**BREMISCHE BÜRGERSCHAFT** **Drucksache 20/1611**
**Landtag** **(zu Drs. 20/1550)**
**20. Wahlperiode** **27.09.22**

# Mitteilung des Senats vom 27. September 2022

## Änderung der Bedrohungslage in der Cybersicherheit: Bremische IT in Großkrisenlagen

Die Fraktion der FDP hat unter Drucksache 20/1550 eine Große Anfrage zu obigem Thema an den Senat gerichtet.

Der Senat beantwortet die vorgenannte Große Anfrage wie folgt:

1. Welche Infrastrukturen im Land Bremen stuft der Senat als sogenannte Kritische Infrastrukturen ein? (Bitte sowohl private als auch staatliche Infrastrukturen aufzählen.)

   Zurzeit existiert die einzige Legaldefinition für Kritische Infrastruktur (KRITIS) im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) und der nachgeordneten Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV). Diese Verordnung legt neun Sektoren und diesen jeweils zugeordnete insgesamt 29 Branchen fest, beispielsweise den Sektor „Energie“ mit den Branchen „Stromversorgung“, „Gasversorgung“, „Kraftstoff- und Heizölversorgung“ und „Fernwärmeversorgung“.

   Für die einzelnen Branchen werden Schwellenwerte festgelegt, bei deren Überschreitung der jeweilige Betrieb als KRITIS gilt, beispielsweise der Betrieb eines Stromverteilernetzes mit einer jährlich entnommenen Arbeit (Energie) von mehr als 3 700 Gigawattstunden oder eine Kanalisation, an die mehr als 500 000 Menschen angeschlossen sind, ein Krankenhaus mit jährlich mehr als 30 000 vollstationären Fallzahlen pro Jahr oder ein Flughafen mit jährlich mehr als 20 000 000 Passagieren. Den KRITIS-Betreibern obliegen dann besondere Pflichten wie

   — dem Bundesamt für Sicherheit in der Informationstechnik eine Kontaktstelle zu benennen,

   — IT-Störungen oder erhebliche Beeinträchtigungen zu melden,

   — IT-Sicherheit auf dem Stand der Technik umzusetzen und

   — dies alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik nachzuweisen.

   Auf Grundlage dieser Schwellenwerte fallen in der Freien Hansestadt Bremen 15 Betriebe und Einrichtungen unter die BSI-KritisV.

   Das Amt für Straßen und Verkehr Bremen (ASV) ist Betreiber von Lichtsignalanlagen. Diese sind nach der BSI-KritisV eine Kritische Infrastruktur im Sektor Transport und Verkehr, Anlagenkategorie Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr.

   Nach Bewertung des Senats haben hierüber hinaus zahlreiche weitere Betriebe und Einrichtungen wichtige Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit

oder andere dramatische Folgen eintreten würden. Beispielhaft seien der Flughafen Bremen und die Bremer Stadtreinigung (DBS) genannt, die für das Funktionieren unseres Gemeinwesens von sehr großer Bedeutung sind, ohne die Schwellenwerte der BSI-KritisV zu erreichen.

Mit dem am 28. Mai 2021 in Kraft getretenen Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) gibt es den neuen KRITIS-Sektor Siedlungsabfallentsorgung (Sammlung, Beseitigung, Verwertung). Um den Jahreswechsel 2022/2023 soll ein entsprechender Referentenentwurf für die dritte Änderungsverordnung der BSI-KritisV vorliegen.

In der Wasserversorgung (das heißt Versorgung mit Nutz- und Trinkwasser) sind die wesernetz Bremen sowie Bremerhaven GmbH als Kritische Infrastrukturen einzustufen. Für die Abwasserentsorgung ist in der Stadtgemeinde Bremen die hanseWasser Bremen GmbH und für Bremerhaven die Bremerhavener Entsorgungsgesellschaft mbH (BEG) als Kritische Infrastruktur einzustufen.

Die Bremer Stadtreinigung und dazugehörige GmbH gehören zu dem KRITIS-Sektor Siedlungsabfallentsorgung. Es ist davon auszugehen, dass sie in der ersten Jahreshälfte 2023 offiziell als KRITIS einzustufen sind.

Die BSAG ist dem Sektor Transport und Verkehr zuzurechnen. Sie ist formal nicht als KRITIS einzustufen, aber dem Bereich systemrelevante Infrastrukturen zuzurechnen.

Den Flughafenbetreibern wurden notwendige Cybersicherheitsmaßnahmen durch die VO (EU) 2019/1583 auferlegt.

2. Welche Unternehmen und auch Zulieferer könnten vor dem Hintergrund des IT-Sicherheitsgesetzes 2.0 zukünftig zu der Kategorie der „Unternehmen im besonderen öffentlichen Interesse“ gehören?

   Unternehmen, die nach dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) in den Bereich der „Unternehmen von besonderem öffentlichen Interesse“(UBI) fallen, sind in der Vergangenheit vom Bund (Bundesamt für Sicherheit in der Informationstechnik) und ergänzend vom Land Bremen (Bereich Wirtschaftsschutz des Landesamtes für Verfassungsschutz) individuell betreut worden.

   Ob und wie diese Unternehmen, die in den Bereich UBI 1 fallen, Teil einer landesspezifischen Cybersicherheitsarchitektur werden, ist zu diesem Zeitpunkt noch nicht abschließend bestimmbar.

   Unternehmen in der weiteren Definition von UBI (2 und 3) stellen mittelbar aus Sicht des Senats wesentliche Teile der hiesigen Daseinsvorsorge sicher und müssen demnach in den Fokus der Cybersicherheitsarchitektur Bremens genommen werden. Hier ist vor allem die Frage der Interdependenzen stärker zu beleuchten, um relevante Wertschöpfungsketten, zum Beispiel durch den Ausfall eines Zulieferers oder Dienstleisters, nicht zu übersehen.

   Die Rechtsverordnung nach § 10 Absatz 5 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik zur Festlegung der genauen Kriterien zur Bestimmung eines Unternehmens als UBI 2 wurde nach hiesiger Information noch nicht erlassen.

3. Von wie vielen Cyberattacken im Land Bremen hat der Senat im Zeitraum von Januar 2019 bis Juni 2022 Kenntnis erhalten?

