BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
22. Wahlperiode

Drucksache 22/10836
07.02.23

Schriftliche Kleine Anfrage

der Abgeordneten Sandro Kappe und Dennis Gladiator (CDU) vom 31.01.23

und Antwort des Senats

Betr.: Cyberkriminalität – Wie hilft der Senat?

Einleitung für die Fragen:

Die größte Gefahr der Digitalisierung ist die Cyberkriminalität.

30 Prozent der deutschen Firmen geben an, dass sie in den letzten drei Jahren einen Schaden von mindestens 1 Million Euro durch Cyberangriffe erlitten haben (Cyber-Security-Report von PricewaterhouseCoopers). Teilweise war die Existenz bedroht.

In den meisten Fällen schleusen die Hacker Schadsoftware ein und verschlüsseln die Daten, welche nur nach einer Lösegeldzahlung freigeschaltet werden. Den Firmen entstehen dadurch erhebliche Kosten für die Wiederherstellung. 24,3 Milliarden Euro Schaden entstehen dadurch deutschlandweit pro Jahr (Studie „Cybersicherheit in Zahlen“).

Zuständig für derlei Vorfälle ist grundsätzlich das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Jedoch arbeiten bereits auch Bundesländer an eigenen Lageberichten. So hat die Fachhochschule des Verfassungsschutzes von Nordrhein-Westfalen einen Lagebericht Wirtschaftsschutz erstellt und das Schutzniveau der Wirtschaft untersucht. Die Ergebnisse waren erschreckend. Das Land Nordrhein-Westfalen hat daher entschieden, der Wirtschaft beratend zur Seite zu stehen.

Vor diesem Hintergrund fragen wir den Senat:

Einleitung für die Antworten:

Die Bedrohungslage durch Cyberkriminalität hat sich in den letzten Jahren weltweit kontinuierlich verschärft und ist für Deutschland unverändert hoch. In Zusammenarbeit zwischen Dataport, den Trägerländern, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie dem Computer Emergency Response Team (CERT) Nord wird die Bedrohungslage regelmäßig neu bewertet und gegebenenfalls Maßnahmen ergriffen. Dies umfasst ständige Kommunikation und Informationsaustausche zwischen diesen Institutionen auf Basis von täglich erstellten Lageberichten, welche vom Nationalen IT-Lagezentrum des BSI erstellt werden. Der Lagebericht informiert die für Cybersicherheit Verantwortlichen in Wirtschaft und Verwaltung über weltweite Vorfälle und Schwachstellen aus Wirtschaft, Politik und Öffentlichkeit.

Cybercrime ist eines der sich am dynamischsten verändernden Kriminalitätsphänomene. Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt.

Polizeilich unterscheidet man zwischen „Cybercrime im engeren Sinne“ (Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten) und „Cybercrime im weiteren Sinne“ (Straftaten, die mittels Informationstechnik begangen werden).

Cybercrime im engeren Sinne umfasst also jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden, zum Beispiel Schadsoftware (Malware), Spam und Phishing, Ransomware (Digitale Erpressung durch Verschlüsselung des Systems), Hacking, DDoS(Distributed-Denial-of-Service)-Angriffe). Der Begriff Cyberkriminalität in der vorliegenden Anfrage wird als Cybercrime im engeren Sinne ausgelegt.

Im Übrigen siehe Drs. 22/9871 und 22/9253.

Dies vorausgeschickt, beantwortet der Senat die Fragen wie folgt:

Frage 1: *Wie viele Anzeigen sind in Hamburg in den Jahren 2019, 2020, 2021 und 2022 zur Cyberkriminalität eingegangen? Diese sind nach Kategorie unterteilt anzugeben.*

Antwort zu Frage 1:

Statistiken im Sinne der Fragestellung werden bei der Polizei nicht geführt.

Die Polizei erfasst Straftaten gemäß dem Straftatenkatalog der Richtlinien für die Erfassung und Verarbeitung der Daten in der Polizeilichen Kriminalstatistik (PKS).

Die statistische Erfassung eines Falles erfolgt nach den Richtlinien für die Führung der PKS mit Abschluss aller polizeilichen Ermittlungen durch die für die Endbearbeitung zuständige Dienststelle bei endgültiger Abgabe der entstandenen Ermittlungsvorgänge beziehungsweise des Schlussberichts an die Staatsanwaltschaft oder das Gericht.

Da die Jahresdaten der PKS 2022 zurzeit noch nicht qualitätsgesichert sind, sind die PKS-Daten zur Gewährleistung eines Minimums an Validität für das Jahr 2022 als kumulative Dreivierteljahreszahlen (Januar bis September) dargestellt. PKS-Zahlen für das Jahr 2022 liegen voraussichtlich im Februar 2023 vor.

Tabelle

PKS-Schlüssel		2019	2020	2021	Jan. bis Sept. 2022
674200	Datenveränderung, Computersabotage §§ 303a, 303b StGB	132	122	126	97
678000	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	448	641	898	837

Die Staatsanwaltschaft kann diese Frage nicht beantworten, da im Vorgangsverwaltungssystem MESTA nicht verlässlich erfasst wird, ob ein Verfahren aufgrund einer Anzeige eingeleitet wurde.

Zur Beantwortung der Frage müssten daher zumindest sämtliche Verfahren der für Cybercrime zuständigen Abteilung 74 aus dem Register 7450 ausgewertet werden, in dem die Cybercrimeverfahren erfasst werden. Allein die Ermittlungen gegen unbekannte Beschuldigte umfassen für den Aktenzeichenjahrgang 2022 mehr als 800 UJs Verfahren. Eine Beiziehung und Auswertung bereits dieser Verfahren ist im Rahmen der für die Beantwortung einer Parlamentarischen Anfrage zur Verfügung stehenden Zeit nicht möglich.

