Große Anfrage
mit Antwort der Landesregierung

Große Anfrage der Fraktion der AfD

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

Sicherheit der IT-Systeme in Wirtschaft und Verwaltung in Niedersachsen

Große Anfrage der Fraktion der AfD, eingegangen am 07.08.2024 - Drs. 19/5043
an die Staatskanzlei übersandt am 16.08.2024

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung
21.01.2025

Vorbemerkung der Fraktion

Die Absicherung von IT-Systemen gewinnt im Zusammenhang mit einer rasanten Digitalisierung und den damit einhergehenden Risiken verschiedenster Cyberangriffsmöglichkeiten eine immer größere Bedeutung.

In einer repräsentativen Umfrage[1] aus den Jahren 2018 und 2019 des Kriminologischen Forschungsinstituts Niedersachsen e. V., in welcher 5 000 Unternehmen befragt wurden, gaben damals rund 41 % der befragten Unternehmen an, in den vorhergehenden zwölf Monaten Ziel eines Cyberangriffs gewesen zu sein, auf den reagiert werden musste.

Angriffe mittels Schadsoftware bilden bei den unterschiedlichen Cyberangriffsarten neben den sogenannten Phishing-Angriffen einen Schwerpunkt der Bedrohungen. Von diesen Ransomware-Angriffen waren laut der Befragung in den vorangegangenen Monaten rund 12 % der Unternehmen betroffen.

Im Koalitionsvertrag der Regierungsparteien ist zu lesen, dass die Digitalisierung eine große Chance für unsere Gesellschaft ist. Mit dieser Großen Anfrage soll festgestellt werden, wie die Situation rund um das Thema Cybersicherheit für niedersächsische Unternehmen ist. Außerdem soll ermittelt werden, welche Maßnahmen, Programme oder finanzielle Hilfen sich bisher bewährt haben und welche noch notwendig sind, um niedersächsische Unternehmen wirksam gegen Cyberangriffe zu schützen und wirtschaftliche Schäden zu vermeiden oder in engen Ausmaßen zu begrenzen.

Im dritten Teil dieser in drei Bereiche aufgeteilten Anfrage soll die Sicherheitslage und der Umgang von Behörden mit Cyberangriffen beleuchtet werden.

Vorbemerkung der Landesregierung

Die Bedrohungslage durch die Gefahr von Cyberangriffen ist insgesamt so angespannt wie nie. Dies macht auch der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für das Jahr 2024[2] deutlich. Die Angreifenden unterscheiden oft nicht zwischen Unternehmen, öffentlicher Verwaltung oder Privatpersonen. Die Bedrohungslage durch Hackerattacken für die IT-Infrastruktur der öffentlichen Verwaltung in Niedersachsen stuft die Landesregierung auf Basis der Erkenntnisse sowohl des Niedersächsischen Computer Emergency Response Teams (N-CERT) als auch der Sicherheitsbehörden unverändert auf einem erhöhten Niveau ein.

---

1 https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5, S. 16 ff., zuletzt aufgerufen am 02.12.2024.

*) Die Drucksache 19/6272 - verteilt am 21.01.2025 - ist durch diese Fassung zu ersetzen. Korrektur der Antwort zu Frage 24.

Im Bereich der Cyberkriminalität sind in den letzten Jahren der Bereich der Lösegelderpressung im Zusammenhang mit Verschlüsselungstrojanern (sogenannte Ransomware-Attacken) und sogenannte Überlastungsangriffe (Distributed Denial of Service, DDoS) immer bedeutender geworden. Zugleich nimmt auch die Bedrohung der öffentlichen digitalen Infrastrukturen durch kriminelle Gruppierungen weiter zu. Neben direkten Angriffen auf die Infrastruktur, bei denen die Schadsoftware beispielsweise über E-Mail verteilt wird, stellen Angriffe auf Software-Lieferanten (Supply-Chain-Angriffe) eine ernstzunehmende Bedrohung für die IT-Sicherheit dar. Hierbei wird Schadsoftware über manipulierte Anwendungen von an sich vertrauenswürdigen Vertragspartnern in eine Organisation eingebracht. Die zunehmende Verflechtung zwischen physischer und digitaler Welt erfordert robuste Resilienzmaßnahmen gegen Bedrohungen aller Art.

Neben der zunehmenden hybriden Bedrohung verstärken weitere Faktoren die ohnehin angespannte Cyberbedrohungslage insbesondere für die Wirtschaft. Dazu zählen beispielsweise ein fortdauernder „Systemwettbewerb“ mit staatlich gelenkten Wirtschaftssystemen, ein hohes Niveau an mobilem Arbeiten, die zunehmende Verbreitung des Internet of Things (IoT) wie auch die Entwicklungen in den Bereichen Künstliche Intelligenz (KI) und Quantencomputer. Aufgrund dieser Bedrohungslage ist ein hohes Sicherheitsniveau für Unternehmen, insbesondere für Einrichtungen der kritischen Infrastruktur, zu schaffen und im Sinne der Daseinsvorsorge auch die Handlungsfähigkeit des Staates zu schützen. In diesem Kontext sei auf bestehende gesetzliche und untergesetzliche Regelungen hingewiesen.

Der Landtag hat mit dem Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) bereits 2019 einen modernen Rechtsrahmen geschaffen. Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, bilden einen Sicherheitsverbund. Jedes Mitglied des Sicherheitsverbundes hat auf der Basis von Risikoanalysen eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit, auch im Hinblick auf andere Mitglieder des Sicherheitsverbundes, zu gewährleisten. Für weite Bereiche der Verwaltung sind durch die Niedersächsische Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) und das darauf basierende Informationssicherheitsmanagementsystem (ISMS) der Niedersächsischen Landesverwaltung untergesetzliche Regelungen getroffen worden, die der Gewährleistung der Informationssicherheit für die unmittelbare Landesverwaltung dienen. Besonders kritische Teile der Landesverwaltung werden durch den am 29.10.2024 beschlossenen gemeinsamen Runderlass der Staatskanzlei und der übrigen Ministerien „Umsetzung der NIS-2-Richtlinie in Niedersachsen (NIS2UmsRdErl)“ adressiert. Einrichtungen im Anwendungsbereich haben erweiterte Anforderungen zur Cybersicherheit zu erfüllen, z. B. hinsichtlich ihres Risikomanagements oder ihrer Meldepflichten bei erheblichen Sicherheitsvorfällen.

Für bundesrechtlich regulierte Bereiche hat der Bundesgesetzgeber mit dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) u. a. eine Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen und Regelungen für Unternehmen im besonderen öffentlichen Interesse getroffen. In diesem Zusammenhang ist auch die Datenschutzgrundverordnung zu nennen, die für die Verarbeitung personenbezogener Daten festlegt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Mit Blick auf die Betroffenheit der Kommunalverwaltungen sei vorausgeschickt, dass die Kommunen ihre IT im Rahmen der kommunalen Selbstverwaltung eigenständig betreiben und daher auch eigenverantwortlich die IT-Sicherheit zu gewährleisten haben. Gleiches gilt für Unternehmen der Privatwirtschaft; verantwortlich für deren Sicherheit sind die Unternehmensleitungen. IT-Sicherheitsvorfälle im kommunalen und privatwirtschaftlichen Bereich werden gegenüber dem Land in der Regel nur dann bekannt, wenn diese seitens der betroffenen Einrichtung freiwillig gemeldet oder über die Presse veröffentlicht werden.

