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

Anfrage der Abgeordneten André Bock und Saskia Buschmann (CDU)

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

## Cyberattacken in Niedersachsen

Anfrage der Abgeordneten André Bock und Saskia Buschmann (CDU), eingegangen am 05.04.2024 - Drs. 19/4007,
an die Staatskanzlei übersandt am 11.04.2024

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 17.05.2024

### Vorbemerkung der Abgeordneten

Immer wieder kommt es laut Medienberichten zu Cyberangriffen auf deutsche Unternehmen, Institutionen und Behörden. So berichtete der NDR am 12.02.2024[1] von einem Cyberangriff auf das Krankenhaus Lindenbrunn in Coppenbrügge. Der Angriff zielte erpresserisch auf das EDV-System und die Telekommunikation in der Klinik. Auf Geldforderungen wurde nicht eingegangen. Patienten und ihre Daten wurden nicht ge- bzw. beschädigt.

Am 04.04.2023 berichtete die ARD-Tagesschau[2] von Cyberangriffen auf mehrere Internetauftritte von Bund und Ländern, in Niedersachsen waren davon die Internetseiten von Polizeibehörden betroffen.

In Niedersachsen können sich betroffene Firmen und Einrichtungen an die Zentrale Ansprechstelle Cybercrime im Landeskriminalamt (ZAC) für die niedersächsische Wirtschaft wenden. Die ZAC bietet professionelle Unterstützung und Koordinationshilfe für niedersächsische Unternehmen, Behörden und Verbände sowohl präventiv als auch nach einem Angriff durch Cyberkriminelle.[3]

### Vorbemerkung der Landesregierung

Die zunehmende Technisierung und Digitalisierung der Wirtschaft, des öffentlichen Sektors und der Gesellschaft bieten vielerlei Chancen, stellen jedoch sämtliche Beteiligten gleichzeitig vor enorme Herausforderungen. Dieser Wandel verändert auch die Kriminalität und beeinflusst immer stärker die operative und strategische Arbeit der Sicherheitsbehörden.

Ermittlungsverfahren im Bereich von Cybercrimedelikten stellen hohe und sehr spezifische Anforderungen an die in diesem Bereich eingesetzten Polizeibeamtinnen und Polizeibeamten, zudem ist der unterstützende Einsatz von IT-Spezialistinnen und IT-Spezialisten mit entsprechender Expertise unabdingbar. Zur Bündelung besonders ausgeprägter Cyber-Ermittlungskompetenz wurden im Jahr 2021 in den Zentralen Kriminalinspektionen der regionalen Polizeidirektionen sogenannte Fachkommissariate Cybercrime eingerichtet, in denen neben dem Landeskriminalamt Niedersachsen insbesondere auch in den Polizeidirektionen besonders umfangreiche oder herausragende Cybercrimeverfahren bearbeitet werden. Darüber hinaus wurden in sämtlichen Polizeiinspektionen sogenannte

[1] https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Nach-Cyberangriff-Klinik-versucht-Schaden-zu-beheben,cyberangriff170.html

[2] https://www.tagesschau.de/inland/cyberattacken-103.html

[3] https://www.lka.polizei-nds.de/kriminalitaet/deliktsbereiche/internetkriminalitaet/zentrale-ansprechstelle-cybercrime-zac-115916.html

Teams Cybercrime eingerichtet, um auch flächendeckend Cyberkompetenz „vor Ort“ für die Bearbeitung von Cybercrimedelikten vorzuhalten.

Weiterhin ist der Fachbereich Cyberabwehr des Niedersächsischen Verfassungsschutzes mit anderen Fachbereichen des Ministeriums für Inneres und Sport mit „Cyber-Bezügen“ eng vernetzt. In der sogenannten Cyberkoordinierungsgruppe, in der neben den Fachbereichen Cyberabwehr und Wirtschaftsschutz des Verfassungsschutzes das Niedersächsische Computer Emergency Response Team (N-CERT), das Landeskriminalamt Niedersachsen und Vertreter des Innenministeriums (IT, Katastrophenschutz, Landespolizeipräsidium) vertreten sind, werden IT-relevante Sachverhalte unter Wahrung des Trennungsgebots besprochen.

