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

Anfrage des Abgeordneten Dr. Marco Genthe (FDP)

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

Cyberkriminalität in Niedersachsen

Anfrage des Abgeordneten Dr. Marco Genthe (FDP), eingegangen am 10.09.2019 - Drs. 18/4562
an die Staatskanzlei übersandt am 12.09.2019

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung
vom 14.10.2019

Vorbemerkung des Abgeordneten

Die Zahl der Fälle von Cyberkriminalität ist laut Polizeilicher Kriminalstatistik seit Jahren ansteigend. Im Jahr 2018 wurden ca. 110 000 Fälle von Cyberkriminalität in Deutschland registriert (vgl. Polizeiliche Kriminalstatistik 2018 des Bundeskriminalamts).

Der Niedersächsische Minister für Inneres und Sport, Boris Pistorius, kündigte im August 2019 die Kampagne „Die Hacker kommen!“ an, mit der die Gesellschaft verstärkt für das Thema Cyberkriminalität und Sicherheit im Netz sensibilisiert werden soll (*Hannoversche Allgemeine Zeitung* vom 20. August 2019: „Land will Cyberangriffe besser abwehren“). Bei der Ankündigung betonte der Minister noch einmal die Gefahr, die von der Cyberkriminalität ausgehe. Um darauf besser vorbereitet zu sein, stelle die Polizei gezielt mehr IT-Experten ein, so Pistorius. Insgesamt seien dadurch in den letzten drei Jahren 150 zusätzliche Stellen entstanden, wobei bei diesen aber auch Experten für Islamismus mit eingerechnet wurden, schränkte der Minister ein (*Braunschweiger Zeitung* vom 20. August 2019: „Pistorius wirbt für mehr Sicherheit im Netz“).

Vorbemerkung der Landesregierung

Im Zeitalter einer zunehmenden Digitalisierung und Abhängigkeit von neuen vernetzten Systemen wächst die Gefahr von Cyberangriffen im privaten wie im gewerblichen Bereich. Zahlreiche auch in Niedersachsen geführte Ermittlungsverfahren belegen, dass die Risiken durch Anzahl und Intensität der Angriffe in unterschiedlichen Bereichen der Cyberkriminalität seit geraumer Zeit spürbar zunehmen. Die Vorgehensweisen reichen von organisierten Cyberangriffen bis hin zu Cyber-Attacken auf Behörden und Kritische Infrastrukturen (KRITIS). Insgesamt ist seit Jahren eine Verschiebung von analoger zu digitaler Kriminalität festzustellen.

Weltweit werden heute Schadprogramme eingesetzt, um beispielsweise Ransomware (Schadsoftware zur Verschlüsselung von Computersystemen) für digitale Erpressungen oder für den Datenabgriff an Computern, Routern oder Internet-of-Things(IoT)-Geräten einzusetzen. Seit Jahren hat auch der Betrieb sogenannter Botnetze (ohne Wissen der Besitzer ferngesteuerte Computersysteme) zugenommen, um sie z. B. für die Durchführung sogenannter DDoS-Angriffe (Distributed Denial of Service) zum Nachteil von Unternehmen oder KRITIS einzusetzen. Mit zunehmender Tendenz ist dabei der Einsatz von Malware bei Routern und Produkten im sogenannten IoT-Umfeld festzustellen.

Die Cyberkriminalität nutzt darüber hinaus die offen im Internet verfügbaren und insbesondere auch die im Darknet erreichbaren Plattformen weltweit im Sinne eines „Crime as a Service“. Auf den digitalen Schwarzmärkten der Underground Economy verwerten Kriminelle die im Internet illegal erlangten Identitäten, Daten und Informationen, beispielsweise für digitale Erpressungen oder das sogenannte Doxing (öffentliches Bloßstellen). Weiterhin im Trend bleiben Betrugstaten (z. B. Wa-

renkreditbetrug durch Bezahlen mit gestohlenen Kreditkartendaten unter Nutzung von Paketstationen) oder das Phishing im Online-Banking.