Die Landesregierung unterstützt Kommunen und Unternehmen bei deren eigenverantwortlicher Wahrnehmung ihrer Aufgaben im Bereich Cybersicherheit, baut diese Angebote weiter aus und koordiniert sie. Beispielsweise bietet das Niedersachsen-CERT, das Computer-Notfallteam des Landes (Computer Emergency Response Team), seinen Warn- und Informationsdienst auch den Kommunen an; die Niedersachsen.next Digitalagentur, der Verfassungsschutz und die Landespolizei informieren

Unternehmen etwa zu einschlägigen Förderprogrammen, zu Schutzmaßnahmen oder zur Schadensbegrenzung bei Cybersicherheitsvorfällen. Aus Sicht der Landesregierung gilt es, Unternehmen und Behörden in Niedersachsen für den Umgang mit Cybergefährdungen zu ertüchtigen. Hierzu gehört auch, zu beraten, zu sensibilisieren und eine potenzielle Anzeigebereitschaft zu erreichen. Um Cyberangriffe schon im Vorfeld abzuwehren bzw. auf deren Bewältigung vorbereitet zu sein, müssen Unternehmen und Behörden in Niedersachsen in eigener Zuständigkeit umfangreiche Management-Maßnahmen treffen und in ihrer Organisationsstruktur verankern. Das umfassende Unterstützungsangebot des Landes sowie die am 24.09.2024 durch die Landesregierung beschlossene Cybersicherheitsstrategie des Landes Niedersachsen tragen dazu bei, die Cybersicherheitsarchitektur in Niedersachsen zu stärken.

I. Cyberangriffe und Cybersicherheit bei Unternehmen, an denen das Land Niedersachsen beteiligt ist

1. Welche Kenntnisse hat die Landesregierung über Cyberangriffe auf die IT bei Unternehmen im Zeitraum von 2018 bis 2023, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist (bitte aufschlüsseln nach Jahren und Art der Angriffe, wie beispielsweise Ransomware-Angriffe oder Angriffe über Schadprogramme)?

Die nachfolgende Tabelle führt die der Landesregierung bekannte Anzahl der Cyberangriffe auf Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, für den angefragten Zeitraum auf:

2018	2019	2020	2021	2022	2023
8	10	19	16	10	7

Bei den Angriffen handelt es sich um unterschiedliche Angriffsarten wie Spyware/Malware, Cross-Site Scripting, Phishing, SQL-Injections, Ramsomware, Botnet-Angriffe, Remote-Code-Execution, Credential-Stuffing, SPAM-Wellen, Überlastungsangriffe (Distributed Denial of Service, DDoS), Attacken auf Firmen-Webseiten und anderes mehr.

Eine valide Zuordnung der Angriffsart zu den einzelnen Angriffen und den Zeiträumen ist nicht möglich, da dies von den Unternehmen nicht in der Weise aufgezeichnet wird.

2. Welche Schäden sind den in Frage 1 benannten Unternehmen im besagten Zeitraum entstanden (bitte jeweils aufschlüsseln nach Jahren)?

Die nachfolgende Tabelle führt den der Landesregierung bekannten monetär entstandenen Gesamtschaden aufgrund der Cyberangriffe für Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, für den angefragten Zeitraum auf:

(Werte in Euro)

2018	2019	2020	2021	2022	2023
-	1 800	270 500	-	-	11 000

Hierbei handelt es sich um keine abschließende Bezifferung des monetären Schadens. Weitere Schäden sind von den Unternehmen als nicht bezifferbar genannt worden, beispielsweise eventuelle Umsatzverluste oder zusätzliche Personalaufwände.

3. Was sind nach Kenntnis der Landesregierung die am häufigsten aufgetretenen Schwachstellen in der Cybersicherheit dieser Unternehmen?

Welche konkreten Schwachstellen bei den in der Antwort zu Frage 1 genannten Unternehmen vorlagen bzw. ausgenutzt worden sind, ist nicht vollumfänglich bekannt.

Häufig werden nach Cyberangriffen folgende Schwachstellen identifiziert:

Veraltete Software und Systeme, schwache Passwörter, mangelnde Mitarbeitenden-Sensibilisierung, fehlende oder unzureichende Datensicherung, offene Ports und Dienste, mangelnde Zugriffskontrollen, fehlende Patch-Management-Strategie, unverschlüsselte Datenübertragungen, mangelhafte Netzwerksicherheit.

4. Bei welchen Cloud-Betreibern sind die Daten gespeichert, auf die die Unternehmen Zugriff haben, und welche der Cloud-Betreiber haben ihren Sitz in Deutschland bzw. der Europäischen Union (bitte für jedes Unternehmen, an dem das Land Niedersachsen beteiligt ist, einzeln aufschlüsseln)?

Allgemein kann beantwortet werden, dass diejenigen Unternehmen mit Landesbeteiligung, die Cloud-Dienste verwenden, nach Kenntnisstand der Landesregierung zum größten und überwiegenden Teil Cloudbetreiber in Deutschland bzw. der Europäischen Union und nur zu einem kleinen Teil außerhalb der Europäischen Union nutzen.

Die Landesregierung braucht einem Auskunftsverlangen nicht zu entsprechen, soweit zu befürchten ist, dass durch das Bekanntwerden von Tatsachen schutzwürdige Interessen Dritter verletzt werden, Artikel 24 Abs. 3 Satz 1 Alt. 3 Niedersächsische Verfassung (NV). Zu den schutzwürdigen Interessen Dritter gehört beispielsweise der grundrechtliche Schutz von Betriebs- und Geschäftsgeheimnissen. Eine detailliertere Beantwortung der Frage ginge mit einer Verletzung von Geschäftsgeheimnissen einher, zudem besteht aus Sicherheitsgründen keine detailliertere Berichtspflicht. Die Auswahl des jeweiligen Cloudanbieters stellt eine geheime Information dar, die Gegenstand angemessener Geheimhaltungsmaßnahmen ist und hinsichtlich derer ein berechtigtes Interesse an der Geheimhaltung besteht, mithin ein Betriebs- und Geschäftsgeheimnis gemäß § 2 Nr. 1 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Die Liste der Cloudanbieter ist weder allgemein bekannt noch leicht zugänglich, da sie nur für einen begrenzten Personenkreis bestimmt ist. Für die Unternehmen mit Landesbeteiligung besteht ein berechtigtes Interesse an der Geheimhaltung, da diese Information vertrauliche Details der IT-Infrastruktur betrifft, deren Offenlegung Dritten Einblicke in Datenspeicherungsstrategien gewähren und potenziell sicherheitsrelevante Schwachstellen offenlegen kann. Eine Veröffentlichung dieser Details könnte von Mitbewerbern oder potenziellen Angreifern ausgenutzt werden, was erhebliche Sicherheitsrisiken für die Einrichtungen darstellen würde. Die Landesregierung hat ein berechtigtes Interesse daran, dass diese Informationen nicht für gezielte Cyberangriffe (beispielsweise unter Vorspiegelung eines falschen Absenders / einer falschen Identität) gegen die Unternehmen mit Landesbeteiligung verwendet werden können. Es handelt sich um sensible Informationen und Geschäftsentscheidungen, die von wesentlicher Bedeutung sind.

5. Hat die Landesregierung auf die Unternehmen, an denen das Land Niedersachsen beteiligt ist, eingewirkt, die Cloud eines deutschen oder europäischen Betreibers zu nutzen?

Es wurde in der Regel seitens der Landesregierung nicht auf Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, eingewirkt. In Einzelfällen kann ein Einwirken durch entsprechende Anforderungen bei der Vergabe von Aufträgen erfolgen.

6. Wie viele und welche IT-Schulungen fanden im Zeitraum von 2018 bis 2023 in den Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, statt?

