www.dihk.de/de/dihk-positionen-zu-nationalen-gesetzesvorhaben-8982

Vorbemerkung der Landesregierung

Gemäß Artikel 288 Abs. 3 des Vertrages über die Arbeitsweise der Europäischen Union ist eine Richtlinie für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Welche Stelle innerhalb der Mitgliedstaaten eine Richtlinie umsetzen muss, richtet sich nicht nach Unionsrecht, sondern nach den jeweiligen innerstaatlichen Kompetenzvorschriften. Diese finden sich für die Bundesrepublik Deutschland in den Artikeln 70 ff. des Grundgesetzes. Dieser Grundsatz gilt auch für die Umsetzung der NIS-2-Richtlinie. Der Bund kann nur solche Vorgaben der NIS-2-Richtlinie in nationales Recht umsetzen, für die er auch über die Gesetzgebungskompetenz verfügt. Die Vorbemerkung der Abgeordneten, dass die Umsetzung in nationales deutsches Recht über das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) erfolgt, ist insoweit unpräzise. Für einige Vorgaben der NIS-2-Richtlinie verfügt der Bund über keine Gesetzgebungskompetenz. Daher sind nach dem Grundsatz des Artikels 70 des Grundgesetzes die Länder für Teile der Umsetzung verantwortlich. Dies gilt insbesondere mit Blick auf Artikel 2 Abs. 2 Buchst. f) Ziffer ii), Artikel 2 Abs. 5, Artikel 7 Abs. 1, Artikel 8 Abs. 1 und Artikel 10 Abs. 1 der NIS-2-Richtlinie.

Hinsichtlich des NIS2UmsuCG hat bislang keine formale Länder- und Verbändebeteiligung im Sinne des § 47 der Gemeinsamen Geschäftsordnung der Bundesministerien stattgefunden. Nach hiesiger Kenntnis befindet sich der Referentenentwurf weiterhin in der internen Ressortabstimmung auf Bundesebene. Bei den angesprochenen „Referentenentwürfen“ aus April und Juli 2023 handelt es sich um geleakte Fassungen, die innerhalb der Bundesregierung nicht abgestimmt waren. Zu geleakten Fassungen wird die Landesregierung keine Stellung beziehen. Bei dem Entwurf aus September 2023 handelt es sich nicht um einen Referentenentwurf, sondern um ein Diskussionspapier des Bundesministeriums des Innern und für Heimat mit wirtschaftsbezogenen Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland. Wesentliche Teile des Gesetzes, insbesondere hinsichtlich der künftigen Zusammenarbeit zwischen Bund und Ländern, waren nicht enthalten. Das Land Niedersachsen hat von der Gelegenheit der Stellungnahme Gebrauch gemacht. Eine abschließende Bewertung ist aufgrund der fragmentierten Vorschriften jedoch nicht möglich.

Die niedersächsische Landesregierung beabsichtigt, dem Beschluss des IT-Planungsrates Bund/Länder vom 03.11.2023 folgend, keinen Gebrauch von der fakultativen Einbeziehung der Kommunalverwaltungsebene zu machen. Insofern werden die Kommunen in ihrer Kernverwaltung von den Vorgaben der NIS-2-Richtlinie nicht betroffen sein. Die Nicht-Einbeziehung bezieht sich jedoch lediglich auf Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 6 Ziffer 35 der NIS-2-Richtlinie. Sowohl kommunale Unternehmen als auch kommunale Eigenbetriebe werden in den Anwendungsbereich der Richtlinie fallen, sofern sie in einem der Sektoren des Anhangs I und II der NIS-2-Richtlinie tätig sind (u. a. Energie, Verkehr, Gesundheitswesen, Trinkwasser, Abwasser und Abfallwirtschaft) und die sogenannte Size-Cap-Rule erfüllen (mind. 50 Beschäftigte und/oder mind. 10 Millionen Euro Jahresumsatz). Ein wesentlicher Teil der kritischen Aufgaben der Daseinsvorsorge einer Kommune wird dadurch von Cybersicherheitsmindestanforderungen betroffen sein. Diese Einrichtungen werden über Bundesrecht reguliert. Dies entspricht der derzeitigen Rechtslage, sofern Kommunen Kritische Infrastrukturen (KRITIS) betreiben.