Frage 2: *Welche Behörden waren in den Jahren 2019, 2020, 2021 und 2022 von Cyberkriminalität betroffen und in welchem Umfang?*

Frage 3: *Wie viele Angriffe konnten die Behörden in Hamburg in den Jahren 2019, 2020, 2021 und 2022 verzeichnen?*

Frage 4: *Welche öffentlichen Unternehmen waren in den Jahren 2019, 2020, 2021 und 2022 von Cyberkriminalität betroffen und in welchem Umfang?*

Frage 5: *Wie viele Angriffe konnten die jeweiligen öffentlichen Unternehmen in den Jahren 2019, 2020, 2021 und 2022 verzeichnen?*

Antwort zu Fragen 2 bis 5:

Statistische Daten im Sinne der Fragestellung werden nicht zentral erfasst.

Frage 6: *Wie viele Beschäftigte im öffentlichen Dienst befassen sich mit Cyberkriminalität und wo sind diese jeweils eingesetzt (Ist-Bestand)?*

Frage 7: *Wie viele Beschäftigte sollen sich im öffentlichen Dienst mit Cyberkriminalität befassen und wo sind diese Stellen eingeplant (Soll-Bestand)?*

Antwort zu Fragen 6 und 7:

Der Besetzungsumfang bei dem für Cybercrime zuständigen LKA 54 beträgt zum Stichtag 1. Januar 2023 72,63 Vollzeitäquivalente (VZÄ). Dem LKA 54 sind mit Stand 1. Januar 2023 insgesamt 84 Dienstposten zugeordnet.

In der Staatsanwaltschaft obliegt die Strafverfolgung der Delikte im Zusammenhang mit „Cyberkriminalität“ der Abteilung 74. Aufgrund der internen Geschäftsverteilung sind der Abteilung hierfür insgesamt 9,1 VZÄ zugewiesen worden, die auch besetzt sind (Ist = Soll).

Beim Amtsgericht Hamburg befassen sich insgesamt fünf Mitarbeiterinnen und Mitarbeiter des Amtsgerichts Hamburg im Rahmen ihres Aufgabenbereiches (unter anderem) mit dem Thema Cyberkriminalität. Dies lässt sich jedoch nicht in VZÄ-Anteile aufspalten.

Nach der Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg (ISLL) richtet die für Informationstechnik zuständige Behörde ein zentrales Informationssicherheitsmanagement ein. Die Behörden benennen für ihren Verantwortungsbereich einen Informationssicherheitsbeauftragten. Aktuell haben alle Behörden einen offiziell bestellten oder einen kommissarischen Vertreter für das Informationsmanagement (Stand: 22.12.2022).

Grundsätzlich befassen sich Beschäftigte aus dem öffentlichen Dienst (Kernverwaltung), die im Fachbereich der Informationssicherheit tätig sind, mit Cyberkriminalität. Da die Informationen über die Beschäftigten, die sich mit Cyberkriminalität beschäftigen, in der Informationssicherheit als schützenswerte Güter eingestuft werden, behält sich der Senat vor, keine näheren Angaben über die Anzahl der Beschäftigten zu machen.

Frage 8: *Befassen sich alle öffentlichen Unternehmen selbstständig mit dem Thema Cyberkriminalität oder wurde eine Gruppe für alle Unternehmen gegründet?*

Frage 9: *Wie viele Beschäftigte befassen sich bei den jeweiligen öffentlichen Unternehmen mit dem Thema Cyberkriminalität?*

Antwort zu Fragen 8 und 9:

Die öffentlichen Unternehmen befassen sich grundsätzlich selbstständig mit dem Thema Cyberkriminalität. Statistische Daten im Sinne der Fragestellung werden nicht zentral erfasst.

Nach Ziffer 4.1.1. lit. h der Compliance-Rahmenrichtlinie gehört zu den Pflichtinhalten aller Compliance-Management-Systeme der öffentlichen Unternehmen die IT-Compliance, welche neben den Themenkomplexen „Daten- und Geheimnisschutz“ und „vertrauliche Informationen“ auch die IT-Sicherheit umfasst.

Die Best-Practice-Empfehlungen der Rahmenrichtlinie führen hierzu aus, dass die Informationssicherheit durch das Unternehmen zu gewährleisten ist. So gilt es unter anderem, alle internen Angelegenheiten des Unternehmens, die nicht öffentlich bekannt gemacht worden sind, vertraulich zu behandeln und vor dem Zugriff und dem Einblick nicht beteiligter Mitarbeiterinnen und Mitarbeiter sowie sonstiger Dritter in geeigneter Weise zu schützen, soweit sich gesetzlich, aus dem Hamburger Corporate Governance Kodex (HCGK), dieser Rahmenrichtlinie oder der Unternehmensverfassung nichts

anderes ergibt. Dafür ist eine dem jeweiligen Unternehmen angepasste, wirksame IT-Sicherheitsinfrastruktur zu implementieren. Dies gilt insbesondere für den Bereich der kritischen Infrastruktur. Auf die IT-Sicherheitsstandards (insbesondere Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg, Rahmensicherheitskonzept der Freien und Hansestadt Hamburg) der Freien und Hansestadt Hamburg in den jeweils aktuell geltenden Fassungen wird ausdrücklich hingewiesen. Vergleichbare Standards sind, angepasst an die Unternehmen, zu etablieren.