Cybercrime hat sich zu einem hochkomplexen, kriminellen Wirtschaftszweig mit eigenen Wertschöpfungsketten entwickelt und bedroht Privatpersonen, Wirtschaftsunternehmen, staatliche Institutionen und dabei insbesondere kritische Infrastrukturen gleichermaßen. Laut Digitalverband Bitkom sorgen Cyberattacken mittlerweile für enorme Schäden. Gemäß der Studie aus dem Jahr 2023 sind bei Unternehmen, die von Diebstahl, Industriespionage oder Sabotage betroffen waren, innerhalb von zwölf Monaten 205,9 Milliarden Euro Gesamtschaden entstanden, davon sind fast drei Viertel, bzw. 148,2 Milliarden Euro, auf Cyberattacken zurückzuführen. Die Ergebnisse der Studie unterstreichen, dass in Zeiten der zunehmenden Vernetzung sämtlicher Lebensbereiche die Resilienz der Gesellschaft und der Wirtschaft gegen steigende Gefahren aus dem Cyberraum weiter ausgebaut werden muss. Aus diesem Grund legen die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Niedersachsen und der Fachbereich Wirtschaftsschutz im niedersächsischen Verfassungsschutz den Schwerpunkt der Prävention darauf, Unternehmen für den Umgang mit Cyberrisiken zu sensibilisieren. Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) hält umfangreiche Informationen für Bürgerinnen und Bürger bereit, die auf jeder Polizeidienststelle oder im Internet[4] kostenfrei bezogen werden können.

**1. Wie viele Fälle von Cyberangriffen gab es in den Jahren 2020, 2021, 2022 und 2023 in Niedersachsen (bitte aufschlüsseln nach Wirtschaft, kritischer Infrastruktur wie Krankenhäusern, Kraftwerken, etc. und Behörden)?**

Die von der Polizei bearbeiteten Straftaten werden nach Abschluss der polizeilichen Ermittlungen in der bundeseinheitlichen Polizeilichen Kriminalstatistik (PKS) erfasst. Aufgrund des erheblichen Dunkelfeldes im Bereich Cybercrime, das in Studien auf bis zu 91,5 % geschätzt wird[5], hat die PKS allerdings nur eine sehr begrenzte Aussagekraft hinsichtlich der tatsächlich verübten Cyber-Straftaten. Zudem werden Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber die Tathandlungen im Ausland oder unbekannten Ortes erfolgt sind (sogenannte Auslandstaten), in der PKS nicht berücksichtigt.

Innerhalb der PKS sind die relevanten Cybercrime-Delikte im sogenannten Summenschlüssel Cybercrime zusammengefasst. Bei diesen Delikten handelt es sich u. a. um das Ausspähen und Abfangen von Daten inklusive deren Vorbereitung (§§ 202 a bis c StGB), die Datenhehlerei (§ 202 d StGB), Computerbetrug (§ 263 a StGB), die Fälschung beweiserheblicher Daten (§ 269 StGB), die Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB) sowie Datenveränderung und Computersabotage (§§ 303 a, b StGB).

Gemäß diesem Summenschlüssel wurden in den Jahren 2020 bis 2023 in Niedersachsen folgende Zahlen erfasst:

- 2020: 8 865 Delikte,
- 2021: 9 464 Delikte,
- 2022: 12 197 Delikte,
- 2023: 13 218 Delikte.

[4] https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/

[5] Dreißigacker, A., von Skarczinski, B. & Wollinger, G. R. (2021). Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020, KFN-Forschungsberichte No. 162. Hannover: KFN.; online abrufbar unter: https://kfn.de/publikationen/kfn-forschungsberichte/

Aufgrund mangelnder Differenzierung in der PKS kann keine separate Darstellung der Fälle von Cybercrime/Cyberangriffen gegen Unternehmen und/oder Behörden, Verwaltungen, Körperschaften sowie Anstalten des öffentlichen Rechts in Niedersachsen erfolgen. Zudem ist laut PKS-Richtlinie bei Straftaten in Tateinheit nur die Straftat mit der höchsten Strafandrohung zu erfassen. Beispielsweise werden Straftaten im Zusammenhang mit Ransomware als Erpressung und nicht als Cybercrime-Straftaten in der PKS registriert. Daher können anhand der PKS keine spezifischen Aussagen zu Cyberattacken getroffen werden.