Zudem besteht bereits eine Vielzahl an rechtlich bindenden Vorgaben, aus denen sowohl die Landesverwaltung als auch die Kommunalverwaltung verpflichtet sind, eine angemessene Informationssicherheit zu gewährleisten. Neben speziellen Anforderungen aus Nutzungsbedingungen und vertraglichen Beziehungen zu Dritten ist jede Behörde insbesondere auf Grundlage datenschutzrechtlicher Anforderungen zum Schutz personenbezogener Daten nach Artikel 24 und 25 DSGVO i. V. m. Artikel 32 DSGVO verpflichtet, eben solche Maßnahmen zu ergreifen. Der Niedersächsische Landesrechnungshof sieht eine Verpflichtung ebenso aus Artikel 20 Abs. 3 GG. Behörden, die das Landesdatennetz betreiben oder an das Landesdatennetz angeschlossen sind, haben weitere Anforderungen zu erfüllen, die sich aus dem 3. Teil des Niedersächsischen Gesetzes über digitale Verwaltung und Informationssicherheit (NDIG) ergeben. Es fehlt an keinem staatlichen Gesamtkonzept zur Cybersicherheit. Die Wirtschaft kann sich aufgrund der bestehenden Regelungen bereits auf sichere IT-Strukturen in den niedersächsischen Verwaltungen verlassen.

1. Wie bewertet die Landesregierung inhaltlich den dritten Referentenentwurf des NIS2UmsuCG mit seinen Lockerungen und Ausnahmen, und welche Position vertritt sie dazu im Bundesrat?

Es wird auf die Vorbemerkung verwiesen. Es liegt kein dritter Referentenentwurf vor, der im Bundesrat beraten werden könnte.

2. Wie viele Unternehmen in Niedersachsen wären von den Pflichtregelungen des NIS2UmsuCG betroffen (bitte nach den Bereichen freie Wirtschaft und Kommunalbetriebe sowie nach den 18 Sektoren ausweisen)?

Zu dieser Frage liegen der Landesregierung keine spezifischen Daten vor. Auf Grundlage der vom Bund geschätzten bundesweit ca. 30 000 betroffenen Unternehmen kann überschlagen werden, dass in Niedersachsen ca. 3 000 Unternehmen betroffen sein könnten. Eine konkrete Erhebung kann aber frühestens dann erfolgen, wenn eine Grundlage in Form eines in der Bundesregierung abgestimmten Referentenentwurfs vorliegt.

3. Welche Kosten für Personal (Informationssicherheitsbeauftragte, Koordinatoren, IT-Personal, externe Berater) und Schulungen müssten die niedersächsischen Kommunen bei einer Implementierung der NIS2-Vorgaben in ihren Haushalten aufwenden bzw. umschichten?

Es wird auf die Vorbemerkung verwiesen. Der Betrieb der IT und die Gewährleistung der IT-Sicherheit in den kommunalen Eigenbetrieben und kommunalen Unternehmen, die von der NIS-2-Richtlinie betroffen sein könnten, liegen in der Verantwortung der jeweiligen Eigentümerstruktur. Aufgrund der Heterogenität der Strukturen sowie unterschiedlicher Reifegrade in der Umsetzung von IT-Sicherheitsmaßnahmen wäre eine verlässliche Erhebung der Kosten unverhältnismäßig. Insoweit wurden die Kosten durch die Landesregierung nicht erhoben.