Im Auftrag des Digital Boards der Behörden für Wirtschaft und Innovation sowie Verkehr und Mobilitätswende hat das Digital Projektmanagement-Office (PMO) der Hamburger Hochbahn AG das Konzept für ein Cybersecurity-Portfolio für die Freie und Hansestadt Hamburg erarbeitet. Dieses soll ein an die jeweilige Bedrohungslage adaptiertes und haushaltsoptimiertes, resistentes und standortweites Sicherheitsniveau schaffen, das sich den neuen Herausforderungen dynamisch und aktiv stellen kann. Mit einem durch REACT-EU-Mittel finanzierten Projekt zum Aufbau eines Cyber Security Portfolios Hamburg werden derzeit prototypisch wesentliche Cyber-Security-Funktionsbausteine auf Basis kollaborativer Zusammenarbeit umgesetzt und bei ersten öffentlichen Unternehmen zum Einsatz gebracht. Für die Umsetzung des Projekts im Projektzeitraum zwischen 15. Februar 2022 und 31. März 2023 hat sich ein Konsortium gebildet, an dem die folgenden Unternehmen als assoziierte Partner beteiligt sind: HPA, Flughafen Hamburg, HOCHBAHN, Hamburg Marketing, Messe Hamburg, hamburg.de, Stromnetz Hamburg, Gasnetz Hamburg, HHLA.

Frage 10: *Wie unterstützt der Senat private Firmen bei Cyberkriminalität? Hier sind die Maßnahmen vor dem Angriff sowie die Maßnahmen nach dem Angriff aufzulisten.*

Frage 11: *Wie unterstützt der Senat öffentliche Unternehmen bei Cyberkriminalität? Hier sind die Maßnahmen vor dem Angriff sowie die Maßnahmen nach dem Angriff aufzulisten.*

Frage 12: *Wie unterstützt der Senat Behörden bei Cyberkriminalität? Hier sind die Maßnahmen vor dem Angriff sowie die Maßnahmen nach dem Angriff aufzulisten.*

Frage 13: *Bietet der Senat Schulungen und Vorträge zur Cyberkriminalität an? Wenn ja, welche und in welchem Umfang?*

Antwort zu Fragen 10 bis 13:

Die öffentlichen Unternehmen haben jeweils eigene IT-Infrastrukturen, die losgelöst von IT-Infrastruktur der Kernverwaltung betrieben werden. Unbeschadet dessen wird derzeit im Rahmen der Cyber-Security-Initiative zwischen den öffentlichen Unternehmen und der Kernverwaltung eine gemeinsame Entwicklung von Services zur Cyber-Gefahrenabwehr angestrebt.

Die Behörden werden von Dataport durch Maßnahmen zur Absicherung der IT-Dienste unterstützt. Das BSI hat einen Standard für gute Sicherheitsmaßnahmen und Prozesse entwickelt, den sogenannten IT-Grundschutz. Dataport ist nach diesem Standard zertifiziert. Durch die Umsetzung der Maßnahmen nach dem IT-Grundschutz-Standard wird Vorsorge gewährleistet. Im Störungsfall stehen Prozesse und Ressourcen im Rahmen des Sicherheitsvorfallmanagements zur Verfügung.

Die Freie und Hansestadt Hamburg führt seit mehreren Jahren erfolgreich organisierte Awareness-Kampagnen für die Behörden und Ämter durch. Dafür wurde ein modulares Baukastensystem mit unterschiedlichen Veranstaltungs- und Online-Formaten, Phishing-Kampagnen sowie Informationsmaterialien entwickelt, welche bedarfsgerecht auf die Anforderungen der einzelnen Organisationseinheiten zugeschnitten werden.

Aufgrund der aktuellen Vorfälle und der stetig wachsenden Bedeutung des Themas hat der Senat den Budgetansatz für das Jahr 2023 um 50 Prozent erhöht.

Die Unterstützungsangebote der Polizei, insbesondere durch das LKA 54, richten sich an alle Unternehmen und Behörden im Sinne der Fragen. Die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA 54 bietet kostenlose Beratungen für Hamburger Unternehmen an. Darunter Awareness-Veranstaltungen, Beratungen zu Back-up-Konzepten sowie für einen IT-Notfallplan zum Thema IT-Sicherheit. Letzteres zielt darauf ab, Unternehmen auf einen Cyber-Notfall vorzubereiten und somit im Angriffsfall die Reaktionszeit und den Schaden zu minimieren. Wird ein bestehender Cyberangriff angezeigt, erfolgt durch das LKA 54 neben den kriminalpolizeilichen Maßnahmen, zu denen aus grundlegenden Erwägungen keine weiteren Angaben gemacht werden, auf Wunsch auch eine anlassbezogene Beratung. Die Inhalte und Konzepte entsprechen dabei dem Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Sowohl die Anzahl an Beratungen als auch der Umfang der angebotenen Leistungen der ZAC haben sich seit 2017 deutlich erhöht. Wesentlicher Schwerpunkt der Beratung liegt beim Erkennen von Gefahren von Cyberangriffen beziehungsweise deren Verhinderung. Bei Bedarf erhalten die Unternehmen weiteres Informationsmaterial wie die BKA-Broschüre „Handlungsempfehlung für die Wirtschaft“, welche auch auf der Internetseite des Bundeskriminalamtes abrufbar ist, sowie den vom LKA im Jahre 2018 erstellten „Awareness-Stick“ (USB-Stick) mit Informationstexten und präventiven Handlungsempfehlungen zu zahlreichen Themen der Cyber-/IT-Sicherheit.

Darüber hinaus wirkt die ZAC auch an der Vorbereitung und Durchführung von IT-Sicherheitsübungen in Unternehmen mit.