Das Landeskriminalamt Niedersachsen führt jedoch seit dem Jahr 2016 für einige Phänomene ein gesondertes Monitoring durch, insbesondere für die Phänomene Ransomware und Distributed Denial of Service (DDoS). Im Rahmen dieses Monitorings kann unterschieden werden, ob natürliche Personen oder Institutionen (z. B. Unternehmen, Behörden, Körperschaften sowie Anstalten des öffentlichen Rechts) betroffen sind. Eine Bewertung im Hinblick auf die Kategorie der betroffenen Institutionen wird nicht durchgeführt.

| Ransomwareangriffe auf Institutionen | | DDoS-Angriffe | |
|---|---|---|---|
| – 2020: | 95 | – 2020: | 21 |
| – 2021: | 102 | – 2021: | 25 |
| – 2022: | 104 | – 2022: | 15 |
| – 2023: | 81 | – 2023: | 15 |

**2. Wie viele Täter konnten ermittelt werden?**

**3. Wie viele Täter wurden verurteilt?**

Die Fragen 2 und 3 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Zu den in der Antwort zu Frage 1 aufgeführten und in der PKS im sogenannten Summenschlüssel Cybercrime zusammengefassten Delikten konnten Tatverdächtige in folgendem Umfang ermittelt werden:

– 2020: 3 513 Tatverdächtige

– 2021: 3 030 Tatverdächtige

– 2022: 3 226 Tatverdächtige

– 2023: 3 422 Tatverdächtige

Eine differenziertere Darstellung bezogen auf die Phänomene Ransomware und DDoS-Angriffe ist aufgrund der in der Antwort zu Frage 1 dargestellten Ausführungen nicht möglich.

Da auf justizieller Seite keine spezielle technische/elektronische Erfassung von Verurteilungen nach Kriterien wie „allgemeine Cyberkriminalität“ erfolgt, ist eine Beantwortung der Frage der erfolgten Verurteilungen nicht möglich. Hierfür wäre eine händische Auswertung aller Verfahren erforderlich, die das im Rahmen einer Kleinen Anfrage Zumutbare und Leistbare übersteigt.

Im Zusammenhang mit Ransomware-Angriffen ist es in den Jahren 2020, 2021, 2022 und 2023 bislang zu keiner Verurteilung gekommen. Für die betreffenden Tatzeiten sind jedoch noch Ermittlungsverfahren anhängig.

**4. Wie hoch war der Schaden durch Zahlungen an die Erpresser (bitte aufschlüsseln nach Jahren)?**

Angegriffene Unternehmen informieren die Polizei nur sehr selten über geleistete Lösegeldzahlungen. Daher sind der niedersächsischen Polizei derzeit nur drei Einzelfälle aus dem Jahr 2023 bekannt. Die Höhe der Lösegeldzahlungen betrug in diesen Fällen 1 072 Euro, 15 600 Euro und 170 000 Euro.

Vonseiten der niedersächsischen Justiz lassen sich konkrete Schadensaufstellungen nicht mit vertretbarem Aufwand ermitteln, weil in den einzelnen Verfahren weder die von den Tätern geforderten „Lösegeldzahlungen“ noch die möglicherweise tatsächlich geleisteten Beträge oder die mutmaßlichen Schadenssummen elektronisch erfasst werden, sondern hierfür alle entsprechenden Verfahrensakten manuell ausgewertet werden müssten. Dies kann jedoch sowohl angesichts der Arbeitsbelastung der Staatsanwaltschaften, deren Kernaufgabe die zügige und nachhaltige Aufklärung und Verfolgung von Straftaten ist, als auch aufgrund der beschränkt zur Verfügung stehenden Zeit im Rahmen einer Kleinen Anfrage zur schriftlichen Beantwortung nicht geleistet werden.