Die Polizei Niedersachsen hat im Jahr 2012 im Rahmen von Analysen zur Entwicklung der neuen Landesstrategie die strategische Relevanz des Phänomens Cyberkriminalität frühzeitig erkannt. Unter der Zielbeschreibung „WIR haben qualifiziertes Personal, die Organisation und Technologie zur Bekämpfung von Cybercrime“ hat dieser Phänomenbereich im strategischen Zielsystem der Strategie 2020 entsprechend Berücksichtigung erfahren. In der Folge wurden unter einem Qualifizierungskonzept Cybercrime die nachfolgend näher erläuterten strategischen Maßnahmen initiiert und umgesetzt.

Erfolgreiche Ermittlungen im Internet, in sozialen Netzwerken und der Umgang mit digitalen Spuren betreffen in zunehmendem Maße alle Mitarbeiterinnen und Mitarbeiter in den ermittelnden Bereichen. Zur Erhöhung der digitalen Kompetenzen wurden in dem Zeitraum vom 01.01.2016 bis zum 22.09.2019 insgesamt 4 714 Teilnehmende durch zentrale Fortbildungen an der Polizeiakademie Niedersachsen beschult, die sich - bedingt durch Mehrfachteilnahmen - auf insgesamt 2 308 Polizeibeamtinnen und -beamte sowie Beschäftigte verteilten.

Als Cyberkriminalität werden auf Grundlage einer bundesweit abgestimmten Definition Straftaten erfasst, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik auch unter Nutzung des Tatmittels Internet begangen werden (Cybercrime im weiteren Sinne). Beim Tatmittel Internet werden grundsätzlich alle Delikte erfasst, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird. Hier kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits Tatbestände erfüllt, als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird.

Von **Cyberkriminalität im engeren Sinne** werden spezielle Delikte wie z. B. Computerbetrug, Ausspähen und Abfangen von Daten einschließlich der Vorbereitungshandlungen und Datenhehlerei, Diebstahl und Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten, Datenveränderung/Computersabotage etc. umfasst. Die Bearbeitung erfolgte bis 2016 in den Fachkommissariaten 3 der Polizeiinspektionen bzw. der Kriminalfachinspektion 3 der Polizeidirektion Hannover, darüber hinaus bei organisierter und bandenmäßiger Tatbegehung und Verursachung hoher wirtschaftlicher Schäden in den Zentralen Kriminalinspektionen und dem Landeskriminalamt Niedersachsen.

Mit Wirkung vom 01.12.2016 wurden im Rahmen einer Pilotierung in sieben Polizeiinspektionen und fünf Zentralen Kriminalinspektionen sogenannte TaskForces Cybercrime/Digitale Spuren mit dem Ziel eingerichtet, unter Zusammenlegung von Ermittlungspersonal, Datenverarbeitungsgruppen und Analysestellen die Bearbeitung von Cyberkriminalität im engeren Sinne zu erproben. Die Polizeidirektion Hannover verfügt über eine vergleichbar ermittelnde Einheit im 3.1 K der KFI 3. In den übrigen Polizeiinspektionen wurden in den Fachkommissariaten 3 sogenannte Teams Cybercrime eingerichtet.

Die Bearbeitung von Delikten der **Cyberkriminalität im weiteren Sinne** erfolgt auf der Grundlage der deliktischen Zuweisung durch eine nicht näher eingrenzbare Zahl an Sachbearbeiterinnen und Sachbearbeitern in den Kriminalermittlungsdiensten der Polizeikommissariate und in den Fachkommissariaten der Zentralen Kriminaldienste der Polizeiinspektionen, soweit sie nicht Cyberkriminalität im engeren Sinne in den speziellen Organisationseinheiten bearbeiten. Neben Delikten der Massenkriminalität, wie z. B. Betrug oder Beleidigung, zählen hierzu auch beispielsweise Phänomene wie Drogenkriminalität, Hehlerei oder auch digitale Erpressung, wenn sie im Kontext des Tatmittels Internet ausgeführt werden. Die Bearbeitung dieser Delikte erfolgt nahezu in jedem Arbeitsbereich durch eine sehr hohe Anzahl von Sachbearbeiterinnen und Sachbearbeitern, die nicht differenziert dargestellt werden kann.