   Eine valide, quantitative Erhebung hinsichtlich der Anzahl von „Cyberattacken“ im Land Bremen ist mangels vorhandener Legaldefinition nicht ohne weiteres möglich. So stellen etwa gezielte Schwachstellenscans eine Vorbereitungshandlung für „Cyberattacken“ dar, ohne dass zwingend

eine tatsächliche Kompromittierung erfolgen muss oder ein Straftatbestand erfüllt wäre. Das Kriminalitätsphänomen „Cybercrime“ wiederum beschreibt eine Vielzahl unterschiedlicher strafrechtlich bewerteter Delikte, welche verschiedene Deliktsbereiche tangieren können.

Auf Grundlage der Daten der Polizeilichen Kriminalstatistik sind im Erfassungszeitraum von Januar 2019 bis einschließlich Dezember 2021 insgesamt 7 878 Straftaten mit Bezug zum Phänomen „Cybercrime“ im Land Bremen erfasst worden.

Unter dem Begriff „Cyberattacke“ wird im weitesten Sinne ein Angriff auf eine Informationstechnologie beziehungsweise entsprechende Infrastrukturen verstanden. Da der Terminus „Cyberattacke“ im polizeilichen Kontext nicht weiter definiert wird, wird zu einer konkreten Beantwortung der Fragestellung daher Bezug zu den in einzelnen Vorgängen skizzierten Sachverhalten genommen. Folglich werden unter „Cyberattacke“, in Anlehnung an das Bundeskriminalamt Lagebild „Cybercrime“, jene Straftaten verstanden, die einen Verstoß gegen:

— § 202a Strafgesetzbuch Ausspähen von Daten,

— § 202b Strafgesetzbuch Abfangen von Daten,

— § 202c Strafgesetzbuch Vorbereiten des Ausspähens von Daten,

— § 303a Strafgesetzbuch Datenveränderung,

— § 303b Strafgesetzbuch Computersabotage,

— § 303b Absatz 4 Strafgesetzbuch Computersabotage in besonders schweren Fällen

darstellen und weiterführend dem Phänomen „Cybercrime“ zugeordnet werden können.

In Anbetracht der dargestellten Operationalisierung konnten im betrachteten Zeitraum von Januar 2019 bis einschließlich Dezember 2021 insgesamt 1 231 Cyberattacken identifiziert werden. Die Ziele der Attacken waren sowohl Privatpersonen, als auch Institutionen, Behörden und Unternehmen.

In den vergangenen Jahren durchgeführte Erhebungen und Forschungen des „Kriminologischen Forschungsinstituts Niedersachsen e. V.“ führten zu der Erkenntnis, dass bundesweit über 90 Prozent der Angriffe nicht polizeilich bekannt geworden sind. Vor diesem Hintergrund ist von einem hohen Dunkelfeld in dem Deliktsbereich auszugehen.

Das für staatlich gelenkte Cyberangriffskampagnen zuständige Landesamt für Verfassungsschutz in Bremen erhielt im angefragten Zeitraum von Januar 2019 bis Juni 2022 Kenntnis von 30 „Cyberattacken“ inklusive entsprechender Vorbereitungshandlungen auf Entitäten im Land Bremen, die in den eigenen Zuständigkeitsbereich fallen.

a) Welche Infrastrukturen, Behörden und Unternehmen waren von Cyberattacken betroffen?

   Die „Angriffe“ richteten sich gegen Institutionen aus der Wirtschaft, der Forschung, gegen staatliche Institutionen und Privatpersonen, wobei die Betroffenheit in der Wirtschaft mit deutlichem Abstand am größten war. Die „Angriffe“ erfolgten branchenübergreifend. Darüber hinaus kam es bei Vereinen, Arztpraxen/Kliniken, Banken sowie Bildungseinrichtungen und Behörden zu erfassten Straftaten im Kontext von „Cyberattacken“.

b) Auf welche Art und Weise haben diese Angriffe stattgefunden?

   Die „Angriffe“ erfolgten auf verschiedene Art und Weise und durch unterschiedliche Angriffstools. So kann zum Beispiel bei einem fest-

gestellten Ransomware-Trojaner (Verschlüsselung aller Systeme) davon ausgegangen werden, dass mittels vorgelagertem Eindringen in die IT-Infrastruktur Daten von Unternehmen abgeschöpft wurden. Eine an die Abschöpfung von Unternehmensdaten anknüpfende Erpressungssituation wird in solchen Fällen als „double Extortion“ bezeichnet, das heißt die Täter verlangen finanzielle Mittel zur Entschlüsselung der IT-Infrastruktur sowie zum Rückkauf der entwendeten Daten.

Mangels spezieller Kennzeichnungen in den polizeilichen Systemen und der Polizeilichen Kriminalitätsstatistik (PKS) werden die unterschiedlichen Arten von „Cyberangriffen“ auf Unternehmen, Behörden und sonstige Institutionen nicht konkret und systematisch erfasst.

Zur Erlangung von Informationen über Art und Weise eines stattgefundenen Cyberangriffes müssten in Anbetracht des Umstands, dass diese Daten keiner automatisiert auswertbaren Erfassung unterliegen, die vorgenannten 1 231 eruierten Vorgänge polizeilich händisch ausgewertet werden, was mit einem vertretbaren Aufwand nicht möglich ist. Gleichwohl lässt sich festhalten, dass die bekannt gewordenen „Angriffe“ unter anderem durch beziehungsweise in Form von Phishing, Spear-Phishing, Credential-Phishing, Brute-Force-Angriffen, Supply-Chain-Angriffen, Distributed Denialof-Service (DDoS), Webshell, ProxyShell-Exploit und Cobalt Strike erfolgten.

c) Wie viele dieser Cyberattacken waren erfolgreich und wie viele konnten schadensfrei abgewehrt werden?

Die Operationalisierung/Messbarkeit des Erfolgs von „Cyberattacken“ im Sinne der Fragestellung kann seitens des Senats nicht valide beurteilt werden. Um bewerten zu können, ob ein Cyberangriff aus Sicht der Angreifenden erfolgreich war, müssten Informationen zur Zielsetzung und Intention dieser vorliegen. Das unerlaubte Eindringen in ein technisches System kann, aber muss nicht zwingend einem Erfolg aus Sicht der Angreifenden gleichkommen. Der Senat wird regelmäßig nicht über erfolgreich abgewehrte Cyberangriffe informiert.

Für den Bereich der Verwaltung kann aus eigener Sicht einschränkend gesagt werden, dass auch hier vereinzelt Mitarbeitende Opfer von oben genannten Phishing-Mails wurden und gefährliche Links aufgerufen haben. Hier wurde in Einzelfällen zwar kurzzeitig Schadcode auf Endgeräten der Verwaltung aktiv aber regelmäßig durch die aktiven Sicherheitsmaßnahmen umgehend ein tatsächlicher Schaden abgewendet und die betroffenen Systeme umgehend bereinigt.