Die Anzahl der nach Kenntnis der Landesregierung im angefragten Zeitraum durchgeführten IT-Schulungen ist der nachfolgenden Tabelle zu entnehmen:

2018	2019	2020	2021	2022	2023
1 312	1 517	1 751	4 242	3 295	2 951

Entsprechend dem Adressatenkreis des Unternehmens sind diverse Schulungsangebote unterbreitet und von den Beschäftigten angenommen worden. Zu den im angefragten Zeitraum aufgeführten

IT-Schulungen zählen neben IT-Sicherheitsgrundschulungen auch spezialisierte Informationssicherheitsschulungen sowohl für die Nutzung als auch für die Entwicklung von Systemen, IT-Schulungen, Schulungen zur Netzwerksicherheit und Cyberkriminalität, zu Leitlinien im Umgang mit IT-Sicherheit, (dienstlichen) Mobilgeräten, zur System- und Benutzerverwaltung, zu Regelungen zu Passwörtern bzw. Passwortphrasen, zum sicheren Arbeiten im Büro, zu Schutzmaßnahmen gegen Computerschädlinge und Internetbetrug, Sicherheit bei Virtualisierungsumgebungen, Erkennung von Störungen, Sicherheitsaspekten bei Cloud-Nutzung, zu Wirtschaftsspionage, Spezialschulungen zu Sicherheitsaspekten bei einzelnen Anwendungen, zu Angriffstechniken, zum Management samt geeigneter organisatorischer Maßnahmen und andere mehr.

7. In welcher Höhe geben die Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, jährlich Geld für Cybersicherheit aus (bitte aufschlüsseln nach Jahren für den Zeitraum der letzten fünf Jahre)?

Die nachfolgende Tabelle zeigt die Gesamtsummen im Zeitraum 2019 bis 2023 auf:

(Werte in Euro)

2019	2020	2021	2022	2023
1 931 900	2 383 700	2 531 800	2 709 900	2 931 500

8. Welche Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, nutzen „HoneySens“ bzw. haben sich diese Lösung in Form einer Open-Source-Lizenz entsprechend ihren Kundenbedürfnissen anpassen lassen?

Die Landesregierung braucht einem Auskunftsverlangen nicht zu entsprechen, soweit zu befürchten ist, dass durch das Bekanntwerden von Tatsachen dem Wohl des Landes Nachteile zugefügt oder schutzwürdige Interessen Dritter verletzt werden, Artikel 24 Abs. 3 Satz 1 Alt. 2 und 3 NV. Eine detailliertere Beantwortung der Frage ginge mit einer Verletzung von Geschäftsgeheimnissen einher, zudem besteht aus Sicherheitsgründen keine detailliertere Berichtspflicht. Der Einsatz oder Nichteinsatz bestimmter Sicherheitsmaßnahmen und -techniken stellt eine geheime Information dar, die Gegenstand angemessener Geheimhaltungsmaßnahmen ist und hinsichtlich derer ein berechtigtes Interesse an der Geheimhaltung besteht. Informationen über konkrete Maßnahmen zur Angriffserkennung in Unternehmensnetzwerken sind weder allgemein bekannt noch leicht zugänglich, da sie nur für einen begrenzten Personenkreis bestimmt sind. Für die Unternehmen mit Landesbeteiligung besteht ein berechtigtes Interesse an der Geheimhaltung, da diese Information vertrauliche Details der IT-Infrastruktur betrifft, deren Offenlegung Dritten Einblicke in Detektionsmechanismen gewähren und potenziell sicherheitsrelevante Schwachstellen offenlegen kann. Eine Veröffentlichung dieser Details könnte von potenziellen Angreifern ausgenutzt werden, was erhebliche Sicherheitsrisiken für die Einrichtungen darstellen würde. Die Landesregierung hat ein berechtigtes Interesse daran, dass diese Informationen nicht für gezielte Cyberangriffe gegen die Unternehmen mit Landesbeteiligung verwendet werden können.

9. Ist der Landesregierung bekannt, ob und, falls ja, mit welchen Maßnahmen die Betriebe, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, ihre Mitarbeiter für das Thema Cybersicherheit sensibilisieren?

Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, sensibilisieren ihre Mitarbeitenden regelmäßig für das Thema Cybersicherheit. Die Sensibilisierung erfolgt überwiegend durch Schulungen und Informationsweitergabe, z. B. durch Intranet-Meldungen, E-Mails oder Besprechungen. Weitere verwendete Sensibilisierungsmaßnahmen sind das Bereitstellen von Cybersicherheitsplattformen, Berichte über Cybervorfälle in anderen Unternehmen, Datenschutzvereinbarungen in den Arbeitsverträgen, Passwortrichtlinien, Durchführung von Trainings, Phishing-Kampagnen, interne Security-Checks durch externe Unternehmen und anderes mehr.

Siehe auch Antwort zu Frage 6.

10. Ist der Landesregierung bekannt, inwieweit Homeoffice-Arbeitsplätze in den Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, in den Jahren 2020 und 2021 von Cyberangriffen betroffen waren (bitte aufschlüsseln nach Jahren und Anzahl, sofern es Cyberangriffe gab)?

Der Landesregierung ist nicht bekannt, dass Homeoffice-Arbeitsplätze von Unternehmen, an denen das Land Niedersachsen unmittelbar bzw. mittelbar beteiligt ist, in den Jahren 2020 und 2021 von Cyberangriffen betroffen waren.

11. Ist der Landesregierung bekannt, ob die Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, gegen Cyberangriffe versichert sind? Falls ja, welche Unternehmen sind in welchem Umfang versichert?

Allgemein kann beantwortet werden, dass der Landesregierung Informationen über entsprechende Versicherungen von Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, vorliegen.

Unter Bezugnahme auf die Begründung zu Frage 4 kann im Übrigen keine detailliertere Antwort erfolgen. Diese Informationen sind in den Unternehmen nur einem engen, ausgewählten Kreis an Personen bekannt. Das berechtigte Interesse liegt darin begründet, dass Informationen über die wirtschaftliche Absicherung der IT-Sicherheit eine Profilierung des Unternehmens ermöglichen, die geeignet sein kann, eine Angriffsentscheidung für gezielte IT-Angriffe zu begründen und Erpressungen gegen das Unternehmen präzise zu gestalten. Mit jedem Informationsdetail wird daher die gezielte Angreifbarkeit und die Wahrscheinlichkeit eines gezielten Angriffes erhöht.

12. Welche Kenntnisse besitzt die Landesregierung über den gegenwärtigen Investitionsbedarf in IT-Sicherheit bei den Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist?

Der gegenwärtige Investitionsbedarf der Unternehmen, an denen das Land Niedersachsen unmittelbar oder mittelbar beteiligt ist, unterscheidet sich signifikant je nach Unternehmen. Die Spanne reicht von Unternehmen, die keinen gegenwärtigen Investitionsbedarf sehen, bis hin zu Unternehmen, die einen gegenwärtigen Investitionsbedarf von über 500 000 Euro pro Jahr sehen.

II. Cyberangriffe und Cybersicherheit bei kleinen und mittleren Unternehmen (KMU)

13. Beabsichtigt die Landesregierung, bei den KMU in Niedersachsen in nächster Zeit Unternehmensbefragungen zur Cybersicherheit durchzuführen, bzw. wurden in den Jahren 2020 und 2021 Unternehmensbefragungen in dieser Gruppe durchgeführt? Falls ja, mit welchen Ergebnissen, bzw. welche Handlungsempfehlungen sind aus den Befragungsergebnissen abzuleiten?

In den Jahren 2020 und 2021 wurden keine Unternehmensbefragungen zur Cybersicherheit durchgeführt.