Die voranschreitende Digitalisierung sowie die stark steigenden Datenmengen müssen ebenso wie die Sicherung und Auswertung neuer digitaler Spuren durch die Polizei bewältigt werden, um durch strukturierte Prozesse konkrete Hinweise zur Gefahrenabwehr zu erlangen, Gefahrenvorsorge zu treffen und eine beweissichere Strafverfolgung zu gewährleisten. Exemplarisch werden an dieser

Stelle die Gefahren bei Cyberattacken auf KRITIS, terroristische Anschläge oder auch Großschadenslagen angeführt. Vor diesem Hintergrund wurden in Niedersachsen seit 2016 fortlaufend externe IT-Spezialistinnen und IT-Spezialisten eingestellt, um auch mit neuen Ansätzen die Aufgabenbewältigung im Zuge der Datenaufbereitung und -nutzung die Sachbearbeiterinnen und Sachbearbeiter zu unterstützen. Zum Teil finden die IT-Spezialistinnen und IT-Spezialisten in den Polizeibehörden auch direkt in bestimmten Phänomenbereichen, z. B. im Staatsschutz oder zur Unterstützung bei der Auswertung von sozialen Medien in Einsatzleitstellen (Open Source Intelligence - OSINT), Verwendung. Im LKA Niedersachsen werden darüber hinaus vier IT-Spezialistinnen bzw. IT-Spezialisten im Bereich des Maschinellen Lernens (Künstliche Intelligenz) eingesetzt.

Im Ministerium für Inneres und Sport sind im Referat 42 - Informationssicherheit, Cybersicherheit - die Dienstposten des Informationssicherheitsbeauftragten der Landesverwaltung (Chief Information Security Officer - CISO), des Referenten für Grundsatzangelegenheiten der Cyber-Sicherheit sowie das Niedersächsischen Computer Emergency Response Team (N-CERT) angesiedelt. Zu den Aufgaben des CISO gehört gemäß Leitlinie zur Gewährleistung der Informationssicherheit, auf strategischer und ressortübergreifender Ebene Sicherheitsvorfälle zu untersuchen und Schwachstellen festzustellen. Dem Referenten für Grundsatzangelegenheiten der Cyber-Sicherheit obliegt die Entwicklung von Strategien zur Abwehr von Cyberattacken, die Koordinierung der Umsetzung der Cyber-Sicherheitsstrategie Niedersachsens, die Vertretung Niedersachsens in der IMK-Arbeitsgruppe Cyber-Sicherheit sowie Geschäftsführung der Koordinierungsstelle Cyber-Sicherheit. Letztere hat die Aufgabe, die Tätigkeiten der Polizei, des Verfassungsschutzes und des Katastrophenschutzes im Bereich der Cyber-Sicherheit zu harmonisieren. Das N-CERT beobachtet kontinuierlich die Cyber-Sicherheitslage, u. a. durch die Auswertung relevanter Informationen der Sicherheitsbehörden, namentlich des LKA Niedersachsen, der Polizeibehörden in Niedersachsen und des niedersächsischen Verfassungsschutzes. Es ist die zentrale Kontaktstelle für IT-Sicherheitsfragen für die Landesverwaltung und die Kommunen in Niedersachsen und Teil der Krisenbewältigungsorganisation bei Cyber-Lagen. Insoweit wird auf den genannten Dienstposten die Bekämpfung von „Cybercrime im engeren Sinne“ auf abstrakt-strategischer Ebene vorangetrieben.