Diese Fälle gingen dann auch nicht als erfolgreiche Angriffe in die Statistik ein.

Gleichwohl hat die Freie Hansestadt Bremen für die Bereiche Hochschulen, Forschungseinrichtungen, Krankenhäuser und die öffentliche Verwaltung im Land Bremen in 2019: 20, 2020: vier, 2021: sechs und im 1. Halbjahr 2022: sieben Ereignisse und in Bremerhaven 2019: zwei, 2020: drei, 2021: ein und im 1. Halbjahr 2022: null Ereignisse notiert.

d) Welche Schäden haben die Attacken jeweils verursacht, die im Sinne der Initiatoren erfolgreich waren?

Auch hier können nur Aussagen für die Verwaltung gemacht werden. Im angefragten Zeitraum sind in der Verwaltung keine Schäden durch Cyberangriffe entstanden.

e) Wie hoch waren die Kosten zur Behebung der jeweiligen Schäden?

Siehe Antwort zu „d“; da in der Verwaltung keine Schäden entstanden sind, sind auch keine Kosten zur Behebung angefallen. In einem

Fall gab eine Organisation an, dass für die Eingrenzung eines Ereignisses ein Aufwand von circa 200 Euro entstanden sei.

f) Wie lange war die Wirkdauer der jeweiligen Angriffe?

Die verursachten Schäden, Kosten zur Behebung und Wirkdauer der jeweiligen „Angriffe“ im Sinne der Fragestellung werden durch den Senat nicht erfasst. Entstandene Schäden infolge eines Cyberangriffs können unterschiedlich ausgeprägte Auswirkungen auf Unternehmen beziehungsweise Institutionen entfalten, wie beispielweise Kostenaufwände für den Wiederaufbau von IT-Infrastrukturen und nicht abzuwendende Produktionsausfälle. Insofern wird an dieser Stelle auf die im Rahmen von wirtschaftsinternen Untersuchungen durch Wirtschaftsverbände, Institutionen und Vereinigungen eruierten Schadensberichte verwiesen. (https://www.bitkom.org/) (Stand 27. September 2022)

In der bremischen Verwaltung gab es im angefragten Zeitraum durch Cyberangriffe keine Ausfälle und daher auch keine Wirkdauer.

g) Welche Störungen wurden jeweils durch die Angriffe verursacht?

Nach Kenntnis des Senats in Bezug auf bekannt gewordene Verfahren verursachten die „Angriffe“ sowohl kurzzeitig andauernde Störungen als auch mehrtägige Produktionsausfälle bis hin zu einem vollständigen Stillstand der unternehmerischen Abläufe.

Für die bremische Verwaltung ist auszuführen, dass es im angefragten Zeitraum keine Störungen durch Angriffe gab.

h) Konnten die Schäden durch die Unternehmen/Infrastrukturen selbst behoben werden und falls nein, welche zusätzliche Kapazitäten/Ressourcen waren notwendig (öffentliche/private Ressourcen)?

Dem Senat liegen diesbezüglich keine Informationen vor; da in der bremischen Verwaltung keine Schäden angefallen sind, musste auch nicht auf externe Ressourcen zurückgegriffen werden.

4. Inwiefern hat sich nach Auffassung des Senats seit 2019 die Gefährdungslage für kritische Infrastrukturen, Behörden und Unternehmen im Land Bremen Opfer von Cyberattacken zu werden, insbesondere auch vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine, verändert?

Der Trend zu einer erhöhten Gefährdungslage im Cyberraum wächst in Abhängigkeit zur zunehmenden Digitalisierung der Gesellschaft und des öffentlichen Raumes ununterbrochen. Jedes Jahr werden mehrere Millionen neue Malware-Varianten bekannt und neue Rekordzahlen von Cyberangriffen beziehungsweise Angriffsversuchen registriert.

Die Wahrscheinlichkeit für Unternehmen, öffentliche Verwaltungen und KRITIS-Betreiber, Opfer staatlich gesteuerter Cyberattacken zu werden, hat mit dem Krieg gegen die Ukraine deutlich zugenommen. Gründe hierfür sind eine grundsätzlich erhöhte Aktivität im Cyberraum, der Wegfall etwaiger außenpolitischer Handlungshemmnisse und das Agieren einer Vielzahl verschiedener Cyberakteure auf allen Seiten der Konfliktparteien, wodurch auch die Gefahr von Spill-Over-Effekten und Kollateralschäden zugenommen hat. Der durch die Presse bekannt gewordene Angriff auf ein Unternehmen aus dem Bereich der Windenergie stellt einen Vorfall dar, bei dem ein Bremer Unternehmen in Mitleidenschaft gezogen wurde. Insbesondere aufwendigere staatliche Cyberaktionen bedürfen einer entsprechenden Vorbereitungs- und Implementationszeit, sodass ein Zeitverzug bei Cyberangriffen im Vergleich zum „analogen“ Krieg nicht ungewöhnlich ist. Die Gefährdungslage im Cyberraum für den Bund und das Land Bremen wird seitens der Sicherheitsbehörden nach wie vor als hoch eingeschätzt.

5. Welche zusätzlichen Maßnahmen sind seit 2019 ergriffen worden, um dem Ausfall Kritischer Infrastrukturen (beispielsweise Strom-, Gas-, Fernwärme- und Wasserversorgung) durch Cyberattacken vorzubeugen?

   Die Freie Hansestadt Bremen hat insbesondere in den Bund-Länder-Arbeitsgruppen der Ständigen Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz) und des IT-Planungsrats aktiv mitgewirkt, um die Ausgestaltung des IT-Sicherheitsgesetzes 2.0 für die Region mitzugestalten. Die vom IT-Sicherheitsgesetz betroffenen Unternehmen haben in ihrem Verantwortungsbereich Informationssicherheitsmanagementsysteme oder branchenspezifische Sicherheitsstandards (B3S) etabliert, um den Anforderungen der zuständigen Behörde (Bundesamt für Sicherheit in der Informationstechnik) zu genügen. Weiterhin haben der Senator für Inneres (Federführung) und der Senator für Finanzen damit begonnen, eine Cybersicherheitsstrategie des Landes Bremen zu entwickeln.