4. Wie viele Cyberangriffe und Hackerattacken (beispielsweise durch Ransomware) auf Unternehmen und Kommunalbetriebe geschahen in Niedersachsen in den Jahren 2021 und 2022 (bitte nach Branchen aufschlüsseln)? Welchen Urhebern lassen sich diese Angriffe zuordnen?

Im Rahmen der polizeilichen Kriminalstatistik (PKS) werden Cyber-Straftaten bundeseinheitlich im Summenschlüssel „Cybercrime“ zusammengeführt. Im Jahr 2021 wurden in Niedersachsen 11 626 Fälle und im Jahr 2022 insgesamt 12 917 Fälle von Cybercrime registriert. Eine individuelle Erfassung von Cybercrime bzw. Cyberangriffen auf Unternehmen, Behörden, Verwaltungen, Körperschaften sowie Anstalten öffentlichen Rechts erfolgt jedoch nicht. Im Übrigen werden bei Straftaten in Tateinheit nur die Straftaten mit der höchsten Strafandrohung in der PKS registriert; beispielsweise werden Straftaten im Zusammenhang mit Ransomware als Erpressung und nicht als Cybercrime-Straftat in der PKS abgebildet.

Abgesehen von der PKS wird in Niedersachsen für die Phänomene Ransomware und Distributed Denial of Service (DDoS) ein gesondertes Monitoring durchgeführt. Eine Aufschlüsselung der betroffenen Unternehmen im Sinne der Anfrage wird dabei allerdings nicht vorgenommen.

Ransomware ist eine bedeutende Variante des Cyberangriffs, wenngleich die Fallzahlen in Relation zur Gesamtzahl der Cyberstraftaten vergleichsweise niedrig sind. Für das Jahr 2022 wurden im Rahmen einer einmaligen Sondererhebung zum Monitoring 55 Strafverfahren zu Ransomware-Angriffen auf mittelständische und größere Unternehmen festgestellt.

Für das Phänomen DDoS wurden im Jahr 2022 insgesamt 15 Fälle registriert, was einen Rückgang um zehn Fälle im Vergleich zum Jahr 2021 bedeutet. Betroffen waren neben Unternehmen u. a. auch Schulen und Vereine. In wenigen Einzelfällen waren auch Privatpersonen betroffen. Betroffene von abgewehrten Attacken zeigen eine geringere Anzeigebereitschaft, da kein Schaden eingetreten ist.

Hinsichtlich der Urheberschaft ist festzustellen, dass die Täterinnen und Täter nach hiesiger Kenntnis in der Regel auf internationaler Ebene arbeitsteilig und mit wechselnder Beteiligung je nach Spezialisierung lediglich kurzfristig zusammenarbeiten (Crime-as-a-Service). Schwierigkeiten bei der Identifizierung von Urhebern ergeben sich durch die Nutzung von Verschleierungen (beispielsweise die Verwendung von VPN-Diensten) sowie durch länderspezifische Rahmenbedingungen in der internationalen Zusammenarbeit mit anderen Staaten.

Auch angesichts der in Deutschland weiterhin fehlenden Vorratsdatenspeicherung fehlt es häufig an verwertbaren Ermittlungsansätzen. Eine konkrete Aussage zu den Urhebern von Cyberangriffen kann daher nur schwer getroffen werden.

5. Wie viele Cyberangriffe und Hackerattacken (beispielsweise durch Ransomware) auf Behörden, Verwaltungen, Körperschaften oder Anstalten öffentlichen Rechts geschahen in Niedersachsen in den Jahren 2021 und 2022? Welchen Urhebern lassen sich diese Angriffe zuordnen?

Es wird auf die Antwort zu Frage 4 verwiesen. Aufgrund der dargestellten Einschränkungen der PKS ist eine Unterscheidung nach Behörden, Verwaltungen, Körperschaften oder Anstalten öffentlichen Rechts nicht möglich. Darüber hinaus besteht hier ebenfalls die Problematik, dass bei Straftaten in Tateinheit lediglich die Straftat mit der höchsten Strafandrohung erfasst wird.