In dem dem Ministerium für Inneres und Sport nachgeordneten Geschäftsbereich IT.Niedersachsen wird im Fachbereich 1 als Fachgebiet 15 das Cyber Defense Operation Center unterhalten, in dem als Teilfachgebiet das Security Operation Center (SOC) angesiedelt ist.

Das SOC soll in der Funktion eines IT-Sicherheitsleitstandes die Aufgaben der operativen Erkennung, Abwehr und Analyse von Bedrohungen der IT-Systeme sowie die Koordination von Gegenmaßnahmen erfüllen. Es arbeitet hierzu eng mit dem N-CERT im Ministerium für Inneres und Sport zusammen, zu dem es eine exklusive Kommunikationsschnittstelle darstellt. Das SOC betreibt technische Systeme und Instrumente zur Erkennung von Schwachstellen und Bedrohungen für die IT-Systeme des Hauses sowie die Detektion von bereits eingetretenen, unbekannten Verletzungen der IT-Sicherheit.

Eine Bekämpfung von Cybercrime im weiteren Sinne erfolgt im SOC in der Regel im Rahmen der Amtshilfe (z. B. bei Auskunftsersuchen im Rahmen von Ermittlungsvorgängen der Polizei) oder bei eigenen Feststellungen möglicher entsprechend strafbarer Handlungen im Landesdatennetz.

1. Wie viele Stellen existieren im Geschäftsbereich des Ministeriums für Inneres und Sport für die Erfassung und Bekämpfung von Cyberkriminalität? Bitte nach Behörden, Polizeidirektionen, Polizeiinspektionen und Verfassungsschutz aufschlüsseln.

Aus organisatorischer Sicht handelt es sich bei einer Stelle um einen in der Aufbauorganisation eingerichteten Dienstposten für verbeamtete Mitarbeiterinnen bzw. Mitarbeiter bzw. um einen Arbeitsplatz für Tarifbeschäftigte. Abweichend davon existiert der Begriff „Stelle“ im haushalterischen Sinne als Ermächtigung zur Beschäftigung und Bezahlung eines Menschen.

Um u. a. dem Phänomen Cybercrime noch wirksamer begegnen zu können, wurden seit dem Jahr 2016 zahlreiche externe Spezialisten für IT-Forensik und IT-Analyse, aber auch andere extern qualifizierte Expertinnen und Experten eingestellt. Insgesamt wurden der Polizei seitdem mehr als 150 zusätzliche Stellen bzw. Beschäftigungsmöglichkeiten in den Bereichen IT-Forensik, Datenanalyse, Social-Media-Manager und für den Bereich Islamismus zur Bekämpfung neuer Kriminali-

tätsformen bereitgestellt. Inbegriffen sind auch die ersten OSINT-Experten, die in den Einsatzleitstellen eingesetzt sind. Es handelt sich dabei um Mitarbeiterinnen und Mitarbeiter, die in den Leitstellen bereits während der Einsatzaufnahme nach zusätzlichen Informationen recherchieren, um sie direkt an die Einsatzkräfte weiterzugeben.

Dies vorangestellt und unter Verweis auf die Ausführungen in den Vorbemerkungen zur Bearbeitung von Delikten der Cyberkriminalität im engeren Sinne und ausgehend von einer vermuteten organisatorischen Intention des Fragestellers zum Begriff der Stelle werden in der **Anlage** die ausschließlich für die Bekämpfung von Cybercrime eingerichteten Dienstposten bzw. Arbeitsplätze aufgeführt.

Darüber hinaus wird auf die Ausführungen zur Bearbeitung von Delikten der Cyberkriminalität im weiteren Sinne bei den Vorbemerkungen verwiesen.

2. Wie viele Stellen sind noch unbesetzt? Bitte nach Behörden, Polizeidirektionen, Polizeiinspektionen und Verfassungsschutz aufschlüsseln.

Siehe hierzu die Anlage zur Frage 1.

3. Wie viele eigenständige Fachabteilungen für Cybercrime gibt es? Welche sind dies?

Eigenständige Fachabteilungen für Cybercrime sind bei der Polizei in Niedersachsen nicht eingerichtet.