   Der Senator für Inneres nimmt sowohl auf der Arbeitsebene als auch auf Leitungsebene mit dem Staatsrat an der „Länderarbeitsgruppe Cybersicherheit“ teil. Diese Plattform dient der Abstimmung der Länder zu den Themen des Nationalen Cyber-Sicherheitsrates (NCSR) und der Berichterstattung an die Innenministerkonferenz (IMK), des allgemeinen Erfahrungsaustauschs der Länder und des Bundes über die Aspekte der Cybersicherheit sowie der Koordination von Initiativen und Maßnahmen zur Erhöhung der Cybersicherheit. Darüber hinaus erarbeitet das Land Bremen zurzeit einen Kooperationsvertrag mit dem Bundesamt für Sicherheit in der Informationstechnik SI (vergleiche Antwort zu Frage 14). Konkrete Maßnahmen, um dem Ausfall Kritischer Infrastrukturen vorzubeugen, obliegen den jeweils zuständigen Ressorts, für die in der Frage bezeichneten Bereiche der Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau.

   Seit März des Jahres 2022 ist das Landeskriminalamt als dem Geschäftsbereich des Senators für Inneres zugeordnete Behörde darüber hinaus Teilnehmer der Allianz für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik in der Gruppe „Behörden und Organisationen mit Sicherheitsaufgaben.“ Das Bundesamt für Sicherheit in der Informationstechnik betreibt mit der Allianz für Cybersicherheit ein Forum, in welchem sich die Teilnehmenden (unter anderem Unternehmen, Behörden mit Sitz in Deutschland) zum Thema Cybersicherheit informieren und austauschen können. Aus diesen Beratungen werden weiterführende Empfehlungen und gewonnene Erkenntnisse geprüft und erforderlichenfalls umgesetzt. Dieses mündet beispielsweise in der Implementierung von behördeninternen Sicherheitsmechanismen, wie zum Beispiel Firewalls oder Notstromversorgungen.

   Im Ressort der Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau wurde im Jahr 2021 die Informationssicherheitsleitlinie der Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau (IS-LL SKUMS) in Kraft gesetzt.

   hanseWasser:

   In der Wasserversorgung und Abwasserentsorgung werden folgende zentrale Maßnahmen durchgeführt:

   — zweijährliche externe Prüfungen gemäß § 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik mit Nachweis gegenüber Bundesamt für Sicherheit in der Informationstechnik,

   — Informationssicherheits-Managementsysteme (ISMS), inklusive interner Audits von Werken nach § 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (inklusive ISO 27001), Management Reviews und Regelsysteme,

— Übungen und Tests (zum Beispiel Notfallübungen in Wasserwerken oder Penetrationstests, das heißt Simulation von Cyberattacken) sowie

— ein Krisen- und Notfallmanagement.

Zudem sind die Abwassernetzwerke in Bremerhaven (zum Beispiel Pumpwerke oder Kläranlagen) weitestgehend als Inselnetz aufgebaut und somit von außen nicht erreichbar oder unterliegen weiteren Zugangsbeschränkungen.

Im Amt für Straßen und Verkehr wurden folgende Maßnahmen ergriffen:

— Einrichtung der Stabsstelle Informationssicherheit.

— Zweijährig stattfindende Prüfung nach §8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, auf Grundlage eines vom Bundesamt für Sicherheit in der Informationstechnik anerkannten branchenspezifischen Sicherheitsstandards (B3S) und durch ein vom Bundesamt für Sicherheit in der Informationstechnik akkreditiertes Prüfunternehmen, um die IT-Sicherheit auf dem Stand der Technik nachzuweisen.

— Ein ergänzendes Audit findet in den Jahren statt, in dem keine Prüfung stattfindet.

— Einrichtung einer Kontaktstelle nach § 8b Absatz 3 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

Die Bremer Stadtreinigung betreibt alle ihre Fachverfahren im Rechenzentrum bei Dataport. Für einen Großteil der Fachverfahren wurden spezielle Sicherheits-SLAs bei Dataport eingekauft.

Die BSAG hat im August 2022 die Stelle eines Informationssicherheitsbeauftragten ausgeschrieben und wird sich nach Stellenbesetzung verstärkt dem Themenbereich der Informationssicherheit annehmen.

Zur Sicherstellung der Stromversorgung wurden bei der Ortspolizeibehörde Bremerhaven (OPB) Notstromaggregate eingesetzt. Sie können kurzfristig einspringen und mit Unterstützung des Technisches Hilfswerk auch über einen längeren Zeitraum betrieben werden. Auf die Gasversorgung ist die Ortspolizeibehörde Bremerhaven grundsätzlich nur indirekt über das Fernwärmenetz (Müllverbrennungsanlage) angewiesen.

Die Feuerwehr Bremerhaven, die die Aufgaben der Ortskatastrophenschutzbehörde wahrnimmt, hat gemeinsam mit der Magistratsverwaltung die Katastrophenschutzpläne, unter anderem in den Bereichen Energie und Informationstechnik, neu aufgestellt. Dazu gehört zukünftig auch die Vorbereitung auf Cyberangriffe/Ausfall KRITIS. Weitere KRITIS-Relevante Bereiche sind ebenfalls erfasst und werden fortwährend auf neue Herausforderungen angepasst.

Weiterhin sind sämtliche Bereiche der Feuerwehr, wie Funkanlagen, die Feuer- und Rettungswache und die Leitstellentechnik, schon vor 2019 ersatz- beziehungsweise notstromversorgt.

6. Welche zusätzlichen Präventionsmaßnahmen zum Schutz vor Cyberattacken sind durch den Senat, beziehungsweise die jeweiligen Behörden, seit 2019 eingeführt und/oder verstetigt worden, insbesondere bei den

   a) Sicherheitsbehörden,

   b) Dienststellen der öffentlichen Verwaltung,

   c) den öffentlichen Versorgungsunternehmen,

   d) den öffentlichen Verkehrsunternehmen,

   e) der in Bremen angesiedelten Industrie und Wirtschaft sowie

   f) den Hochschulen und Forschungsinstituten in Bremen?

a) Sicherheitsbehörden

Das Landesamt für Verfassungsschutz in Bremen ist im Rahmen seiner rechtlichen Befugnisse für die Spionageabwehr fremder Nachrichtendienste und somit auch für die Abwehr staatlich gesteuerter Cyberangriffe zuständig. Wesentlicher Bestandteil der Cyberabwehr ist neben Attribution und Detektion die Prävention durch den Wirtschaftsschutz. Das Landesamt für Verfassungsschutz führt diesbezüglich sowohl mit geheimschutzbetreuten Unternehmen als auch mit KRITIS-Betreibern und Unternehmen von besonderem öffentlichem Interesse regelmäßig Sensibilisierungsgespräche zu Gefährdungen sowie aktuellen Themen und Entwicklungen. In dem Zuge können unter anderem „Indicators of Compromise“ und entsprechende Detektionsregeln zur Identifikation von maliziöser Software zur Verfügung gestellt werden.