Beschäftigte der Behörden können Schulungsveranstaltungen des Zentrums für Aus- und Fortbildung (ZAF) zur Informationssicherheit selbstständig buchen und wahrnehmen. Zu den Veranstaltungen im ZAF siehe Anlage 1.

Frage 14: *Welche Kurse zur Cyberkriminalität bietet die Volkshochschule an? Welche weiteren sind geplant?*

Antwort zu Frage 14:

Die Hamburger Volkshochschule (VHS) bietet zur Cyberkriminalität im Rahmen ihres Themenschwerpunktes Digitale Sicherheit beziehungsweise Digitale Selbstverteidigung seit vielen Jahren und regelmäßig mehrmals pro Jahr wiederholt unter anderem folgende Kurse an:

- „Cyberangriffe und Abwehrmaßnahmen“
- „Rechtsverletzungen im Internet“
- „Die Datenkrake kommt“
- „Rechtssicherheit im Internet“
- „Ist Ihr Smartphone, Ihr Laptop wirklich sicher fürs Internet?“
- „Human Hacking“
- „Hardware Hacking: Computer-Sprechstunde“
- „Hardware Hacking 1: So wird Ihr Handy geknackt (und Ihr Laptop auch)“
- „Hardware Hacking 2: Sprechstunde Internetsicherheit“
- „Verschlüsselung: Daten und E-Mails im Internet schützen“
- „Cyber Security“
- „Cyber Security leichtgemacht“
- „Hardware Hacking 1: Angriffe aus dem Internet“

Seit 2017 hat die VHS circa 50 dieser und ähnlicher Kurse angeboten und plant regelmäßig neue wie aktuell zum Beispiel den Kurs „Big Data, Cookies und Datenschutz“.

Daneben werden die Themenschwerpunkte Digitale Sicherheit beziehungsweise Digitale Selbstverteidigung ebenfalls in allen Computer- und Smartphone-/Tablet-Einführungs- und Aufbaukursen behandelt. Allein in 2023 haben bis dato circa 70 solcher Kurse stattgefunden oder sind in Planung.

Zudem greift die VHS die Themenschwerpunkte Digitale Sicherheit beziehungsweise Digitale Selbstverteidigung auch immer im Bereich der Politischen Bildung auf. Dazu bietet die VHS derzeit folgende Kurse an:

- „Fake News, Filterblasen, Verschwörungen - Durch kritisches Denken Informationen vertrauen“
- „Künstliche Intelligenz: Wann ist die Maschine schlauer als der Mensch?“
- „Was macht die polizeiliche Kriminalprävention? In der Reihe: Komplizen für die Zukunft“
- „Verschwörungsideologien: Gefahren, Strategien, Gegenmaßnahmen“

Geplant sind hier weitere Angebote, die die digitale Mündigkeit der Hamburger Bürgerinnen und Bürger fördern und sie in diesem Zusammenhang für den Aspekt Cyberkriminalität sensibilisieren sollen. Dies unter anderem in Kooperation mit dem TIDE (Hamburgs Communitysender und Ausbildungskanal) für einen gemeinsamen Bildungsurlaub (BU).

Seit 2023 erfolgt eine Kooperation der VHS mit dem Landeskriminalamt (LKA), Bereich Kriminalprävention, die sowohl bei Multimedia-Veranstaltungen als auch in der Politischen Bildung zum Tragen kommt.

In diesem Zusammenhang finden beispielsweise seit 2023 in den Räumen der VHS Vorträge des LKA für sogenannte Best Agers im Internet statt.

Frage 15: *Welche Studiengänge in Hamburg befassen sich mit Cybersicherheit? Sind welche geplant?*

Antwort zu Frage 15:

Im Bachelorstudiengang Polizei des Fachhochschulbereichs der Akademie der Polizei Hamburg finden für die Laufbahnzweige Schutz-/Wasserschutz- sowie Kriminalpolizei jeweils verpflichtende Lehrveranstaltungen zu Cybercrime statt. Diese haben einen Umfang von insgesamt 30 beziehungsweise 40 Unterrichtseinheiten im Präsenzstudium und 36 Unterrichtseinheiten im Selbststudium. Daneben bestehen Wahlangebote etwa des hochschuleigenen Projekts „Netzwerk Digitale Polizei“.

Ein spezifischer Studiengang zu Cyberkriminalität ist bislang nicht geplant.

Die Studiengänge mit Bezügen zur Cybersicherheit sind der Anlage 2 zu entnehmen.

Frage 16: *Viele Landeskriminalämter weisen Cyber-Hotlines auf. Hier können sich Betroffene bei einem Befall direkt melden. Weist Hamburg auch eine entsprechende Hotline auf?*

Wenn ja, wie wurde die Wirtschaft über die Nummer informiert und welchen Service können Firmen hier einholen?

Wenn nein, wieso nicht und ist eine Einrichtung geplant?

Antwort zu Frage 16:

Die ZAC hat eine Hotline eingerichtet, die während der Bürozeiten besetzt ist. Außerhalb der Bürozeiten ist eine Erreichbarkeit über den Notruf der Polizei (110) gewährleistet.

Über die Webseite www.polizei.de sind die Kontaktdaten der ZAC einsehbar und alle Serviceleistungen der ZAC beschrieben. Darüber hinaus können weitere Informationen über die ZAC auch auf der Seite des Netzwerk Standortsicherheit Hamburg https://www.netzwerkstandortsicherheit.hamburg/ aufgerufen werden.

Frage 17: *Hat der Senat wie das Land Nordrhein-Westfalen bereits einen Lagebericht Wirtschaftsschutz erstellt und das Schutzniveau der Wirtschaft untersucht?*

Wenn ja, mit welchen Ergebnissen?