Gemäß RdErl. d. MI v. 17.10.2017 - 21.11-01512 - „Organisation der Polizei des Landes Niedersachsen“ erfolgt die polizeiliche Aufgabenwahrnehmung und damit die Bearbeitung von „Cybercrime“ in den Polizeidienststellen. Im Einzelnen sind dies folgende 34 fest eingerichtete Organisationseinheiten:

– fünf in den Zentralen Kriminalinspektionen Braunschweig, Göttingen, Lüneburg, Oldenburg und Osnabrück - Fachkommissariat „Wirtschafts-, Korruptions- und IuK-Kriminalität (Cybercrime)“,

– eine im Zentralen Kriminaldienst der Polizeidirektion Hannover - Kriminalfachinspektion 3 „Wirtschafts-, Betrugs-, Umwelt-, Korruptions- und Amtsdelikte; Finanz- und Vermögenermittlungen, IuK-Kriminalität (Cybercrime)“,

– 27 in den Polizeiinspektionen im Zentralen Kriminaldienst - Fachkommissariat 3 „Wirtschafts-, Korruptions-, und IuK-Kriminalität (Cybercrime)“ und

– eine im Landeskriminalamt Niedersachsen - Dezernat 38 „Zentralstelle Iuk-Kriminalität (Cybercrime)“.

Mit der Einrichtung von je einer Pilotorganisationseinheit „TaskForce Cybercrime/Digitale Spuren“ in den Zentralen Kriminalinspektionen Braunschweig, Göttingen, Lüneburg, Oldenburg sowie Osnabrück sowie in sieben ausgewählten Polizeiinspektionen wurde die Sachbearbeitung aus den dortigen originären Fachkommissariaten „Wirtschafts-, Korruptions-, und IuK-Kriminalität (Cybercrime)“ herausgelöst. Die „TaskForces Cybercrime/Digitale Spuren“ sind ein Zusammenschluss der Sachbearbeiterinnen und Sachbearbeiter aus den Bereichen der Cybercrime-Ermittlungen mit Experten der IT-Beweissicherung und der Analyse aus anderen Fachkommissariaten.

Weiterhin gibt es im Landeskriminalamt Niedersachsen direkt bei der Behördenleitung angegliedert ein Projekt für die „Weiterentwicklung der polizeilichen Analyse“, welches u. a. auch den Themenbereich Cybercrime abbildet.

In der Polizeiakademie Niedersachsen wurde in der Abteilung 1, Studiengebiet 1 (Kriminalwissenschaften) ein Aufgabenfeld Cybercrime eingerichtet. Diese zentrale Stelle verantwortet u. a. die Aus- und Fortbildung, Weiterentwicklung und Forschung zu diesem Themenbereich.

4. Wie viele Personen sind in den mit der Bekämpfung von Cyberkriminalität betrauten Institutionen des Landes Niedersachsen beschäftigt? Bitte nach Behörden, Polizeidirektionen, Polizeiinspektionen und Verfassungsschutz aufschlüsseln.

Die Frage nach „mit der Bekämpfung von Cyberkriminalität betrauten Institutionen“ impliziert in Verbindung mit den Fragen zu 1 und 2, dass damit Personen in externen Institutionen gemeint sind. Dazu ist festzustellen:

Durch den Polizeibereich sind keine Institutionen mit der Bekämpfung von Cyberkriminalität betraut worden. Gleiches gilt für die Abteilungen 4 sowie 5 des Ministeriums für Inneres und Sport.

5. Welche Delikte im Bereich der Cyberkriminalität werden besonders häufig begangen?

Im Hinblick auf die Vorbemerkung handelt es sich weit überwiegend um Fälle von Computerbetrug.