Die Polizei Bremen hat im Bereich der Informationssicherheit zwei zusätzliche Stellen geschaffen, die im Laufe des Jahres 2022 besetzt werden sollen. Das für das Kriminalitätsphänomen „Cybercrime“ zuständige Referat der Polizei Bremen (K134) nimmt unter anderem die gefahrenabwehrende Präventionsarbeit zum Thema Cybercrime wahr. In Gestalt einer „Zentralen Ansprechstelle Cybercrime“ (ZAC) werden als Aufgabe des Landeskriminalamtes Wirtschaftsunternehmen und sonstigen Institutionen/Bereichen mit Bezug zur Wirtschaft unternehmensbegleitende Awareness-Maßnahmen durch das K 134 angeboten.

Sowohl in der Polizei Bremen als auch in der Ortspolizeibehörde Bremerhaven erfolgen wiederkehrende Sensibilisierungen der Mitarbeitenden in Bezug auf das Thema „Cybersicherheit.“ Darüber hinaus stehen verschiedene Fortbildungsveranstaltungen, wie zum Beispiel „Informationssicherheit am Arbeitsplatz“, zur Verfügung.

Weiterhin erfolgt in Zusammenarbeit mit den Betreibern der IT-Systeme der Behörden eine fortwährende Prüfung und gegebenenfalls Anpassung eben jener Systeme vor dem Hintergrund der sich dynamisch wandelnden Anforderungsprofile an die IT-Sicherheit.

Im Bereich der IT-Leitstelleninfrastruktur der Feuerwehr Bremerhaven wurde seit 2019 eine neue IT-Architektur implementiert, die unter anderem Cyberattacken auf Backup-Systeme verhindern soll.

b) Dienststellen der öffentlichen Verwaltung

In der zentralen IT-Infrastruktur des Landes werden Angriffserkennungssysteme eingesetzt, die insbesondere beim zentralen Verzeichnisdienst des Landes Auffälligkeiten automatisch registrieren und melden.

Bestehende Passwortrichtlinien in Bremen und Bremerhaven wurden den Entwicklungen entsprechend angepasst.

Das vom Senator für Finanzen zentral koordinierte Fortbildungsprogramm für Informationssicherheitsbeauftragte wurde fortgesetzt. Sowohl in Bremen als auch in Bremerhaven werden für die Beschäftigten der Stadtverwaltung Sensibilisierungsmaßnahmen (Fortbildungen) angeboten. Neben internen Fortbildungen zur Informationssicherheit am Arbeitsplatz findet regelmäßig die Veranstaltung „Die Hacker kommen“ statt.

Zusätzlich können die Beschäftigten das E-Learning-Tool „Behörden-IT-Sicherheitstraining (BITS)“ nutzen, welches in den Intranets zu finden ist.

Anlassbezogen werden in den Intranets Hinweise auf Entwicklungen oder Gefährdungen im IT-Bereich gegeben.

Ein wesentlicher und wichtiger Punkt zur Unterstützung der Präventionsmaßnahmen sind die Erkenntnisse, die das CERT Nord, das „Computer Emergency Response Team" für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt, und das Bundesamt für Sicherheit in der Informationstechnik dem Land Bremen und den Stadtverwaltungen Bremen und Bremerhaven zur Verfügung stellen.

c) Öffentliche Versorgungsunternehmen,

d) öffentliche Verkehrsunternehmen,

e) in Bremen angesiedelte Industrie und Wirtschaft

Bezüglich der öffentlichen Versorgungsunternehmen, der öffentlichen Verkehrsunternehmen und der in Bremen angesiedelten Industrie und Wirtschaft wird auf Frage 5 verwiesen.

Ergänzend wird zu der in Bremen angesiedelten Industrie und Wirtschaft folgendes ausgeführt:

Der Flughafen Bremen führt seit langem umfangreiche IT-Sicherheitsmaßnahmen durch. Bestärkt durch die Vorgaben der Verordnung (EU) 2019/1583 werden die Maßnahmen intensiviert und einer Begutachtung unterzogen. Die Überwachung der Maßnahmen obliegt der Luftsicherheitsbehörde sowie dem Bundesamt für Sicherheit in der Informationstechnik.

Auch im maritimen Bereich nimmt die Bedrohung durch Cyberangriffe stetig zu. Hingewiesen sei hier auf Angriffe auf diverse Großreedereien. Das hat die Senatorin für Wissenschaft und Häfen dazu veranlasst, die Sensibilität im Bereich Cybersicherheit für den Bereich der bremischen Häfen zu erhöhen. Daher wurde in 2019 bei bremenports die Institution des Port Cyber Security Officers (PCSO) geschaffen. Dieser berät die Unternehmen in den Häfen und auch die in den Häfen zuständigen Behörden im Bereich Cybersicherheit und trägt somit zur erhöhten Sensibilisierung in diesem Feld bei.

f) Hochschulen und Forschungsinstitute in Bremen

Die Universität baut ein Informationssicherheitsmanagementsystem nach CISIS12 in Zusammenarbeit mit dem Senator für Finanzen auf. Die ersten Schritte sind bereits erfolgt und auch mit den anderen Hochschulen abgestimmt.

An den Hochschulen Bremen und Bremerhaven ist die Besetzung der Stelle eines Informationssicherheitsbeauftragten erfolgt beziehungsweise in Arbeit.

7. Wie sind die für die Cybersicherheit zuständigen Behörden im Land Bremen personell und finanziell ausgestattet? Ist diese Ausstattung im Angesicht der gegenwärtigen Bedrohungslage noch ausreichend, wenn ja, warum, wenn nein, wo muss mit welchen Geldern nachgebessert werden?

Neben der in der Antwort auf Frage 6 genannten Aufgabe ist das K134 der Polizei Bremen im Zuge der Wahrnehmung von polizeilichen Aufgaben der Strafverfolgung bei Fällen von Cybercrime im engeren Sinne (§§ 202ad, 303ab Strafgesetzbuch) originär verantwortlich. Zusätzlich werden durch das K134 anderen Ermittlungsdienststellen der Direktion Kriminalpolizei/Landeskriminalamt sowie der Ortspolizeibehörde Bremerhaven ermittlungsbegleitende Beratungs- und Unterstützungsmöglichkeiten zum Thema Cybercrime angeboten. Hinsichtlich der personellen Ausstattung des Referats wird auf die Antworten auf die Fragen 17 und 19 verwiesen.