Wenn nein, wieso nicht?

Antwort zu Frage 17:

Der Digitalverband Bitkom untersucht seit 2015 jährlich, wie es um die deutsche Wirtschaft beim Thema Wirtschaftsschutz bestellt ist, und hat mit der Studie ein Instrument entwickelt, das umfassende Erkenntnisse über Cyberangriffe auf die deutsche Wirtschaft gibt. Die aktuelle Studie 2022 wurde gemeinsam mit dem Verfassungsschutz

vorgestellt. Die Ergebnisse decken sich mit dem Lagebericht des Landes Nordrhein-Westfalen, der sich wiederum auf die Bitkom-Studie stützt. Kernbotschaften sind: In Zeiten der zunehmenden Vernetzung aller Lebensbereiche muss die Resilienz der deutschen Wirtschaft gegen steigende Gefahren aus dem Cyberraum weiter ausgebaut werden. Es gilt, einen ganzheitlichen und nachhaltigen Schutz der deutschen Wirtschaft zu etablieren, der nicht allein IT-bezogene Maßnahmen, sondern auch risikominimierende Pläne in den Bereichen Organisation und Personal umfasst. Dabei muss stets ein enger und vertrauensvoller Erfahrungsaustausch mit den Sicherheitsbehörden aufrechterhalten werden. Die Ergebnisse der Studie gelten auch für Hamburg.

Fachlicher Bedarf für eine eigene Studie des Senats besteht daher nicht. Der Verfassungsschutz hat im Verfassungsschutzbericht 2021 auf Seiten 141 fortfolgende über elektronische Angriffe berichtet und dabei die Öffentlichkeit über die Erkenntnisse der Bitkom-Studie „Wirtschaftsschutz 2021“ informiert. Allgemein ist darauf hinzuweisen, dass der Verfassungsschutz für Cybercrime zwar nicht zuständig ist, mittels seiner Präventionstätigkeit bezogen auf Cyberbedrohungen und -angriffe durch Nachrichtendienste fremder Staaten sowie durch seine Mitwirkung in der Geheimschutzbetreuung wesentlich zur Cybersicherheit Hamburgs beiträgt.

Frage 18: *Wie viele der öffentlichen Unternehmen haben eine Cyberversicherung abgeschlossen?*

Frage 19: *Welche öffentlichen Unternehmen planen den Abschluss einer Cyberversicherung?*

Antwort zu Fragen 18 und 19:

Statistische Daten im Sinne der Fragestellung werden nicht erfasst.

Frage 20: *Mitarbeiter sind häufig die größte Schwachstelle. Welche öffentlichen Unternehmen schulen die Mitarbeiter bezüglich Cyberkriminalität? Welche planen dies?*

Frage 21: *Welche Behörden schulen die Mitarbeiter bezüglich Cyberkriminalität? Welche planen dies?*

Antwort zu Fragen 20 und 21:

Die Ermittlungssachbearbeiter Cybercrime des LKA müssen besondere Qualifizierungserfordernisse erfüllen, beispielsweise ein polizeiliches Cybercrime-Studium, „Fortbildungsprogramm Cybercrime und IT-Sicherheit“, „Nordic Computer Forensics Investigator (NCFI)“, ein einschlägiges Studium (beispielsweise Informatik, Computerforensik) oder vergleichbare Qualifizierungen, die an der Technischen Hochschule Brandenburg, der Fachhochschule Kiel im Rahmen der Cybercrime-Ausbildung des Nordverbundes oder der Polizeihochschule Oslo (Norwegen) im Rahmen einer Kooperation erworben werden können.

Zusätzlich nehmen während der Ausbildung alle Nachwuchskräfte des Laufbahnabschnittes I (mittlerer Dienst) an einem zweitägigen Lehrgang „Digitalisierung im polizeilichen Alltag“ teil. Es werden dabei unter anderem Inhalte zum Umgang mit Straftaten der Cyberkriminalität, Schutz und Umgang mit verdächtigen (Phishing-)E-Mails sowie Regeln im Umgang mit Spam vermittelt.

Im Übrigen siehe Antwort zu 10 bis 13.

Frage 22: *Wie bewertet der Senat die Gefahr durch Cyberkriminalität für die Behörden sowie für die öffentlichen Unternehmen?*

Frage 23: *Welche Maßnahmen zum Schutz hat der Senat ergriffen?*

Antwort zu Fragen 22 und 23:

Die Gefährdungslage hat sich in den letzten Jahren kontinuierlich verschärft. Dabei sind eine zunehmende Professionalisierung der Cyberkriminalität, die Nutzung des Cyberraums für staatliche Aktionen im Kontext von Spionage und Kriegsführung, aber auch die Ergänzung regulärer Kriegsführung durch Cyberangriffe zu verzeichnen. Die dabei

zunehmende Professionalisierung führt nicht nur zu immer komplexeren Bedrohungen, sondern auch zu einer immer höheren Geschwindigkeit der Angriffe.

Die Verschlechterung der zwischenstaatlichen Beziehungen seit dem Beginn des russischen Angriffskrieges erhöht zusätzlich das Risiko durch Angriffe auf Regierungs- und Wirtschaftseinrichtungen.

Informationen zu konkreten Bedrohungslagen werden den Behörden und öffentlichen Unternehmen durch das CERT-Nord regelmäßig sowie anlassbezogen zur Verfügung gestellt.

Im Übrigen siehe Drs. 22/9871 und 22/9253 und die regelmäßigen Veröffentlichungen des BSI (https://www.bsi.bund.de, zum Beispiel „Die Lage der IT-Sicherheit in Deutschland 2022“).