**5. Auf wie hoch schätzt die Landesregierung den wirtschaftlichen Schaden insgesamt (Zahlungen an Erpresser, wirtschaftlicher Ausfall)?**

Konkrete Schätzungen für Niedersachsen liegen der Landesregierung nicht vor, im Übrigen wird auf die in der Vorbemerkung der Landesregierung erwähnte Studie des Branchenverbandes Bitkom verwiesen.

Im PKS-Summenschlüssel Cybercrime (vgl. Antwort zu Frage 1) werden Schadenssummen lediglich für Delikte aus dem Bereich Computerbetrug ausgewiesen, es handelt sich dabei ausschließlich um die von den Tätern erlangte Summe. Der gesamte wirtschaftliche Schaden (durch Arbeitsausfälle, IT-Dienstleister, Systembereinigung etc. entstandene Kosten) wird statistisch nicht erfasst. Der „Schaden durch erlangtes Gut in Euro“ gestaltet sich in den Jahren 2020 bis 2023 laut PKS wie folgt:

– 2020: 8 262 302,00 Euro

– 2021: 7 025 597,00 Euro

– 2022: 9 040 700,00 Euro

– 2023: 11 172 105,00 Euro

**6. Gab es Fälle, in denen durch den Ausfall der IT-Anlagen Leib und Leben gefährdet bzw. beeinträchtigt wurden oder es sogar zu Todesfällen gekommen ist? Wenn ja, wie und warum?**

Es sind keine Fälle bekannt geworden, in denen es infolge eines Angriffes auf Computersysteme in Niedersachsen zu einer Gefährdung von Personen oder zu Todesfällen gekommen ist.

**7. Wie viele Personen arbeiten derzeit in der ZAC im LKA (bitte aufschlüsseln nach Tätigkeiten)?**

Die ZAC Niedersachsen verfügt über sieben Mitarbeitende. Dabei handelt es sich um vier Beamte des Polizeivollzuges sowie drei angestellte IT-Spezialisten.

**8. Wie viele Fälle hat die ZAC seit dem Jahr 2020 bis zum 31. Dezember 2023 betreut (bitte aufschlüsseln nach Jahren)?**

Die Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) ist eine polizeiliche Beratungsstelle für Firmen, Verbände und Behörden bei der Prävention von Cyberkriminalität, zudem fungiert sie als erste Ansprechpartnerin im Schadensfall. Cybercrime-Ermittlungen werden durch die ZAC selbst nicht durchgeführt.

In den Jahren 2020 bis 2023 gestaltete sich das Anfragenaufkommen wie folgt:

– 2020: 616

– 2021: 414

– 2022: 329

– 2023: 431

**9. Ist eine ständige Rund-um-die-Uhr-Erreichbarkeit der fachlichen Expertinnen und Experten gewährleistet? Wenn ja, in welcher Form? Wenn nein, warum nicht?**

Das Landeskriminalamt Niedersachsen hat im Jahr 2021 eine Quick-Reaction-Force (QRF) eingerichtet. Inhaltlich befasst sich die QRF mit Erstmaßnahmen sowie der Betreuung und Beratung von Unternehmen, die Opfer von Cybercrimeattacken geworden sind. Die QRF setzt sich aus spezialisierten Mitarbeitenden der ZAC sowie spezialisierten Mitarbeitenden aus dem Bereich der Cybercrime-Ermittlungen des Landeskriminalamts Niedersachsen zusammen.

Außerhalb von allgemeinen Bürozeiten ist die QRF im Rahmen einer Rufbereitschaft werktags von 16:00 Uhr bis 22:00 Uhr sowie samstags von 08:30 Uhr bis 22:00 Uhr erreichbar. Eine ad hoc-Erreichbarkeit außerhalb der beschriebenen Zeiten ist gewährleistet. In der Vergangenheit wurde jeder Cybervorfall umgehend von der QRF bzw. der ZAC betreut sowie Kontakt zu den sachbearbeitenden Fachkommissariaten Cybercrime aufgenommen.