Die Geschäftsverteilung des Landesamtes für Verfassungsschutz ist gemäß Verschlusssachenanweisung als „STRENG GEHEIM“ eingestuft, insofern muss eine Beantwortung dieser Frage in Bezug auf das LfV unterbleiben.

Der Senator für Inneres rechnet perspektivisch damit, dass es erforderlich werden wird, die für Cybersicherheit zuständigen Behörden seines Geschäftsbereichs sowie der Stadt Bremerhaven personell und materiell substanziell zu stärken, um das in diesem Bereich erheblich erhöhte Arbeitsaufkommen sachgerecht bewältigen zu können. Die entsprechenden Bedarfe sollen in dem eingerichteten Projekt Cybersicherheit des Senators für Inneres erhoben werden.

8. Inwiefern werden diese Präventionsmaßnahmen regelmäßig einer Evaluation in Bezug auf ihre Wirksamkeit unterzogen?

   Die Präventionsmaßnahmen in der Cyberabwehr werden sowohl intern als auch durch den Verbund der Polizeien des Bundes und der Länder (einschließlich der Ortspolizeibehörde Bremerhaven) fortlaufend evaluiert und an aktuelle Gegebenheiten und Entwicklungen angepasst. Eine Revision der Sicherheitseinrichtungen der Polizei wurde zuletzt aufgrund des Ukrainekonfliktes durchgeführt.

9. Inwieweit gibt es mittlerweile bei den zuständigen Behörden ein „Worst-Case-Szenario“ für Cyberattacken, insbesondere vor dem Hintergrund, dass im Jahr 2019 weder die Ortspolizeibehörde Bremen, noch die Feuerwehr Bremen im Besitz entsprechender Notfallpläne waren? Inwiefern wurden entsprechende Abwehr- oder Einsatzpläne seit 2019 bei den anderen Behörden vor dem Hintergrund der veränderten Bedrohungslage angemessen angepasst? Inwiefern gibt es im Land Bremen weiterhin Behörden, die keine entsprechenden Abwehr- und Einsatzpläne haben?

   Die IT-Sicherheitsmaßnahmen der Polizei Bremen, der Ortspolizeibehörde Bremerhaven und der Feuerwehren richten sich nach IT-Sicherheitskonzepten, die fortwährend an die veränderte Sicherheitslage angepasst werden. Die Behörden verfügen über mehrere Datensicherungsebenen sowie über Notfall- und Wiederherstellungspläne für zentrale Bereiche ihrer IT-Landschaft.

10. Inwiefern sind das Land Bremen und die Städte Bremen und Bremerhaven auf eventuelle Großschadenslagen, welche durch Cyberattacken hervorgerufen werden, vorbereitet, und wie sehen diese Vorbereitungen aus?

    Gesellschaft und Wirtschaft zeichnen sich zum einen durch hohe Komplexität und vielschichtige Wechselwirkungen und Abhängigkeiten aus, zum anderen gibt es kaum noch Prozesse, die nicht von funktionierenden IT-Strukturen abhängen. Somit können „erfolgreich“ vorgenommene Cyberattacken verschiedene Arten von Großschadenslagen und Katastrophen bewirken. Aus diesem Grund ist es unmöglich, jeweils fallspezifische Vorbereitungen zu treffen, es gilt vielmehr, die für Gefahrenabwehr zuständigen Behörden und Einrichtungen generalistisch vorzubereiten, indem zum einen Leistungsfähigkeit und Einsatzbereitschaft sichergestellt werden und zum anderen Zuständigkeiten und Führungsorganisation festgelegt sind. Darüber hinaus liegen für die Polizeien und Feuerwehren objektbezogene Pläne, Dienstvorschriften, Konzepte sowie betriebliche Gefahrenabwehrpläne nach Störfallrecht vor. Die Entwicklung der Cybersicherheitsstrategie für das Land Bremen sieht darüber hinaus eine fortwährende Risikoanalyse in der Bewertung relevanter Themenfelder vor und schafft somit einen Mechanismus, auf sich verändernde Gefahrenlagen im Rahmen der Gefahrenprävention adäquat zu reagieren.

    Selbstverständlich sind begleitend von den Betreibern der KRITIS alle technischen und organisatorischen Maßnahmen zur Vorbeugung vor und Abwehr von Cyberattacken zu ergreifen.

    Bei der Stadtverwaltung Bremerhaven ist bezogen auf die Daten ein Rückspielen aus dem Backup und für die Netzwerke eine Abschottung der Netze möglich. Bei durch Cyberangriffe verursachten Großschadenslagen werden das Bundesamt für Sicherheit in der Informationstechnik und ge-

gebenenfalls andere benachbarte Behörden und Organisationen mit Sicherheitsaufgaben durch die Ortspolizeibehörde Bremerhaven eingebunden.

Falls die verursachten Schäden über eine Großschadenslage hinaus das Leben, die Gesundheit, die Umwelt, erhebliche Sachwerte oder die lebenswichtige Versorgung der Bevölkerung in einem solchen Maße gefährden, dass zur Bekämpfung die für die Gefahrenabwehr zuständigen Behörden mit den Feuerwehren und Rettungsdiensten sowie den Einheiten und Einrichtungen des Katastrophenschutzes unter zentraler Leitung zusammenwirken müssen, bilden die Kommunen und erforderlichenfalls das Land einen Katastrophenschutzstab.

11. Welche Aufgaben im Rahmen der gesamtbremischen IT-Sicherheit nehmen die bei dem Senator für Finanzen angesiedelten CIO (Chief Information Officer) und der CISO (Chief Information Security Officer) wahr? Über welche personellen und finanziellen Ressourcen verfügen diese jeweils?

    Der CIO trägt die Verantwortung für die im Ressort des Senators für Finanzen vertraglich abgesicherten IT-Dienstleistungen für die bremische Verwaltung (ohne den Magistrat der Stadt Bremerhaven). Dies betrifft insbesondere die zentralen Infrastrukturen und Dienste sowie die Vertretung in den entsprechenden Aufsichtsgremien der Anstalt des öffentlichen Rechts Dataport.

    Die Aufgaben umfassen weiterhin die Sicherstellung der Digitalen Souveränität, die Digitalisierung von Verwaltungsdienstleistungen und die Weiterentwicklung von Basisinfrastrukturen. Der CIO ist zudem Mitglied des IT-Planungsrats und vertritt die bremischen Interessen zusammen mit und für Bund, Länder und Kommunen.