Mit Blick auf die wiederkehrenden Studien zum Thema IT- und Cybersicherheit, etwa des BSI, des Branchenverbandes Bitkom e. V. und der Deutschen Industrie- und Handelskammer (DIHK) sowie nunmehr auch von der HDI-Versicherung, plant die Landesregierung derzeit keine Befragungen in nächster Zeit.

14. Welche IT-Fachfirmen haben in den Jahren 2022 und 2023 niedersächsische KMU zum Thema Cybersicherheit beraten, und wie hoch waren die Kosten dafür?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

Nach Auskunft der von der Landesregierung zu dieser Frage beteiligten niedersachsen.digital, des Digitalverbandes unter dem Dach der Unternehmerverbände Niedersachsen (UVN), gibt es eine Reihe an dortigen Mitgliedsunternehmen, die in diesem Bereich tätig sind. Die Anbieter bedienen unterschiedlichste Themenfelder. Angaben zu den Kostenaufwendungen wurden gegenüber der Landesregierung hierbei nicht gemacht.

15. Wie viele Veranstaltungen hat die Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) für niedersächsische Unternehmen im Bereich Cybersicherheit im Jahr 2023 durchgeführt, und welche Schwerpunkte wurden thematisch bei diesen Veranstaltungen gesetzt?

Die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes (LKA) Niedersachsen hat im Jahr 2023 insgesamt 114 Veranstaltungen im Sinne der Anfrage durchgeführt.

Die ZAC bietet u. a. Veranstaltungen und Vorträge an, in denen allgemeine Gefahren im Internet thematisiert werden. Es werden auch zielgerichtete Veranstaltungen für Geschäftsführungen, Mitarbeitende oder die IT-Bereiche von niedersächsischen Unternehmen angeboten. Ein sehr erfolgreiches Veranstaltungs-/Präventionsformat sind die sogenannten Cyberabwehrübungen bzw. Planspiele für niedersächsische Wirtschaftsunternehmen, die durch die ZAC gemeinsam mit der Industrie- und Handelskammer (IHK) Niedersachsen sowie einer Unternehmensberatung veranstaltet werden. Im Rahmen der Cyberabwehrübungen versuchen die Teilnehmenden, in Krisenteams einen simulierten (realitätsnahen) Ransomware-Angriff auf eine fiktive Firma zu bewältigen. Dabei werden die Teilnehmenden zielgerichtet durch anwesende Mitarbeitende der ZAC beraten und unterstützt. Das Ziel der hier benannten Übungen besteht insbesondere darin, die notwendigen Reaktionen bei einem Ransomware-Angriff kennenzulernen bzw. zu optimieren sowie grundsätzlich die Resilienz der Unternehmen im Bereich Cyberabwehr zu fördern. Darüber hinaus werden u. a. auch die polizeilichen Unterstützungsleistungen im Schadensfall sowie Präventionshinweise vermittelt.

16. Wie ist die Studienlage zur Internetkriminalität und zu Cyberangriffen im Land Niedersachsen? Sind aktuelle Studien durch die Landesregierung in Auftrag gegeben? Werden Studien, bei denen die Auftraggeber Dritte sind, vom Land Niedersachsen finanziert?

Durch das LKA Niedersachsen werden seit dem Jahr 2013 unter dem Titel „Befragung zu Sicherheit und Kriminalität in Niedersachsen“ sogenannte Dunkelfeldstudien durchgeführt. Dabei wird auch der Deliktsbereich Cybercrime abgebildet. Diese repräsentativen Dunkelfeldstudien, bei denen jeweils 40 000 Personen ab 16 Jahren mit Hauptwohnsitz in Niedersachsen angeschrieben und um Teilnahme gebeten werden, erfolgen grundsätzlich im zweijährigen Turnus und werden fortlaufend aktualisiert. Die Befragung im Jahr 2015 enthielt einen Schwerpunktfragenkomplex zu Cybercrime. Die Ergebnisse der jeweiligen Dunkelfeldstudien sind im Internet veröffentlicht.[3]

In einige übergreifende Studien und Lageberichte sind auch Daten zu Einrichtungen in Niedersachsen eingeflossen. Zu diesen Studien gehört auch das bereits genannte Forschungsvorhaben des Kriminologischen Forschungsinstituts Niedersachsen e. V. (KFN) in Zusammenarbeit mit PricewaterhouseCoopers GmbH (PwC) unter dem Titel „Cyberangriffe gegen Unternehmen“. Die Ergebnisse dazu sind veröffentlicht, das Projekt ist näher beschrieben unter www.cybercrime-forschung.de. Die Studie mit ca. 5 000 befragten Unternehmen ist dabei sehr umfangreich.

17. Wie viele KMU in Niedersachsen, an denen das Land Niedersachsen nicht unmittelbar oder mittelbar beteiligt ist, nutzen „HoneySens“ bzw. haben sich diese Lösung in Form einer Open-Source-Lizenz entsprechend ihren Kundenbedürfnissen anpassen lassen?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

[3] https://www.lka.polizei-nds.de/forschung/dunkelfeldstudie/dunkelfeldstudie-115379.html

18. Wie viele Cyberangriffe auf Unternehmen wurden in Niedersachen in den Jahren 2022 und 2023 sowie im ersten Halbjahr 2024 jeweils angezeigt?

Aufgrund von bundesweit einheitlichen Regularien der polizeilichen Kriminalstatistik (PKS) werden in der PKS nur die Straftaten berücksichtigt, bei denen der Tatort in Deutschland liegt. Dabei wird der Tatort auf den Ort beschränkt, an dem der Täter oder die Täterin handelt. Da höherwertige und komplexere Straftaten von Cybercrime (sogenannte Cybercrime im engeren Sinne) in der Mehrzahl über weltweite Datennetze begangen werden, kann der Handlungsort der Täterinnen und Täter oft nicht eindeutig festgestellt werden mit der Folge, dass diese Straftaten in der PKS keine Berücksichtigung finden. Weiterhin können konkrete Geschädigte, sowohl Firmen, Unternehmen und Behörden als auch Personen, aufgrund der Anonymisierung nicht individuell aus der PKS herausgelesen werden.

Um zu den Phänomenen Ransomware und DDoS dennoch qualitätsgeprüfte Aussagen treffen zu können, wurde in der ZAC des LKA Niedersachsen ein Monitoring auf Grundlage der Daten aus dem polizeilichen Vorgangsbearbeitungssystem NIVADIS eingerichtet. Die im Rahmen des sogenannten Monitorings Cybercrime erhobenen Fallzahlen hinsichtlich betroffener Institutionen für Niedersachsen werden nachfolgend tabellarisch dargestellt:

	Ransomware	DDoS
2022	104	15
2023	79	15
2024, 1. HJ	21	4

19. Ist der Landesregierung bekannt, ob KMU in Niedersachsen in einer messbaren Größenordnung gegen Cyberangriffe versichert sind?

Daten speziell zur Lage in Niedersachsen sind der Landesregierung nicht bekannt.

20. Welche politischen Maßnahmen erachtet die Landesregierung gegebenenfalls für sinnvoll, um zeitnah Cyberangriffe auf niedersächsische Unternehmen einzudämmen?

Maßgeblich für eine effektive Eindämmung sind funktionierende Präventions-, Detektions- und Reaktionsprozesse in den Unternehmen. Dies unterstützt die Landesregierung auf strategischer und operativer Ebene. Mit der Cybersicherheitsstrategie für das Land Niedersachsen hat die Landesregierung am 24.09.2024 eine Handlungsgrundlage verabschiedet. Weitere politische Rahmenbedingungen werden maßgeblich durch die EU und den Bund gesetzt, etwa mit der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) und deren Umsetzung. Grundsätzliche Impulse werden schließlich vom digital.Rat eingeholt.