Das Niedersächsische Computer-Emergency Response Team (N-CERT) beobachtet eine kontinuierlich steigende Anzahl von sogenannten Hochrisiko-Objekten pro Monat. Diese können unterschiedliche Schadsoftwaretypen enthalten. Die Anzahl schwankt je nach Aktivität einer „Angriffswelle“. Es kann sich dabei beispielsweise um unerlaubte Zugriffsversuche auf Bestandteile der IT-Infrastruktur handeln oder auch um Schadsoftware, die direkt an Empfängerinnen und Empfänger in den Behörden per E-Mail oder andere Kommunikations-Kanäle adressiert werden.

Gemäß § 14 Abs. 2 des Niedersächsischen Gesetzes über digitale Verwaltung und Informationssicherheit (NDIG) ist jedes Mitglied des Sicherheitsverbundes verpflichtet, dem N-CERT als Zentralstelle für Informationssicherheit Sicherheitsvorfälle in einer von ihr vorgegebenen Form unverzüglich mitzuteilen, wenn diese geeignet sind, auch die IT-Sicherheit bei anderen Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, zu beeinträchtigen. Für das Jahr 2021 wurden dem N-CERT 25 schwerwiegende Sicherheitsvorfälle aus der Landesverwaltung gemeldet. Für das Jahr 2022 wurden dem N-CERT 36 schwerwiegende Sicherheitsvorfälle gemeldet. Ein schwerwiegender Sicherheitsvorfall hat domänenübergreifende oder sonstige erhebliche Auswirkungen (vgl. Nr. 2.2 der Informationssicherheitsrichtlinie über den strukturierten Umgang mit Sicherheitsvorfällen). Es erfolgt bei der Erfassung durch das N-CERT jedoch keine spezifische Kategorisierung hinsichtlich der Verursachung durch Cyberangriffe oder Hackerattacken.

Mit Blick auf die Betroffenheit der Kommunalverwaltungen wird darauf hingewiesen, dass die Kommunen ihre IT und die Gewährleistung der IT-Sicherheit im Rahmen der kommunalen Selbstverwaltung eigenständig verantworten. Das Land unterstützt die Kommunen in beratender Funktion. Mangels gesetzlicher Verpflichtungen, IT-Sicherheitsvorfälle an das Land zu melden, werden solche daher nur dann bekannt, wenn diese seitens der betroffenen Kommune freiwillig an das N-CERT gemeldet werden. Im Jahr 2021 wurden dem N-CERT sieben schwerwiegende Sicherheitsvorfälle seitens der Kommunen gemeldet. Im Jahr 2022 wurden dem N-CERT drei schwerwiegende Sicherheitsvorfälle seitens der Kommunen gemeldet.

6. Welche Leistungen im Zusammenhang mit der NIS-Richtlinie (1 und 2), dem KRITIS-Dachgesetz und dem Onlinezugangsgesetz (OZG) haben das Computer-Emergency Response Team (N-CERT) und die niedersächsischen Digitallotsen seit dem Jahr 2021 erbracht?

Gemäß § 14 NDIG hat das N-CERT eine gesetzliche Verankerung als Zentralstelle für Informationssicherheit erfahren. Im Rahmen der Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) erfüllt das N-CERT darüber hinaus weitere Aufgaben innerhalb der Landesverwaltung. Zudem unterstützt es seit vielen Jahren die niedersächsischen Kommunalverwaltungen mit einem umfangreichen

Beratungsangebot. Diese Leistungen stehen nicht im Zusammenhang mit der NIS-2-Richtlinie, dem KRITIS-Dachgesetz und dem OZG.