6. In wie vielen Fällen waren Behörden Ziel von Cyberangriffen? Bitte aufschlüsseln, welche Behörden betroffen waren.

Für die Landesverwaltung gibt es eine Richtlinie über den Umgang mit Sicherheitsvorfällen und daraus resultierende Meldepflichten in Form eines gemeinsamen Runderlasses. Hierin sind Meldeverpflichtungen über Sicherheitsvorfälle gegenüber dem Computer Emergency Response Team beim Ministerium für Inneres und Sport (N-CERT) für die unmittelbare Landesverwaltung festgelegt.

Wenn beispielsweise ein Virenscanner eine Schadsoftware erkennt, dann wird dies noch nicht als Sicherheitsvorfall eingestuft, sondern erst dann, wenn weitere Sicherungseinrichtungen die Schadsoftware erkennen und abwehren und die Art des Angriffs geeignet ist, eine Bedrohung für andere Teile des Landesdatennetzes darzustellen. Die Fallzahlen über Sicherheitsvorfälle oder Cyberangriffe hängen also davon ab, was konkret unter einem solchen Vorfall verstanden wird.

Nach den Vorschriften der Richtlinie über den Umgang mit Sicherheitsvorfällen sind im Jahr 2018 dem N-CERT 107 Sicherheitsvorfälle gemeldet worden. Für das Jahr 2019 sind bislang 90 Sicherheitsvorfälle gemeldet worden.

Aus IT-Sicherheitsgründen kann eine detaillierte Darstellung oder weitere Aufschlüsselung nach Behörden nicht erfolgen, da hierdurch potenziellen Angreifern Hinweise auf mögliche Angriffswege gegeben würden.

7. Wie viele Ermittlungen im Bereich der Internetkriminalität sind aufgrund von Informationen ausländischer Sicherheitsbehörden seit 2015 eingeleitet worden (bitte nach Jahren und Delikt aufschlüsseln)?

In Niedersachen erfolgt keine Erfassung darüber, wie viele konkrete Ermittlungen sich aufgrund der genannten Informationsübermittlungen ergeben haben. Seit 2015 sind im Landeskriminalamt Niedersachsen im Dezernat 22 (Internationale polizeiliche Zusammenarbeit) 1 564 Vorgänge erfasst, in denen im Zusammenhang mit der Begrifflichkeit Cybercrime ein Austausch mit anderen Staaten erfolgte. Grundsätzlich werden alle eingehenden Informationen ausländischer Sicherheitsbehörden im Sinne des § 163 StPO geprüft und soweit erforderlich Ermittlungsverfahren eingeleitet.

8. Plant die Landesregierung organisatorische Änderungen im Bereich der Bekämpfung der Internetkriminalität? Wenn ja, inwiefern und wann?

Cybercrime im weiteren Sinne umfasst solche Delikte, die unter Nutzung des Tatmittels Internet begangen werden, wie z. B. der Warenbetrug über bekannte Online-Auktionsplattformen. Die Landesregierung plant hierzu keine organisatorischen Änderungen. Die digitalen Ermittlungskompetenzen werden gleichwohl in allen Bereichen weiter ausgebaut.

Cybercrime im engeren Sinne umfasst spezielle Delikte wie z. B. Computerbetrug, Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei (§§ 202 a, 202 b, 202 c, 202 d StGB), z. B. Diebstahl und Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten, Datenveränderung/Computersabotage etc. Im Zuge der Umsetzung der Ergebnisse des Projektes „Strategische Organisationsanpassung in der Polizei Niedersachsen“ ist zur Bekämpfung der Cybercrime im engeren Sinne vorgesehen, die Pilotorganisationseinheiten zu verändern. Die Ermittlungskomponenten werden perspektivisch aus dem Pilotstatus in die Alltagsorganisation überführt. Sie werden somit dauerhafter und integraler Bestandteil der Organisationsstrukturen der Zentralen Kriminaldienste und der Zentralen Kriminalinspektionen. Hier soll auch weiterhin eine Fokussierung auf herausragende Delikte erfolgen, bei denen beispielsweise komplexe Schadsoftware mit dem Ziel der Manipulation von IT-Anlagen eingesetzt wurde und deshalb besondere Methodenkompetenzen erforderlich sind.