Veranstaltungs-nummer	Startdatum	Veranstaltungstitel	Organisationseinheit zum Anmeldezeitpunkt	Anzahl
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1
			Behörde für Justiz und Verbraucherschutz	1
			Behörde für Stadtentwicklung und Wohnen	1
			Behörde für Umwelt, Klima, Energie und Agrarwirtschaft	2
			Bezirksamt Hamburg-Nord	1
			Bezirksamt Harburg	1
			Bezirksamt Wandsbek	2
			BIS Amt für Migration	1
			BJV - Finanzgericht Hamburg	1
			BJV - Hamburgisches Oberverwaltungsgericht	1
			BJV - Landgericht Hamburg	1
			FB - Steuerverwaltung	1
			Landesbetrieb Geoinformation und Vermessung	2
		Hacken kann so einfach sein, Schutz vor Hackern	Landesbetrieb Straßen, Brücken und Gewässer	1
008067-0001	**21.03.2019**	ebenfalls! - Workshop zur Informationssicherheit	Technische Universität Hamburg	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1
			Behörde für Stadtentwicklung und Wohnen	1
			Bezirksamt Hamburg-Nord	3
			Bezirksamt Wandsbek	1
			BIS Amt für innere Verwaltung und Planung	1
			BIS Polizei	1
			BIS V	2
			BJV - Amtsgericht Hamburg	1
			BJV - Justizvollzugsanstalt Billwerder	1
		Hacken kann so einfach sein - Schutzmaßnahmen	BSB - Gymnasien	1
008067-0002	**20.11.2019**	ebenfalls! - Workshop zur Informationssicherheit	Finanzbehörde	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1

			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	2
			BIS Amt für innere Verwaltung und Planung	1
			BJV - Finanzgericht Hamburg	1
			Landesbetrieb Geoinformation und Vermessung	9
		Hacken kann so einfach sein, Schutz vor Hackern	Personalamt	2
008067-0003	**21.03.2019**	ebenfalls! - Workshop zur Informationssicherheit	Tutoren	1
			Behörde für Schule und Berufsbildung	2
			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	1
			Bezirksamt Bergedorf	1
			Bezirksamt Eimsbüttel	2
			Bezirksamt Hamburg-Mitte	1
			BIS V	1
			Hamburger Institut für Berufliche Bildung (LB)	1
			Landesbetrieb ZAF/AMD	1
		Hacken kann so einfach sein - Schutzmaßnahmen	Rechnungshof	2
008067-0004	**20.11.2019**	ebenfalls! - Workshop zur Informationssicherheit	Senatskanzlei	1
			BIS Feuerwehr (Verwaltung)	1
			BIS Polizei	2
			BJV - Finanzgericht Hamburg	1
			Finanzbehörde	1
		SK: IT-Sicherheitsbeauftragte in der öffentlichen	Rechnungshof	1
009220-0001	**22.06.2020**	Verwaltung - Basis-Kompaktveranstaltung	Zentrum für Personaldienste (LB)	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1
			Behörde für Schule und Berufsbildung	2
			Behörde für Verkehr und Mobilitätswende	2
			Behörde für Wirtschaft und Innovation	2
			Bezirksamt Eimsbüttel	1
			Bezirksamt Hamburg-Nord	2
			BJV - Landgericht Hamburg	1
			FB - Finanzämter	1

			Hamburgischer Datenschutzbeauftragter	1
			Kasse.Hamburg (LB)	1
			Senatskanzlei	1
		WS: Cybercrime - Schutz vor cyberkriminellen	Universität Hamburg	1
009422-0022	**08.04.2021**	Handlungen	Zentrum für Personaldienste (LB)	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1
			Behörde für Wirtschaft und Innovation	1
			Landesbetrieb ZAF/AMD	1
			Personalamt	1
009462-0001	**08.10.2020**	Hacker School - IT für Alle - KI	Tutoren	1
			Behörde für Kultur und Medien	1
			Behörde für Stadtentwicklung und Wohnen	1
			Behörde für Umwelt, Klima, Energie und Agrarwirtschaft	1
			Bezirksamt Bergedorf	1
			Bezirksamt Hamburg-Nord	1
			Bezirksamt Harburg	1
			BIS Feuerwehr (Verwaltung)	1
			Landesbetrieb Geoinformation und Vermessung	1
			Personalamt	1
009470-0001	**08.10.2020**	Hacker School - IT für Alle - Python	Senatskanzlei	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	1
			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	1
			Bezirksamt Altona	1
			BIS Feuerwehr (Verwaltung)	1
			BIS Polizei	1
			Landesbetrieb Hamburger Volkshochschule	1
			Senatskanzlei	1
009470-0002	**23.05.2022**	Hacker School - IT für Alle (online)	Zentrum für Personaldienste (LB)	2
			Behörde für Kultur und Medien	1
			Behörde für Schule und Berufsbildung	1
			Behörde für Stadtentwicklung und Wohnen	1