Die Umsetzung der NIS-2-Richtlinie erfolgt für den Mitgliedstaat Deutschland - insbesondere soweit Unternehmen betroffen sind - im Wesentlichen durch Bundesrecht. Aus Sicht der Landesregierung ist eine zeitnahe Umsetzung der NIS-2-Richtlinie und der damit verbundenen Maßnahmen erforderlich. Die Überprüfung bestehender technischer Infrastrukturen, deren Optimierung und Aktualisierung sind dabei zwingende Voraussetzung, um ein Sicherheitsniveau, wie in der NIS-2-Richtlinie gefordert, erreichen zu können.

Operativ wird mit dem Digitalbonus.Niedersachsen-innovativ Unternehmen die Möglichkeit gegeben, aufsetzend auf einen Innovationsschub Gelder für Cybersicherheitsmaßnahmen zu beantragen. Parallel wird das Angebot der Niedersachsen.next Digitalagentur durch die Kooperation mit der Transferstelle Cybersicherheit und mit dem European Digital Innovation Hub für KI und Cybersicherheit (DAISEC) in Beratung, Wissenstransfer und Aufklärung ausgebaut.

Ein Cyberangriff auf ein niedersächsisches Unternehmen setzt die Interaktion eines Akteurs voraus. Diese Handlungen an sich einzudämmen oder zu verhindern, ist auch seitens der Sicherheitsbehörden oft nicht möglich. Das Beratungs- und Dienstleistungsangebot des Wirtschaftsschutzes zielt da-

her darauf ab, Unternehmen dahin gehend zu informieren und zu sensibilisieren, Angriffe frühestmöglich zu erkennen sowie Schutzmaßnahmen im Vorfeld zu installieren. Dies verhindert nicht unbedingt die Handlungen eines fremden Akteurs, aber im besten Fall eine schadhafte Auswirkung.

Mit dem Krieg in der Ukraine geht eine Strategie der „hybriden Kriegsführung“ einher. Diese ist mit verschiedenen Formen illegitimer Einflussnahme auf Staaten und Gesellschaften durch fremde Staaten verbunden und umfasst gerade auch Cyberangriffe und Desinformationskampagnen. Dem hat die Landesregierung dahin gehend Rechnung getragen, eine zentrale Ansprechstelle für die länder-, ressort- und ebenenübergreifende Vernetzung einzurichten - einen sogenannten Single Point of Contact (SPoC) Hybrid. Dieser SPoC ist im Ministerium für Inneres und Sport (MI), in der Abteilung 5 (Verfassungsschutz), angebunden. Er hat die vorrangige Aufgabe der Schaffung klarer Informations- und Kommunikationsstrukturen in der länder-, ressort- und ebenenübergreifenden Vernetzung, um umgehende Informationssteuerungen und Sensibilisierungen zu gewährleisten.

Die übergreifende strategische Koordination der heutigen und der künftigen Maßnahmen der Landesregierung im Bereich Cybersicherheit ist sowohl innerhalb des Landes als auch hinsichtlich der Zusammenarbeit mit dem Bund und den anderen Ländern unbedingt erforderlich. Hierfür setzt sich die Landesregierung auch weiterhin konsequent ein.

21. Inwiefern sind niedersächsische Behörden ausreichend vorbereitet und ausgestattet, um vor allem KMU bei Fragen zur IT-Sicherheit wirksam zu unterstützen?

Eine Aufgabe der Unterstützung von KMU im Bereich Cybersicherheit liegt operativ bei der Niedersachsen.next Digitalagentur und ihren Partnern wie der Transferstelle Cybersicherheit und DAISEC. Ihre Angebote stellen sich nach heutiger Einschätzung als angemessen dar. Sie werden umfangreich wahrgenommen, dennoch können aber regelmäßig alle interessierten Unternehmen an den Angeboten teilnehmen.

Um der steigenden Gefahr von Cyberkriminalität entgegenzuwirken, wurden im Jahr 2011 zudem in jedem Bundesland bei den Landeskriminalämtern sowie beim Bundeskriminalamt (BKA) die ZAC gegründet. Sie stehen als professionelle Ansprechstellen für Behörden, Unternehmen und Verbände zur Verfügung. Ihr Schwerpunkt liegt dabei einerseits auf der Prävention und Verhinderung von Cyberangriffen durch entsprechende Sensibilisierungsformate. Andererseits stehen die ZAC-Dienststellen auch nach einem Angriff für öffentliche Einrichtungen und Unternehmen als Beratungsinstanzen zur Verfügung.

Im Angriffsfall - auch außerhalb der Regelarbeitszeit - erhalten die betroffenen Unternehmen regelmäßig Unterstützung durch die Fachkommissariate Cybercrime der regionalen Polizeidirektionen oder im Einzelfall auch durch die bei der ZAC angesiedelte Quick-Reaction-Force des LKA Niedersachsen. Neben der Initiierung strafverfolgender Maßnahmen beraten und unterstützen die Ermittlerinnen und Ermittler sowie Cyber-Forensiker die betroffenen Unternehmen intensiv.

Die Polizei Niedersachsen begegnet dem Deliktsphänomen Cybercrime durch spezialisierte Sachbearbeitung, die sowohl in der Abteilung 6 des LKA Niedersachsen (Digitales Service- und Kompetenzzentrum) als auch in den Fachkommissariaten Cybercrime der Polizeidirektionen vorhanden ist. Die Bearbeitung von Sachverhalten mit Cybercrimebezug wird dort durch speziell fortgebildete Polizeibeamtinnen und -beamte sowie IT-Spezialistinnen und -Spezialisten gewährleistet.

Im Allgemeinen beeinflussen verschiedenste Umstände die Wirksamkeit der Unterstützung, vor allem bei KMU. Dabei sind insbesondere folgende Aspekte zu nennen:

– Allgemeine Dynamik von Bedrohungslagen

  Die IT-Sicherheitslandschaft verändert sich rasant. Die Behörden müssen mit der Dynamik neuer Technologien und neuer Angriffsszenarien Schritt halten. Das zuständige Personal der Polizei Niedersachsen befasst sich daher fortlaufend mit aktuellen Entwicklungen und nimmt dabei entsprechende Fortbildungsangebote bei internen sowie externen Anbietern in Anspruch.

– Vielfalt der KMU

  KMU sind sehr heterogen. Sie unterscheiden sich in Größe, Branche, digitaler Reife und damit auch in ihren spezifischen IT-Sicherheitsbedürfnissen. Die ZAC des LKA Niedersachsen bereitet entsprechende Beratungs- und Präventionsformate zielgerichtet und individuell anhand o. g. Parameter vor und agiert somit zielgruppenadäquat. Die ZAC des LKA Niedersachsen ist aktuell personell und technisch ausreichend ausgestattet, um die KMU bei Fragen zur IT-Sicherheit wirksam zu unterstützen.

– Kooperation mit anderen Akteuren

  Eine effektive Unterstützung von KMU erfordert eine enge Zusammenarbeit mit der Wirtschaft, IT-Sicherheitsunternehmen und anderen Behörden. Entsprechende Kooperationen werden durch die ZAC des LKA Niedersachsen anlassbezogen eingegangen, beispielsweise für o. g. Präventionsformate wie die Cyberabwehrübungen, die gemeinsam mit der IHK und einer Unternehmensberatung durchgeführt werden. Das LKA Niedersachsen ist zudem Mitglied einer Sicherheitskooperation mit dem Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom) e. V.