    Die CISO-Stelle beim Senator für Finanzen ist als Landesbeauftragter für Informationssicherheit der Verwaltung ausgewiesen. Die Aufgaben umfassen insbesondere die Leitung der interministeriellen Arbeitsgruppe Informationssicherheit, die Fortentwicklung des zentralen Informationssicherheitsmanagementsystems, die Entwicklung von übergreifenden Compliance-Anforderungen sowie die Vertretung Bremens in länderübergreifenden Gremien. Die CIO- und die CISO-Stellen sind für diese Aufgaben mit angemessenen personellen und finanziellen Ressourcen ausgestattet worden.

12. Inwiefern gibt es eine standardisierte Vorfallbearbeitung nach einer Cyberattacke? Wie unterscheidet sich die Vorfallbearbeitung nach einer erfolgreichen Cyberattacke von der einer abgewehrten Cyberattacke?

    Für den internen Ablauf über die Meldung eines IT-Sicherheitsvorfalls gibt es einen Prozessablauf, in dem dann auch weitere Institutionen in der Meldekette, wie zum Beispiel das CERT Nord mit einbezogen sind.

13. Inwiefern wurden seit 2019 die Dienste von „white hat“ Hackern im Land Bremen in Anspruch genommen, um entsprechende Sicherheitslücken in bremischen IT-Infrastrukturen aufzudecken? Inwiefern hat die Firma Dataport entsprechende Dienste in Anspruch genommen?

    Dataport hat bereits im Jahr 2019 begonnen, im Zuge des Auf- und Ausbaus des Cyber-Defense-Centers eigene Expertise im Bereich „White Hacking“ und PEN-Testing aufzubauen. Seit 2020 stehen ausgebildete PEN-Tester bei Dataport zur Verfügung.

    Tests mit Bezug auf durch Bremen genutzte IT-Betriebsinfrastrukturen und Verfahren bei Dataport wurden durch das Cyber-Defense-Center von Dataport durchgeführt.

    Angaben über eine darüberhinausgehende Beschäftigung von White Hackern liegen dem Senat nicht vor.

14. Inwieweit hat sich die Kooperation des Landes Bremen bei dem Thema Cybersicherheit innerhalb des föderalen Zusammenspiels und in der Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik seit 2019 verändert?

    Der Senator für Inneres und der Senator für Finanzen stehen in einem engen Austausch mit dem Bundesamt für Sicherheit in der Informationstechnik, um ein bilaterales Abkommen zur Unterstützung in Sachen Cybersicherheit voranzubringen. Aktuell befinden sich die Kooperationsfelder in der Abstimmung. Föderale Kooperationen beim Thema Cybersicherheit sind – neben den Gremien des IT-Planungsrates - insbesondere in der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz aufgewachsen. Dort, wo Informationssicherheit einer Organisation zu kurz greift, sind in den letzten Jahren weitere Möglichkeiten der kooperativen Zusammenarbeit geprüft und auch vollzogen worden. Vor allem betrifft dies die Bereiche der Aus- und Fortbildung, der Hospitation von Länderbeschäftigten im „Nationalen Cyber-Abwehrzentrum (Cyber-AZ)“. Der Ausbau des föderalen Verwaltungs-CERT Verbunds (VCV) wurde weiterverfolgt. Insgesamt haben elf Länder mit dem Bundesamt für Sicherheit in der Informationstechnik Absichtserklärungen unterzeichnet, die eine vertiefte Zusammenarbeit gewährleisten sollen. Erste Länder haben nach den Vorgaben des Bundesministeriums des Innern und für Heimat Kooperationsverträge mit dem Bundesamt für Sicherheit in der Informationstechnik geschlossen. Auch Bremen hat eine finale Abstimmung über die inhaltlichen Punkte einer Kooperationsvereinbarung durchgeführt. Die Länder haben zudem eine gemeinsame Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien entwickelt.

    Darüber hinaus findet zwischen dem Bundesamt für Sicherheit in der Informationstechnik und dem Verfassungsschutzverbund über das Bundesamt für Verfassungsschutz ein enger und professioneller Austausch statt. An dem Grundsatz der Zuständigkeit des Verfassungsschutzverbundes bei nachrichtendienstlich gesteuerten Cyberangriffen hat sich in den letzten Jahren keine Änderung ergeben.

    Das Landeskriminalamt setzt als Teilnehmer der Allianz für Cybersicherheit des Bundesamt für Sicherheit in der Informationstechnik in der BOS Gruppe die Sicherheitsvorgaben seitens des Bundesamt für Sicherheit in der Informationstechnik um und bezieht zum Beispiel Sicherheits- und Warnmeldungen aus unterschiedlichen Quellen, wie CERT-Land, CERT-Bund, sowie von verschiedenen Dienstleistern und wertet diese auf Relevanz für eigene Systeme aus, um die darin vorgegebenen Maßnahmen für eigene Systeme zu prüfen und umzusetzen.

15. Wie bewertet der Senat die am 12. Juli 2022 von der Bundesinnenministerin Nancy Faeser vorgestellte Cybersicherheitsagenda, insbesondere vor dem Hintergrund einer möglichen Grundgesetzänderung und der Neuverteilung der Zuständigkeiten zwischen dem Bund und den Ländern?

    Das Bundesamt für Sicherheit in der Informationstechnik ist mit Blick auf die Regelungen im Land Bremen bereits heute faktisch einer der wichtigsten Kooperationspartner für die Belange der Informationssicherheit. Die konkrete Weiterentwicklung in diesem Themenfeld ist noch Gegenstand der Erörterung zwischen Bund und Ländern.

    Den Ländern wurde hierzu ein Konzeptpapier zum Ausbau des Bundesamts für Sicherheit in der Informationstechnik zu einer Zentralstelle im Bund-Länder-Verhältnis übermittelt. An der Cybersicherheitsstrategie des Bundes war der Senat nicht beteiligt.

    Bis jetzt liegen dem Senat keine konkreten Vorschläge zur Grundgesetzänderung vor, sodass diese Absicht bislang in keinem politischen Meinungsbildungsprozess mündete. Eine Anpassung des Grundgesetzes

primär vor dem Hintergrund der vom Bundesamt für Sicherheit in der Informationstechnik vorgeschlagenen Unterstützung bei der Detektion von Angriffen in den Landesnetzen durch Sensorik des Bundes erscheint jedoch möglicherweise notwendig.