			Behörde für Umwelt, Klima, Energie und Agrarwirtschaft	1
			Bezirksamt Altona	1
			Bezirksamt Eimsbüttel	1
			Bezirksamt Hamburg-Mitte	1
			Bezirksamt Harburg	1
			BIS Amt für innere Verwaltung und Planung	1
			BJV - Verwaltungsgericht Hamburg	1
			Hamburger Institut für Berufliche Bildung (LB)	1
			Institution/Firma	1
		Informationssicherheit - Aktuelle Bedrohungslagen und	Landesbetrieb Geoinformation und Vermessung	1
009521-0001	**18.03.2021**	wie ich mich schützen kann - Online-Veranstaltung	Landesbetrieb Straßen, Brücken und Gewässer	1
			Behörde für Justiz und Verbraucherschutz	1
			Behörde für Stadtentwicklung und Wohnen	1
			Bezirksamt Altona	1
			Bezirksamt Hamburg-Nord	1
			Bezirksamt Wandsbek	2
			BIS Feuerwehr (Verwaltung)	1
			Bürgerschaftskanzlei	1
			Hamburger Institut für Berufliche Bildung (LB)	1
		Informationssicherheit - Aktuelle Bedrohungslagen und	Landesbetrieb Straßen, Brücken und Gewässer	1
009521-0002	**17.03.2022**	wie ich mich schützen kann (online)	Personalamt	1
			Behörde für Kultur und Medien	1
			Behörde für Schule und Berufsbildung	1
			Bezirksamt Altona	1
			Bezirksamt Harburg	1
			Bezirksamt Wandsbek	1
			BIS Amt für Migration	1
		Informationssicherheit - Phishing und Pharming - Den	BJV - Staatsanwaltschaft Hamburg	1
		Datenpiraten hilflos ausgeliefert? - Online-	BJV - Verwaltungsgericht Hamburg	1
009522-0001	**14.06.2021**	Veranstaltung	Rechnungshof	1

			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	3
			Behörde für Schule und Berufsbildung	2
			Bezirksamt Altona	2
			Bezirksamt Eimsbüttel	1
			Bezirksamt Wandsbek	1
			BIS Amt für innere Verwaltung und Planung	1
			BJV - Staatsanwaltschaft Hamburg	1
			FB - Steuerverwaltung	1
			Finanzbehörde	2
			Hamburg Port Authority AöR	2
			Institution/Firma	1
			Kasse.Hamburg (LB)	2
			Landesbetrieb Geoinformation und Vermessung	1
			Landesbetrieb Straßen, Brücken und Gewässer	1
		Informationssicherheit - Smartphones - Der Trojaner in	Landesbetrieb ZAF/AMD	1
009523-0001	**28.10.2021**	Ihrer Tasche (Online)	team.arbeit.hamburg	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	3
			Behörde für Schule und Berufsbildung	2
			Behörde für Verkehr und Mobilitätswende	2
			Bezirksamt Eimsbüttel	1
			Bezirksamt Hamburg-Nord	1
			Bezirksamt Harburg	1
			BIS Polizei	1
			BJV - Amtsgericht Hamburg	1
			BJV - Hamburgisches Oberverwaltungsgericht	1
			Bürgerschaftskanzlei	2
			Finanzbehörde	2
			Hochschule für Angewandte Wissenschaften Hamburg	1
			Landesbetrieb Erziehung u. Beratung	1
		Informationssicherheit - Smartphones - Der Trojaner in	Landesbetrieb Staats- und Universitätsbibliothek Hamburg	2
009523-0002	**27.10.2022**	Ihrer Tasche (Online)	Landesbetrieb ZAF/AMD	1

noch Anlage 1

			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	2
			Bezirksamt Altona	1
			Bezirksamt Bergedorf	1
			Bezirksamt Harburg	2
			BIS Amt für innere Verwaltung und Planung	1
			BJV - Verwaltungsgericht Hamburg	1
			FB - Steuerverwaltung	1
			Kasse.Hamburg (LB)	1
			Landesbetrieb Straßen, Brücken und Gewässer	1
		Informationssicherheit - Mobile Datenträger - Schadsoftware selbst installiert (Online)	Zentrum für Personaldienste (LB)	1
00524-0001	**09.12.2021**		Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	10
			Behörde für Justiz und Verbraucherschutz	14
			Behörde für Kultur und Medien	1
			Behörde für Schule und Berufsbildung	13
			Behörde für Verkehr und Mobilitätswende	10
			Behörde für Wirtschaft und Innovation	10
			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	7
			Bezirksamt Altona	20
			Bezirksamt Bergedorf	9
			Bezirksamt Eimsbüttel	17
			Bezirksamt Harburg	19
			Bezirksamt Wandsbek	15
			BIS Amt für Migration	9
			BJV - Amtsgericht Hamburg	1
			Bürgerschaftskanzlei	4
			Finanzbehörde	14
			Hochschule für Angewandte Wissenschaften Hamburg	1
			Landesbetrieb Verkehr	1
			Landesbetrieb ZAF/AMD	5
			Personalamt	6
			Senatskanzlei	8

noch Anlage 1

		Informationssicherheit - Mobile Datenträger -	Stromnetz Hamburg GmbH	1
009524-0002	**08.12.2022**	Schadsoftware selbst installiert (Online)	Telefonischer HamburgService	1
			Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration	2
			Behörde für Justiz und Verbraucherschutz	2
			BJV - Amtsgericht Hamburg	1
			BJV - Arbeitsgericht Hamburg	1
			BJV - Finanzgericht Hamburg	1
			BJV - Hamburgisches Oberverwaltungsgericht	1
			BJV - Staatsanwaltschaft Hamburg	1
			BJV - Verwaltungsgericht Hamburg	1
			FB - Steuerverwaltung	1
			Finanzbehörde	1
			Landesbetrieb Geoinformation und Vermessung	1
			Landesbetrieb Straßen, Brücken und Gewässer	1
			Rechnungshof	1
009936-0001	**15.09.2021**	SK: IT-Grundschutz BASIS für BSI-Praktiker	Senatskanzlei	1
			Behörde für Justiz und Verbraucherschutz	1
			Behörde für Kultur und Medien	1
			BIS Amt für innere Verwaltung und Planung	1
			BIS Feuerwehr (Verwaltung)	1
			BIS Polizei	2
			BJV - Arbeitsgericht Hamburg	1
			BJV - Staatsanwaltschaft Hamburg	1
			Institution/Firma	1
			Landesbetrieb Verkehr	1
009936-0002	**27.06.2022**	SK: IT-Grundschutz BASIS für BSI-Praktiker	Technische Universität Hamburg	1
			Behörde für Umwelt, Klima, Energie und Agrarwirtschaft	1
			Behörde für Wirtschaft und Innovation	1
			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	1
			Kasse.Hamburg (LB)	1
			Landesbetrieb Geoinformation und Vermessung	1
		Cybercrime - Schutz vor cyberkriminellen Handlungen	Landesbetrieb Straßen, Brücken und Gewässer	1