  Neben dem LKA Niedersachsen bietet beispielsweise auch das MI, Abteilung 5 (Verfassungsschutz), Beratungs- und Förderangebote für KMU im Bereich IT-Sicherheit an, z. B. im Rahmen der jährlichen Wirtschaftsschutztagung. Durch diese vielfältigen Angebote von Polizei und Verfassungsschutz bestehen Netzwerke und Plattformen, die den Austausch zwischen Behörden, Wirtschaft und Wissenschaft fördern und interessierte niedersächsische Unternehmen bei Fragen der IT-Sicherheit unterstützen.

22. Welche Förderungen für Mitarbeiterschulungen durch Landesmittel im Bereich der Cybersicherheit existieren für KMU, und inwieweit wurden die Mittel abgerufen (bitte aufschlüsseln für die Jahre 2022 und 2023)?

Für die Jahre 2022 und 2023 gab es keine dezidierten Förderprogramme des Landes zur Weiterbildung im Bereich Cybersicherheit.

23. Sieht die Landesregierung bei der Bekämpfung der Cyberkriminalität Lücken beim Informationsaustausch zwischen Behörden und betroffenen Unternehmen? Falls ja, welche und wie sollen diese geschlossen werden?

Aus Sicht der Landesregierung bestehen mitunter deutliche Lücken beim Informationsaustausch zwischen Behörden und von Cyberattacken betroffenen Unternehmen. Nicht alle betroffenen Unternehmen melden Cyberangriffe, z. B. aus Angst vor Reputationsverlust, weil sie die Auswirkungen unterschätzen oder weil Unternehmen Bedenken hinsichtlich des Schutzes ihrer Geschäftsgeheimnisse haben. Dies erschwert es den Behörden, ein umfassendes Bild der Bedrohungslage zu gewinnen und gezielte Maßnahmen zu ergreifen. Im Bereich Cybercrime muss daher von einem hohen Dunkelfeld ausgegangen werden. Es besteht daher weiterhin ein großer Bedarf, die KMU für die Risiken von Cyberangriffen zu sensibilisieren und für präventive Cybersicherheitsmaßnahmen zu gewinnen. Insbesondere mit der Umsetzung der NIS-2-Richtlinie ist eine Vielzahl von Unternehmen gefordert, höhere Sicherheitsanforderungen umzusetzen. Die Landesregierung setzt darüber hinaus weiterhin auf umfassende und fortwährende Aufklärungskampagnen, um das Bewusstsein für Cyberrisiken in der Wirtschaft zu schärfen.

Die rechtlichen Grundlagen für die Zusammenarbeit zwischen Behörden und Unternehmen sind zudem oft komplex. Regelungen wie das KRITIS-Dachgesetz oder die NIS-2-Richtlinie sind daher zu begrüßen.

Bei der Aufgabenerfüllung sind die jeweiligen Zuständigkeiten zu beachten. Beispielsweise fällt die strafrechtliche Verfolgung und Bekämpfung von Cyberkriminalität nicht in den Aufgabenbereich des Verfassungsschutzes. Behördenintern findet im Rahmen der gesetzlichen Möglichkeiten ein guter

und regelmäßiger Austausch zwischen dem Verfassungsschutz (Cyberabwehr und Wirtschaftsschutz), dem LKA (ZAC), dem Grundsatzbereich Cybersicherheit sowie dem N-CERT statt. In der Kommunikation mit betroffenen Unternehmen ist der Informationsaustausch immer einzelfallabhängig davon, inwieweit ein Unternehmen bereit ist, Informationen mit den Sicherheitsbehörden zu teilen. Seitens des Verfassungsschutzes werden alle kommunizierbaren, d. h. nicht der Verschlusssachenanweisung unterliegenden, Informationen weitergeleitet und wird den Unternehmen signalisiert, als Ansprechpartner zur Verfügung zu stehen.

Im Hinblick auf den allgemeinen Informationsaustausch finden regelmäßige und vertrauensvolle Austauschformate zwischen Unternehmen und Behörden statt. Zu nennen sind etwa der Arbeitskreis IT-Sicherheit beim Wirtschaftsministerium, den die Niedersachsen.next Digitalagentur koordiniert. An diesem nehmen niedersächsische Unternehmen, IT-Dienstleister, Expertinnen und Experten sowie Sicherheitsbehörden und Ministerien teil. Über die Integration der Transferstelle Cybersicherheit in den Arbeitskreis und die zielgerichtete Erweiterung um wirtschaftliche Perspektiven wird der Austausch intensiviert. Des Weiteren nimmt das Land an sogenannten Fokusgruppen von niedersachsen.digital teil, bei denen ebenfalls einschlägige Akteure vertreten sind.

24. Warum wurde das Problem „Cybercrime“ nicht als eine eigene Herausforderung in dem Kapitel „Wirtschaft“ im aktuellen Koalitionsvertrag aufgenommen?

Der Koalitionsvertrag wurde ausschließlich zwischen den beiden Vertragsparteien verhandelt und abgestimmt. Die Landesregierung ist keine Vertragspartei, sodass ihr keine Erkenntnisse im Sinne der Fragestellung vorliegen.

25. Welche Kenntnisse besitzt die Landesregierung über die Kosten, die KMU in Niedersachsen für die Einrichtung, den Betrieb und die Instandhaltung von IT-Sicherheit monatlich aufbringen?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

Grundsätzlich ist festzustellen, dass die Kosten für IT-Sicherheit u. a. je nach Unternehmensgröße, Branche, vorhandenen IT-/OT-Infrastrukturen und individuellen Sicherheitsanforderungen stark variieren können. Sie umfassen verschiedene Kostenpositionen wie Hardware, Software, Dienstleistungen und Mitarbeiterschulungen.

26. Welche Kenntnisse besitzt die Landesregierung über den gegenwärtigen Investitionsbedarf der niedersächsischen KMU in die IT-Sicherheit?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

Allerdings gibt es Hinweise auf einen vorhandenen Investitionsbedarf. Zunächst zeigt der BSI-Lagebericht[4], dass Cyberangriffe in Häufigkeit und Intensität zunehmen. Dies deutet auf einen wachsenden Bedarf an IT-Sicherheitsinvestitionen hin. Ferner steigt laut der Studie des Branchenverbandes Bitkom e. V. die Bereitschaft bei den Unternehmen, in Cybersicherheit zu investieren.[5] Schließlich werden bestehende Förderprogramme des Bundes fortgesetzt und offenbar vonseiten der Unternehmen angenommen. Auch die Rückmeldung aus den Unternehmen anlässlich der Weiterentwicklung des Digitalbonus zu Digitalbonus.niedersachsen-innovativ fiel entsprechend aus.

---

4 BSI: Die Lage der IT-Sicherheit in Deutschland 2023, veröffentlicht: 02.11.2023. Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

5 Bitkom: Wirtschaftsschutz 2023. Abrufbar unter: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

27. Wie viele KMU in Niedersachsen beschäftigen zur Cyberabwehr Informatiker bzw. verfügen über eine eigene IT-Abteilung, die entsprechend aufgestellt ist, um Cyberangriffe abzuwehren bzw. entstandene Schäden zu beheben?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

Grundsätzlich lässt sich feststellen, dass je kleiner das Unternehmen und je weniger IT-fokussiert das Geschäftsmodell ist, desto geringer die Wahrscheinlichkeit des Vorliegens einer entsprechend aufgestellten IT-Abteilung ist. Dabei zeigen Studien, dass zunehmend auch kleinere Unternehmen das Ziel von Cyberangriffen werden. Zudem geben 35 % der Unternehmen bei der DIHK-Studie an, dass das Fehlen von Cybersecurity-Fachkräften eine zentrale Herausforderung sei.[6]

28. Wie viele KMU in Niedersachsen haben in den Jahren 2022 und 2023 ihre Mitarbeiter im Umgang mit IT weiterqualifiziert bzw. geschult, um die Datensicherheit im jeweiligen Unternehmen zu verbessern, und gab es hierfür vom Land Niedersachsen gezielte Angebote?