Für landesinterne Stellen sind Fachexpertinnen und -experten im Bedarfsfalle auch außerhalb der normalen Bürozeiten erreichbar.

**10. Wurde angesichts der seit dem Ukrainekrieg veränderten Bedrohungslage die ZAC personell verstärkt? Wenn ja, wann und in welchem Umfang? Wenn nein, warum nicht?**

Die Bedrohungslage durch Cybercrimedelikte ist konstant hoch. Im Zusammenhang mit dem völkerrechtswidrigen Angriffskrieg Russlands auf die Ukraine wurde für Niedersachsen allerdings kein signifikanter Anstieg festgestellt. Alle Vorfälle konnten bisher im Rahmen der Alltagsorganisation bearbeitet werden, sodass eine personelle Verstärkung der ZAC bisher nicht erforderlich gewesen ist. Im Übrigen wird auf die Antwort zu Frage 11 verwiesen.

**11. Ist eine weitere Aufstockung des Personals der ZAC geplant? Wenn nein, warum nicht?**

Im Jahr 2021 wurde die ZAC personell verstärkt und die QRF eingerichtet. Die ZAC ist derzeit personell ausreichend ausgestattet, um auf Cybercrimevorfälle sofort und angemessen reagieren zu können und Präventionsformate für Unternehmen anzubieten. Vor diesem Hintergrund ist eine weitere Aufstockung des Personals der ZAC aktuell nicht geplant. Soweit sich die Bedrohungslage erheblich verändern sollte, wird die Polizei Niedersachsen hierauf adäquat reagieren.

**12. Welche Befugnisse besitzen Behörden in Niedersachsen, um Cyberangriffe frühzeitig erkennen und abwehren zu können (bitte die Rechtsgrundlagen nennen)?**

Die Befugnisse niedersächsischer Behörden zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit innerhalb der Netze der Verwaltungen sind im „Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit“ (NDIG) geregelt. Seit Verabschiedung des Gesetzes am 23.10.2019 bildet der dritte Teil des Gesetzes den rechtlichen Schwerpunkt beim Einsatz geeigneter Sensoriken zur Abwehr von durch Sicherheitslücken, Schadprogramme oder Angriffe verursachten Gefahren für die IT-Sicherheit.

Die verschiedenen Ermächtigungsgrundlagen sind im zweiten Abschnitt des dritten Teils aufgeführt.

Die Befugnis, Maßnahmen nach dem zweiten Abschnitt (§§ 17 bis 30 NDIG) innerhalb der Verwaltungsnetze zu treffen, erhalten Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. Ein IT-System gilt im Sinne des Gesetzes als mit dem Landesdatennetz verbunden, wenn es direkt oder über ein untergeordnetes behördeneigenes Netz (z. B. lokale Netze oder Datennetze der Kommunen) technisch angeschlossen ist (§ 1 Abs. 2 NDIG).

Vorausgeschickt sei, dass die Auswertung von Daten, die keinen Personenbezug aufweisen, keiner Rechtsgrundlage bedarf, da kein Grundrechtseingriff stattfindet.

Die Ermächtigungen nach §§ 18 bis 23 NDIG unterliegen wegen des damit verbundenen Grundrechtseingriffs strengen Voraussetzungen, deren Einhaltung mit erheblichem technischem und vor

allem auch organisatorischem Aufwand für eine Behörde verbunden ist. Daher hat der Gesetzgeber eine Pflicht, diese Maßnahmen umzusetzen, lediglich den großen zentralen IT-Betrieben übertragen, vgl. § 15 Abs. 1 und 4 NDIG.

Die §§ 18 bis 23 NDIG regeln sodann die verfassungsrechtlich konforme Erhebung und Auswertung von Daten.