Gleiches gilt für die Digitallotsen. „Digitallotsen“ ist weder ein geschützter Begriff noch eine Funktionsbezeichnung. Das Land Niedersachsen unterstützt die Qualifizierung von Mitarbeiterinnen und Mitarbeitern aus den niedersächsischen Kommunen zu sogenannten Digitallotsen. Es werden praxisnahe Kenntnisse und hilfreiche Instrumente, u. a. zum Digitalisierungsmanagement und der Informationssicherheit, vermittelt. Parallel hat es auch das Angebot einer entsprechenden Schulung für Mitarbeiterinnen und Mitarbeiter der unmittelbaren Landesverwaltung gegeben.

7. Welche Unterstützung plant das Land den Unternehmen und Kommunen bei der Erfüllung des NIS2UmsuCG zu leisten?

Unternehmen, kommunale Eigenbetriebe, kommunale Unternehmen und Zweckverbände, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, werden voraussichtlich aufgrund der Gesetzgebungskompetenz des Bundes in den Anwendungsbereich des Gesetzes über das Bundesamt in der Informationstechnik (BSIG) fallen. Insofern wird das Bundesamt für Sicherheit in der Informationstechnik die zuständige Aufsichtsbehörde sein, die die betroffenen Einrichtungen bei der Umsetzung vorrangig unterstützen wird. Dennoch bietet auch das Land Niedersachsen Unterstützungsangebote an. Es fanden sowohl für Unternehmen als auch für die niedersächsischen Kommunen bereits Informationsveranstaltungen statt, in denen die NIS-2-Richtlinie, die Umsetzung und die Anforderungen vorgestellt wurden. Mangels konkreter Regelungen sind konkretere Unterstützungsleistungen derzeit noch nicht planbar. Insbesondere gilt es zunächst, die Anforderungen aus der NIS-2-Richtlinie zu schärfen und diese an etablierten Standards zu orientieren.

8. Wie ist der Stand der Umsetzung der ITSiV-PV bei den Verwaltungen von Land und Kommunen in Niedersachsen? Welche Überschneidungsbereiche oder Dopplungen bestehen zu den BSI-Standards, dem ISMS und dem NIS2UmsuCG?

Für das Land Niedersachsen werden die IT-Komponenten im Portalverbund durch IT.Niedersachsen, dem zentralen IT-Dienstleister des Landes, betrieben. Unmittelbar und mittelbar an den Portalverbund angebundene Komponenten werden hierüber mit dem Portalverbund verknüpft. IT.Niedersachsen setzt die Regelungen der ITSiV-PV für diese IT-Komponenten weitgehend um. Für die bislang noch nicht vollständig umgesetzten Maßnahmen sind Umsetzungszeitraume festgelegt und erforderliche Risikoanalysen durchgeführt worden. Bereits jetzt werden zahlreiche Sicherheitsmaßnahmen auf der Grundlage von IT-Sicherheitskonzepten umgesetzt.

Die zentrale Stelle des Landes gemäß § 2 Abs. 13 ITSiV-PV wurde eingerichtet. Informationen über den Stand der Umsetzung der ITSiV-PV in den niedersächsischen Kommunen liegen der Landesregierung nicht vor.

Bei der Umsetzung der ITSiV-PV kommen bestimmte technische Richtlinien und BSI-Standards oder die ISO/IEC 2700X zur Anwendung. Bei einem Informationssicherheitsmanagement-System hingegen handelt es sich um ein übergreifendes Prozessmanagement, dass die Gewährleistung der Informationssicherheit sicherstellen soll. Insofern sind die Anforderungen der ITSiV-PV im Rahmen des ISMS zu berücksichtigen. Ebenso verhält es sich zukünftig mit den Umsetzungsregelungen zur NIS-2-Richtlinie.

9. Wie steht die Landesregierung zu der von der DIHK (und dem BDI) geäußerten Kritik an den Regelungen und Umsetzungsproblemen der NIS-2-Richtlinie?

Es wird auf die Vorbemerkung verwiesen.

(Verteilt am 16.02.2024)