Der Landesregierung liegen zu dieser Frage keine Daten vor.

Seitens des Landes gab und gibt es über die Niedersachsen.next Digitalagentur die Möglichkeit einer Erstberatung. Bezüglich weiterer Schulungsangebote ist auf entsprechende Angebote von Partnern wie der Transferstelle Cybersicherheit und von DAISEC hinzuweisen, die ebenfalls aus öffentlichen Mitteln finanziert sind.

Insgesamt wird das Thema von den Unternehmen als wichtig wahrgenommen, wie sich in der DIHK-Studie zeigt (siehe Antwort zu Frage 27).

29. Welche wirtschaftlichen Schäden sind niedersächsischen KMU in den Jahren 2021, 2022 und 2023 durch Cyberangriffe entstanden (bitte aufschlüsseln nach Jahren und Schadenshöhe)?

Valide Daten speziell zur Lage der KMU in Niedersachsen sind der Landesregierung nicht bekannt. Bundesweite Studien und bekanntgewordene Einzelfälle aus Niedersachsen legen nahe, dass jährlich erhebliche Schäden bei niedersächsischen KMU entstehen.

Eine Studie des Versicherers HDI stellt für 2022 fest, dass deutschlandweit mehr als 1 Million der rund 3,5 Millionen KMU Opfer von Cyberangriffen waren. Die durchschnittliche Schadenshöhe betrug 95 000 Euro. Eine konkrete Bezifferung für Niedersachsen ist auf dieser Grundlage mangels wissenschaftlich-methodischer Absicherung nicht möglich, der Betrag kann jedoch als grobe Orientierung dienen.

Eine Studie des Branchenverbandes Bitkom e. V. geht z. B. für das Jahr 2023 bundesweit von Schäden in Höhe von 146 Milliarden Euro infolge von Cyberattacken aus. Diese Zahlen lassen sich allerdings nicht ohne weiteres auf KMU übertragen, da die befragte Grundgesamtheit Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von mindestens 1 Million Euro umfasst. Das bedeutet einerseits, dass auch große Unternehmen (größer als KMU) umfasst sind, und andererseits, dass sehr kleine Unternehmen nicht erfasst wurden.

Etwaige Zahlen zu wirtschaftlichen Schäden bei KMU aus den Meldungen der Unternehmen an niedersächsische Sicherheitsbehörden sind angesichts der oben zu Frage 23 dargestellten fehlenden Meldepflicht und geringen Meldebereitschaft nicht extrapolierbar. Selbst wenn Unternehmen Angaben zu finanziellen Schäden machen, kann in der Regel nicht differenziert werden, ob die registrierten Schadenssummen durch die Tat selbst (z. B. die Erpressungssumme) oder im Nachhinein (Kosten

[6] DIHK: Digitalisierungsumfrage 2023, Stand Februar 2024. Abrufbar unter: https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/digitalisierung/digitalisierungsumfrage-23

durch beauftragte IT-Unternehmen, Reparaturen, Produktionsausfall, Vertragsstrafen etc.) entstanden sind. Es ist von einem äußerst großen, aber im Umfang nicht bezifferbaren Dunkelfeld auszugehen.

III. Cyberangriffe auf Behörden und Kritische Infrastruktur

30. Wie viele Angriffe auf niedersächsische Einrichtungen und Behörden sowie auf die Kritische Infrastruktur sind der Landesregierung seit dem Jahr 2021 bekannt (bitte aufschlüsseln nach Jahren sowie jeweils nach angegriffener Einrichtung, Behörde und Infrastruktur)?

Die zur Beantwortung dieser Frage erforderlichen Informationen werden nicht verpflichtend erfasst und liegen somit nicht vollumfänglich vor (vgl. Ausführungen zu Frage 18).

Angriffe auf niedersächsische Einrichtungen und Behörden

Ransomware

Jahr	Niedersächsische Einrichtungen oder Behörden
2021	2 Fälle
	1 Schule
	1 Landkreis
2022	2 Fälle
	2 Schulen
2023	1 Fall
	1 Hochschule
2024 - 1. bis 3. Quartal	keine Fälle

Angriffe auf niedersächsische Einrichtungen und Behörden

DDoS

Jahr	Niedersächsische Einrichtungen oder Behörden
2021	1 Fall
	1 Anstalt öffentlichen Rechts
2022	3 Fälle
	1 Schule (2 Fälle)
	1 Körperschaft des öffentlichen Rechts
2023	keine Fälle
2024 - 1. bis 3.Quartal	2 Fälle
	1 Polizeibehörde
	1 Schule

Darüber hinaus werden dem N-CERT mehrere Hundert sogenannter Hochrisikoobjekte pro Monat gemeldet, die unterschiedliche Schadsoftwaretypen enthalten können. 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 Kommunikationskanäle adressiert wird.

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. Siehe hierzu auch die Vorbemerkung der Landesregierung.

Angriffe gegen Kritische Infrastruktur

Ransomware

Jahr	Kritische Infrastruktur
2021	keine Fälle
2022	2 Fälle
	1 Energieversorgungsunternehmen
	1 Unternehmen aus der Medizinbranche

Jahr	Kritische Infrastruktur
2023	1 Fall
	1 Verkehrsunternehmen
2024 - 1. bis 3.Quartal	keine Fälle

Angriffe gegen Kritische Infrastruktur

DDoS

Jahr	Kritische Infrastruktur
2021	1 Fall
	1 Verkehrsunternehmen
2022	keine Fälle
2023	keine Fälle
2024 - 1. bis 3.Quartal	keine Fälle

Es besteht bei KRITIS-Unternehmen keine Meldepflicht gegenüber niedersächsischen Sicherheitsbehörden, da diese Unternehmen bundesrechtlich reguliert sind. Eine Meldeverpflichtung besteht hier insbesondere gegenüber dem BSI.

31. Welche Schäden sind dabei entstanden, und welche Schadenshöhe ist der Landesregierung bekannt (bitte aufschlüsseln wie in Frage 1)?

Eine exakte Bezifferung von Schadenshöhen durch Sicherheitsvorfälle bei den Behörden ist nicht möglich.

Öffentlich bekanntgewordene Sicherheitsvorfälle deuten auf unterschiedliche Schäden und Schadenshöhen hin.

Zur Schadenshöhe bei betroffenen nicht-öffentlichen Einrichtungen liegen der Landesregierung keine exakten Informationen vor, siehe auch Antwort zu Frage 29.

32. Beabsichtigt die Landesregierung, eine Meldepflicht für Cyberangriffe auf kommunale Einrichtungen und niedersächsische Behörden einzuführen? Falls ja, wann? Falls nein, warum nicht?

Alle Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, sind Mitglieder eines Sicherheitsverbundes, vgl. § 13 Abs. 1 Satz 1 NDIG. Gemäß § 14 Abs. 2 NDIG ist jedes Mitglied des Sicherheitsverbundes (§13 Abs. 1 Satz 1 NDIG) verpflichtet, der Zentralstelle für Informationssicherheit (Niedersächsisches Computer Emergency Response Team - N-CERT) 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. Die nach § 13 Abs. 2 NDIG mit dem Landesdatennetz verbundenen anderen Stellen unterliegen der Meldepflicht zwar nicht unmittelbar, werden jedoch im Regelfall durch die Vereinbarung bzw. die Anschlussbedingungen entsprechend verpflichtet (Drs. 18/4900 S. 15).