§ 18 NDIG zielt auf die Daten von Verzeichnis- und Berechtigungsdiensten ab. Dies ermöglicht beispielsweise den Einsatz eines Advanced Threat Analytics - Systems (ATA-System), bei dem Metadaten aus dem Verzeichnisdienst Active Directory erhoben und ausgewertet werden.

In § 19 NDIG wird die erste von drei Auswertungsstufen zum Einsatz von Security Information Event and Management- (SIEM-) und von Intrusion Detection System / Intrusion Prevention System (IDS-/IPS-) Systemen abgebildet.

Bei § 19 Abs. 1 NDIG handelt es sich um eine Zweckänderungsnorm. Die in Absatz 1 Satz 2 enumerativ genannten, bereits auf Grundlage anderer Normen erhobenen Ereignisdokumentationen (sogenannte log-files) dürfen aufgrund der Ermächtigung auch zum Zwecke der Abwehr von Gefahren für die IT-Sicherheit herangezogen und automatisiert in einem SIEM-System ausgewertet werden.

§ 19 Abs. 2 NDIG regelt die automatisierte Durchsuchung des Datenverkehrs. Dazu dürfen Daten an Übergabe- und Knotenpunkten automatisiert erhoben, entschlüsselt und unverzüglich ausgewertet werden. Es handelt sich also um eine Echtzeitanalyse, bei der nach Abweichungen vom zuvor festgelegten Normalzustand oder nach bekannter Schadsoftware gesucht wird (IDS-/IPS-System).

§ 20 NDIG trifft Regelungen zur weiteren automatisierten und nicht-automatisierten Auswertung aller Daten, die nicht Inhaltsdaten sind. Dabei unterscheidet Absatz 1 und Absatz 2 danach, welchen Grad an Anhaltspunkten (zureichende oder hinreichende) die Auswertung nach § 18 oder § 19 NDIG zutage gefördert hat.

Für eine Speicherung und tiefere Auswertung von Inhaltsdaten gilt hingegen der § 21 NDIG. Anders als bei § 20 NDIG dürfen nur Daten aus § 19 NDIG bei Vorliegen von zureichenden oder hinreichenden tatsächlichen Anhaltspunkten automatisiert und nicht-automatisiert weiter ausgewertet werden. Des Weiteren erfolgt ebenfalls wieder eine Differenzierung nach dem Grad der vorliegenden Anhaltspunkte.

§ 22 NDIG stellt eine Öffnungsklausel dar, um eine Auswertung des nach § 19 Abs. 2 NDIG erhobenen Datenverkehrs durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu ermöglichen. Bislang wurde noch kein entsprechendes Gegenstück seitens des Bundes geschaffen. Durch einen Ausbau des BSI zu einer Zentralstelle für Informationssicherheit könnten jedoch neue Impulse gesetzt werden, um eine bessere verstetigte Zusammenarbeit ermöglichen zu können.

Durch § 23 NDIG wird eine zeitlich befristete, rollierende Speicherung der Daten nach § 19 Abs. 2 NDIG zugelassen, um diese auch nachträglich noch auswerten zu können. Um jedoch auf diesen Datenbestand zugreifen zu dürfen, sind besonders scharfe Anforderungen in Absatz 3 geregelt. Eine solche Auswertungsmöglichkeit ist insbesondere im Bereich der IT-Forensik bei festgestellten Vorfällen wichtig.

Vonseiten des IT-Bereiches im Niedersächsischen Verfassungsschutz wird, zusätzlich zu den Sicherheitsmechanismen der übrigen Landesverwaltung, der gesamte ein- und ausgehende Datenverkehr der Verfassungsschutzabteilung durch zusätzliche Sicherheitstechnik überwacht, um mögliche Cyberangriffe auf die IT des Verfassungsschutzes frühzeitig erkennen und abwehren zu können. Die rechtlichen Grundlagen hierfür sind mit dem Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) identisch mit denen, die für die übrige Landesverwaltung gelten.