Die Komponente der Bearbeitung digitaler Spuren soll zeitnah mit anderen unterstützenden Services (IT-Spezialistinnen und IT-Spezialisten, Analysestellen, Kriminaltechnik, etc.) in einem neuen - noch näher zu beschreibenden - Fachkommissariat gebündelt werden.

Anlage

Organisationseinheit	für Cybercrime i. e. S. eingerichtete Dienstposten/Arbeitsplätze gesamt	davon eingerichtet in 2016, über Doppelhaushalt 2017/2018 sowie Nachtragshaushalt 2018	von gesamt nicht besetzt
MI gesamt	**15**	**0**	**2**
Polizeidirektion Braunschweig gesamt	**41**	**7**	**9**
davon Polizeiinspektion Braunschweig	18	4	3
davon Polizeiinspektion Salzgitter/Peine/Wolfenbüttel	4	0	0
davon Polizeiinspektion Wolfsburg/Helmstedt	3	0	0
davon Polizeiinspektion Gifhorn	3	0	0
davon Polizeiinspektion Goslar	3	0	0
davon Zentrale Kriminalinspektion Braunschweig	10	3	6
Polizeidirektion Göttingen gesamt	**50**	**9**	**1**
davon Polizeiinspektion Göttingen	22	3	0
davon Polizeiinspektion Hildesheim	4	1	0
davon Polizeiinspektion Hameln-Pyrmont/Holzminden	4	1	0
davon Polizeiinspektion Nienburg/Schaumburg	4	1	0
davon Polizeiinspektion Northeim	4	1	1
davon Zentrale Kriminalinspektion Göttingen	12	2	0
Polizeidirektion Hannover gesamt	**20**	**7**	**2**
davon Zentraler Kriminaldienst	20	7	2
Polizeidirektion Lüneburg gesamt	**35**	**7**	**4**
davon PI Celle	4	1	0
davon Polizeiinspektion Harburg	2	0	0
davon Polizeiinspektion Heidekreis	3	0	0
davon Polizeiinspektion Rotenburg	3	0	0
davon Polizeiinspektion Stade	5	1	1
davon Polizeiinspektion Lüneburg/Lüchow-Dannenberg/Uelzen	6	1	2
davon Zentrale Kriminalinspektion Lüneburg	12	4	1
Polizeidirektion Oldenburg gesamt	**48**	**8**	**4**
davon Polizeiinspektion Cloppenburg/Vechta	6	1	1
davon Polizeiinspektion Cuxhaven	4	1	0
davon Polizeiinspektion Delmenhorst/Oldenburg-Land/Wesermarsch	6	0	0
davon Polizeiinspektion Diepholz	5	1	2
davon Polizeiinspektion Oldenburg-Stadt/Ammerland	6	1	0
davon Polizeiinspektion Verden/Osterholz	6	1	1
davon Polizeiinspektion Wilhelmshaven/Friesland	5	1	0
davon Zentrale Kriminalinspektion Oldenburg	10	2	0

Organisationseinheit	für Cybercrime i. e. S. eingerichtete Dienstposten/Arbeitsplätze gesamt	davon eingerichtet in 2016, über Doppelhaushalt 2017/2018 sowie Nachtragshaushalt 2018	von gesamt nicht besetzt
Polizeidirektion Osnabrück gesamt	**69**	**9**	**22**
davon Polizeiinspektion Osnabrück	27	2	9
davon Polizeiinspektion Emsland/Grafschaft Bentheim	24	2	8
davon Polizeiinspektion Leer/Emden	1	1	0
davon Polizeiinspektion Aurich/Wittmund	2	2	0
davon Zentrale Kriminalinspektion Osnabrück	15	2	5
Landeskriminalamt Niedersachsen gesamt	**26**	**23**	**8**

Stand: 01.09.2019

(Verteilt am 16.10.2019)