Geeignet zur Beeinträchtigung der IT-Sicherheit einer anderen mit dem Landesdatennetz verbundenen Stelle (auch innerhalb des faktischen Sicherheitsverbundes i. S. von § 13 Abs. 2 NDIG) sind Sicherheitsvorfälle mit domänenübergreifenden Auswirkungen, die also bereits eine Ressource beeinträchtigen, die auch von der anderen Stelle genutzt wird (vgl. Nr. 2.2 Satz 2 ISRL-ISi-Vorfälle), aber auch domänenspezifische Sicherheitsvorfälle, die zwar nur die IT-Systeme der betroffenen Stelle beeinträchtigen, bei denen jedoch entweder die Wahrscheinlichkeit eines erneuten Sicherheitsvorfalles ähnlicher Ausprägung in der Landesverwaltung nicht ausgeschlossen werden kann oder die Vorgehensweise darauf schließen lässt, dass gezielt Schadensereignisse in der Landesverwaltung vorbereitet werden (vgl. Nr. 2.2 Satz 3 ISRL-ISi-Vorfälle).

Die Behörden, die in den Anwendungsbereich des Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 29.10.2024 „Umsetzung der NIS-2-Richtlinie in Niedersachsen (NIS2UmsRdErl)“ fallen, unterliegen erweiterten Meldepflichten.

Für kommunale Verwaltungen sind bislang keine Meldepflichten bezüglich IT-Sicherheitsvorfällen gesetzlich verankert. Die niedersächsischen Kommunen sind nicht Mitglieder des Sicherheitsverbundes i. S. von § 13 Abs. 1 Satz 1 NDIG. Der Gesetzgeber hat sich bewusst dafür entschieden, den Kommunen wegen ihrer aus der kommunalen Selbstverpflichtung erwachsenen Organisationshoheit keine Vorgaben zu machen, zumal die Strukturen der Kommunen - auch bei ihren IT-Systemen - sehr heterogen sind (Drs. 18/1598 S. 64). Kommunen können Meldungen über IT-Sicherheitsvorfälle auf freiwilliger Basis an das N-CERT melden.

Dies gilt jedoch nicht für die Einrichtungen der Kommunen, die als Kritische Infrastrukturen i. S. von § 2 Abs. 10 BSI-Gesetz i. V. m. der BSI-Kritisverordnung definiert sind. Diesbezüglich gelten umfassende Meldepflichten, z. B. nach § 8b Abs. 4 BSI-Gesetz, gegenüber dem BSI.

33. Welche Software zur Abwehr von Cyberangriffen wird in niedersächsischen Behörden genutzt, und beabsichtigt die Landesregierung gegebenenfalls in niedersächsischen Behörden den Umstieg auf Open-Source-Software? Falls ja, ab wann?

Die Landesregierung braucht einem Auskunftsverlangen nicht zu entsprechen, soweit zu befürchten ist, dass durch das Bekanntwerden von Tatsachen dem Wohl des Landes Nachteile zugefügt werden, Artikel 24 Abs. 3 Satz 1 Alt. 2 NV. Aus Sicherheitsgründen kann zur Software, welche zur Abwehr von Cyberangriffen eingesetzt wird, keine detailliertere Auskunft erteilt werden. In diesem Bereich kommt auch Open-Source-Software zum Einsatz, allerdings kann aus Sicherheitsgründen hierzu ebenfalls keine nähere Aussage getroffen werden. Der Einsatz oder Nichteinsatz bestimmter Software-Sicherheitsprodukte stellt eine geheime Information dar, die Gegenstand angemessener Geheimhaltungsmaßnahmen ist und hinsichtlich derer ein berechtigtes Interesse an der Geheimhaltung besteht. Informationen über konkrete Software zur Angriffsabwehr in Behördennetzwerken sind weder allgemein bekannt noch leicht zugänglich, da sie nur für einen begrenzten Personenkreis bestimmt sind. Für die Behörden besteht ein berechtigtes Interesse an der Geheimhaltung, da diese Information vertrauliche Details der IT-Infrastruktur betrifft, deren Offenlegung Dritten Einblicke in Erkennungs- und Abwehrmechanismen gewähren und potenziell sicherheitsrelevante Schwachstellen offenlegen kann. Eine Veröffentlichung dieser Details könnte von potenziellen Angreifern ausgenutzt werden, was erhebliche Sicherheitsrisiken für die Einrichtungen darstellen würde. Die Landesregierung hat ein berechtigtes Interesse daran, dass diese Informationen nicht für gezielte Cyberangriffe gegen die Behörden verwendet werden können.

34. Plant die Landesregierung für niedersächsische Einrichtungen und Behörden den Einstieg beim europäischen Clouddienst Gaia-X? Falls ja, ab wann?

Hierzu bestehen derzeit keine landesweiten Planungen der Landesregierung.

35. Hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bisher niedersächsische Kommunalverwaltungen in Fragen der Cybersicherheit beraten? Falls ja, wann und in wie vielen Fällen?

Die Aufgaben des BSI sind in § 3 BSI-Gesetz normiert. Unabhängig von verfassungsrechtlichen Bedenken dahin gehend, ob das BSI einzelnen Kommunen Beratungen im Rahmen von § 3 Abs. 1 Nr. 13 a, 14, Abs. 2 BSI-Gesetz überhaupt anbieten darf, findet eine solche in der Praxis aufgrund der Vielzahl von Kommunen nicht statt. Stattdessen stellt das BSI Kommunen beispielsweise Handreichungen und Empfehlungen zu unterschiedlichen Themen zur Verfügung oder führt gemeinsam mit weiteren Partnern Veranstaltungen durch, die sich an eine Vielzahl an Kommunen richten. Eine individuelle Beratung erfolgt jedoch nicht.

36. Konnte das BSI niedersächsische Kommunalverwaltungen in Einzelfällen bei der Bewältigung von Vorfällen helfen? Falls ja, wann und in wie vielen Fällen?

Der Landesregierung sind keine Fälle bekannt, in denen das BSI eine Kommune in Niedersachsen bei der Bewältigung eines IT-Sicherheitsvorfalls unterstützt hat.

37. Was spricht aus Sicht der Landesregierung gegebenenfalls dagegen, die Kommunen mit in die Liste der Kritischen Infrastruktur aufzunehmen? Falls nichts dagegenspricht, wann werden entsprechende Regelungen erarbeitet und umgesetzt?

Kritische Infrastrukturen sollen künftig auf Grundlage eines KRITIS-Dachgesetzes identifiziert werden. Die Bundesregierung hat am 06.11.2024 einen entsprechenden Gesetzentwurf vorgelegt. Über den Arbeitskreis für Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung der Ständigen Konferenz der Innenminister und -senatoren der Länder haben die Innenressorts der Länder frühzeitig umfangreich Stellung zum Referentenentwurf genommen und gebündelt gefordert, dass auch der Sektor Staat und Verwaltung im KRITIS-Dachgesetz genannt wird.

Teile von Kommunen sind bereits auf Grundlage des BSI-Gesetzes als Kritische Infrastruktur identifiziert. Dies gilt etwa für Abwasserbetriebe oder den Öffentlichen Personennahverkehr, wenn die Schwellenwerte des BSI-Gesetzes i. V. m. der BSI-KRITIS-Verordnung überschritten werden.

38. Beabsichtigt die Landesregierung gegebenenfalls zur Aufnahme der Kommunen in die Liste der Kritischen Infrastruktur eine Bundesratsinitiative zum IT-Sicherheitsgesetz zu initiieren? Falls ja, wann?

Eine Bundesratsinitiative zur pauschalen Aufnahme von Kommunen in bundesgesetzliche KRITIS-Vorschriften ist derzeit nicht beabsichtigt.

(Verteilt am 21.01.2025)