Die Zuständigkeit der Bearbeitung von Sachverhalten mit Bezug zu elektronischen Angriffen, die einen nachrichtendienstlichen Hintergrund haben, ist im Fachbereich Cyberabwehr in der Spionageabwehr des Niedersächsischen Verfassungsschutzes verankert. Die rechtliche Grundlage für die Tätigkeit des Fachbereiches Cyberabwehr stellt § 3 Abs. 1 Nr. 2 Niedersächsisches Verfassungsschutzgesetz dar. Hier heißt es: „Aufgabe der Verfassungsschutzbehörde ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten

und Unterlagen, über (…) sicherheitsgefährdende oder geheimdienstliche Tätigkeiten in der Bundesrepublik Deutschland für eine fremde Macht…“. Bei der Aufklärung möglicher Cyberangriffe ist der Fachbereich Cyberabwehr auf die freiwillige Mitarbeit der betroffenen Personen/Institutionen angewiesen, da der Niedersächsische Verfassungsschutz über keine Exekutivbefugnisse verfügt.

Die Polizei nimmt ihre Aufgaben im Bereich „Cybercrime“ gefahrenabwehrrechtlich nach dem Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) aber auch im Rahmen der Strafatenverfolgung (§ 163 Strafprozessordnung) wahr. Um gefahrenabwehrrechtlich tätig zu werden, beispielsweise um bevorstehende Angriffe auf niedersächsische Unternehmen erkennen und diese entsprechend warnen zu können, kann auf die allgemeinen Befugnisse zur Datenverarbeitung (§§ 30 ff. NPOG) zurückgegriffen werden. Weiterhin stehen aber auch besondere Ermächtigungen wie z. B. die Telekommunikationsüberwachung (§§ 33 a ff. NPOG) unter den dort genannten Voraussetzungen zur Verfügung.

**13. Reichen diese Befugnisse zur Überwachung und Kontrolle des Datenverkehrs aus?**

Mit dem NDIG verfügt Niedersachsen über eines der fortschrittlichsten Informationssicherheitsgesetze in Deutschland. Die hierin geregelten Befugnisse zur Überwachung und Kontrolle des Datenverkehrs reichen grundsätzlich aus, um den derzeitigen Gefahren für die IT-Sicherheit niedersächsischer Behörden zu begegnen.

Jedoch gilt es, die schnellen Entwicklungen im Bereich der Informationstechnik weiterhin aktiv zu begleiten und auf Neuerungen sowohl in der Bedrohungslage als auch in der Technik zu reagieren.

So wird zum einen die zunehmende Verlagerung der Datenverarbeitung in die Cloud beobachtet. Anders als bisher werden Informationen nicht mehr ausschließlich on premise in eigenen Rechenzentren verarbeitet. Einige Anbieter ändern gar dahin gehend ihre Geschäftsmodelle, dass keine selbst betreibbare on premise-Software mehr angeboten wird. Zwar bieten diese Anbieter in der Regel auch umfangreiche und professionelle Sicherheitspakete an, jedoch gilt es zu berücksichtigen, dass dadurch unter Umständen eine Auswertung durch private Dritte erfolgt.

Eine ähnliche Schwierigkeit im Rahmen der Auswertung ergibt sich aus dem anhaltenden und sich durch den demografischen Wandel zuspitzenden Fachkräftemangel. Für die Auswertung werden technisch wie fachlich hochqualifizierte Personen benötigt. Hier steht die Verwaltung in erheblichem Wettbewerb mit der freien Wirtschaft. Insbesondere finanziell sieht sich hier der öffentliche Dienst starken Herausforderungen gegenüber, die zum größten Teil selbst ausgebildeten Fachkräfte zu halten. Gleichzeitig kann das vorhandene Personal perspektivisch nur schwer in der erforderlichen Breite ausgebildet werden. Die Landesregierung setzt sich daher dafür ein, die Attraktivität der Landesverwaltung für qualifizierte Fachkräfte weiter zu erhöhen. Gleichsam wird es künftig auch von besonderer Bedeutung sein, zu prüfen, welche Leistungen zur Entlastung des vorhandenen Personals auch durch eine Beauftragung privater Dritter erfolgen kann.

(Verteilt am 23.05.2024)