noch Anlage 1

010139-0001	**31.03.2022**	(online)	Landesbetrieb Verkehr	1
			Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke	1
			BIS Amt für innere Verwaltung und Planung	2
			BIS Polizei	1
			BJV - Hanseatisches Oberlandesgericht	1
			Dataport (AöR)	1
			FB - Steuerverwaltung	1
			Hamburgischer Datenschutzbeauftragter	2
			Personalamt	1
010773-0001	**13.12.2022**	SK: IT-Grundschutz BASIS für BSI-Praktiker (online)	Senatskanzlei	1
Gesamtergebnis				**442**

Hochschule	Studiengänge mit Bezügen zur Cybersicherheit	
	aktuell	**geplant**
Universität Hamburg	Bachelorstudiengang Informatik Bachelorstudiengang Software-System-Entwicklung - Pflichtveranstaltung „Verteilte Systeme und Systemsicherheit“ (in allen anderen Bachelorstudiengängen auch im Rahmen von Proseminaren, Seminaren, Projekten und Abschlussarbeiten belegbar). Masterstudiengang Informatik (M. Sc.) - Studienschwerpunkt IT-Security (mehrere Module im Umfang von 24 Leistungspunkten)	entfällt
Technische Universität Hamburg	Alle Informatikstudiengänge. Bachelorstudiengang Computer Science Bachelorstudiengang Data Science - Jeweils Modul „Einführung in die Informationssicherheit“ - Jeweils Modul „Rechnernetze und IT-Sicherheit“ (auch in den Bachelorstudiengängen Allgemeine Ingenieurwissenschaften, Engineering Science, Elektrotechnik, General Engineering Science und Technomathematik belegbar). - Modul „Informatik für Ingenieure“ Masterstudiengang Computer Science Masterstudiengang Informatik-Ingenieurwesen - Komplementäre Kurscluster zur Cybersicherheit von IT-Systemen und Cybersicherheit von Softwareanwendungen. Masterstudiengang Information and Communication Systems - Thema “Sichere und zuverlässige IT-Systeme“ in den Modulen „Sicherheit von Cyber-Physischen Systemen“, „Angewandte Kryptographie“, „Data Science zur Cybersicherheit“, „Entwicklung von sicherer Software“, „Software Sicherheit“, „Entwurf von Dependable Systems“ und „Softwaretesten“. Masterstudiengang Mechatronics, Microeletronics and Microsystems Masterstudiengang Theoretischer Maschinenbau - Modul “Entwurf von Dependable Systems“.	Ab Wintersemester 2023/2024 Studiengang Data Science (befasst sich u.a. mit dem Thema Sicherheit und Cybersicherheit.

Hochschule für Angewandte Wissenschaften	Bachelor-Studiengang Medien und Information - Wahlpflichtkurs Cyber Attacken Bachelor-Studiengang Media Systems - Pflichtmodul Kryptographie Master-Studiengang Wirtschaftsingenieurwesen /Masterschwerpunkt Informationstechnik - Cybersecurity 1 – Grundlagen der Informationssicherheit - Cybersecurity 2 – Penetration Testing und Zertifikat zum Vorfall-Experten gemäß Bundesamt für Sicherheit in der Informationstechnik - Drahtlose Sensornetze - Distributed Ledger Technology Alle Studiengänge des Departments Informatik - Pflichtmodul IT-Security Bachelor-Studiengang eGovernment (ab WiSe 2023/2024) - mehrere Module, in denen die Cybersicherheit Teil des Curriculums ist.	Master-Studiengang Cybersecurity in Kooperation mit der Technischen Hochschule Lübeck
Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg	- Bachelor-Studiengang Logistik - Master-Studiengang Informatikingenieurwesen (wird im Oktober 2024 eingestellt) - Master-Studiengang Erneuerbare Energien und intelligente Netze - Master-Studiengang Wirtschaftsingenieurwesen - Master-Studiengang Engineering Science: Defence Systems	- Bachelor-Studiengang Digital Engineering (ab Oktober 2024) - Master-Studiengang Digital Engineering (ab Oktober 2024)
Bucerius Law School	Masterprogramm: - Wahl-Lehrveranstaltung Legal Technology and Operations - Wahl-Lehrveranstaltung Blockchain Law inklusive Cyberkriminalität Summer Program: - Wahl-Lehrveranstaltung Legal Technology and Operations International Program: - Wahl-Lehrveranstaltung Introduction to Legal Technology, Operations and Innovation Bachelor of Laws-Studiengang: - Wahl-Lehrveranstaltung Ideen der Informatik im Studium Generale - Wahl-Lehrveranstaltung Einführung in die Programmierung im Studium Generale	entfällt

	- Wahl-Lehrveranstaltung Recht und Technologie (ab Herbst 2023)	
NBS Northern Business School	Bachelor-Studiengang Sicherheitsmangement	entfällt
Europäische Fernhochschule Hamburg	Keine	Master-Studiengang Wirtschaftsinformatik inklusive Schwerpunkt IT-Security (im Jahr 2024)