Die mit einer Grundgesetzänderung einhergehende Aufgabenerweiterung beim Bundesamt für Sicherheit in der Informationstechnik könnte dort zwar insbesondere ein personelles Aufwachsen zur Folge haben. Gleichzeitig würde es jedoch keine Aufgabenübertragung seitens der Länder an den Bund geben; eine landesspezifische Cybersicherheitsstrategie und -architektur kann dies folglich nicht ersetzen. Vielmehr stellen die länderspezifischen Cybersicherheitsstrategien einen wichtigen Baustein in der föderalen und auf Kooperation und Koordination ausgerichteten Cybersicherheitsstrategie des Bundes dar. Durch einen Aufgabenzuwachs beim Bundesamt für Sicherheit in der Informationstechnik ist insofern keine substanzielle Entlastung in den Ländern zu erwarten.

16. Wie hat sich die Zahl von Cyberattacken insbesondere auf kleinere und mittlere Unternehmen im Land Bremen seit 2019 entwickelt? Ist seit dem 24. Februar 2022 eine auffällige Entwicklung bei der Zahl der Attacken festzustellen?

    Klein- und Mittelständische Unternehmen – sogenannte KMU – zählen gemäß bundesweiter Statistiken zu den Hauptbetroffenen von Cyberangriffen. Eine entsprechende Datenlage, welche dezidierte Rückschlüsse in Bezug auf die Betroffenheit von KMU zulässt, wird durch die Sicherheitsbehörden im Land Bremen nicht erfasst.

17. Inwieweit bieten die zuständigen Behörden Bremer Unternehmen Beratungsgespräche an und für welche Zielgruppen, in welcher Häufigkeit, durch wen und in welcher Intensität wurden diese Beratungsgespräche seit 2019 jeweils angenommen? Welche Hilfestellung wird gerade für kleinere und mittlere Unternehmen im Rahmen der Prävention von Cyberattacken angeboten? Welche spezifischen Hilfestellungen für kleinere und mittlere Unternehmen gibt es, wenn diese bereits Opfer einer Cyberattacke geworden sind?

    Die Polizei Bremen bietet im Rahmen von Awareness-Maßnahmen Wirtschaftsverbänden, Institutionen oder sonstigen Bereichen eine Begleitung im Rahmen von Vorträgen an. Durch die Ortspolizeibehörde Bremerhaven werden ebenfalls Beratungsgespräche für Firmen und Privatpersonen durchgeführt. In Bremerhaven nehmen Privatpersonen dieses Angebot wenige Male wöchentlich wahr. Firmen nehmen das Angebot aufgrund eigener IT-Fachabteilungen beziehungsweise -Spezialisten seltener war. Daher sind hier keine Präventionsangebote vorgesehen. Im Fall einer vorliegenden Cyberattacke wird über das Landeskriminalamt Bremen Hilfe angeboten.

    Weitere Hilfestellungen oder Betreuungen durch die Polizei Bremen, die Ortspolizeibehörde Bremerhaven und das Landeskriminalamt für Klein- und Mittelständische Unternehmen oder andere Betroffene nach einem Angriff erfolgen nur in Einzelfällen, da sich die Zuständigkeit und damit verbunden auch die Ausrichtung der Polizeien auf strafrechtliche Ermittlungen und die Erforschung eines Sachverhaltes konzentriert. Eine weiterführende Begleitung im Sinne des Wiederaufbaus einer IT-Infrastruktur obliegt der zuständigen IT-Abteilung des Unternehmens oder externen IT-Dienstleistern.

    Der perspektivische Ausbau eines entsprechenden Beratungsangebotes wird im Rahmen des Projektes Cybersicherheit bewertet.

18. Welche Zuständigkeiten hat das K13 Cybercrime/Digitale Spuren bei der Kriminalpolizei Bremen? Welche Zuständigkeiten fallen hier insbesondere dem K134 Cybercrime zu, und mit welchen Stellen kooperieren sie?

Das Referat K13 Cybercrime/Digitale Spuren der Direktion Kriminalpolizei/Landeskriminalamt der Polizei Bremen besteht aus vier Abschnitten, die sich in die Aufgabenbereiche

K131 – Digitale Forensik,

K132 – Telekommunikationsüberwachung,

K133 – Zentralstelle Video,

K134 – Cybercrime-Ermittlungen, OSINT/SOCMINT

aufteilen.

Die Polizei Bremen nimmt in der Rolle als Landeskriminalamt jene (LKA-) Aufgaben wahr, welche kraft originärer Zuweisung oder gemäß ermittlungsbegleitender Auftragslage ebenfalls für die Ortspolizeibehörde Bremerhaven übernommen werden. Das Referat K13 der Polizei Bremen – in der Rolle als Landeskriminalamt - unterstützt die Ortspolizeibehörde Bremerhaven unter anderem in Bereichen der

— Digitalen Forensik, mit speziellen Hard-/Softwareprodukten (unter anderem dem Auslesen von IOS-Systemen),

— Zentralstelle Video, mit der Anwendung Hinweisportal/SIDAN in Großschadenslagen und

— Cybercrime-Ermittlungen, mit der Recherche von kryptierten Währungen.

Der Bereich Automotive-IT befindet sich zurzeit im Aufbau und ist aktuell im Abschnitt K132 verortet. Hierzu gehört ebenfalls die Landesansprechstelle ermittelnde Automotive-IT (eAIT), welche administrativ eine zentrale Landeskriminalamt-Aufgabe darstellt. Die Entwicklung von Fähigkeiten der Datensicherung beziehungsweise Aufbereitung/Auswertung selbiger obliegt individuell den jeweiligen Behörden.

In den Abschnitt K134 Cybercrime fallen die folgenden Zuständigkeiten:

— Warenkreditbetrug zum Nachteil von Telekommunikationsdiensten, SIM-Swap-Verfahren, Geldwäscheverfahren mit Bezug SIM-Swap, Microsoft-Support-Betrugsverfahren: keine Verfahren Cybercrime im engeren Sinne;

— Cybercrime-Ermittlungen (Cybercrime im engeren Sinn – §§ 202ad, 303ab Strafgesetzbuch);

— Kriminaltechnische Unterstützungen der Ermittlungsreferate der Polizei Bremen in unterschiedlichsten technischen Themen (unter anderem Mail-Header-Analyse, IP-/DNS-Recherche);

— Kriminaltechnische Unterstützungen der Ermittlungsreferate der Polizei Bremen in OSINT/SOCMINT (Open Source INTelligence/SOCial Media INTelligence) zur Nutzung quelloffener Internetdaten für Ermittlungsverfahren;

— Nicht technische Bildanalyse (Detektion von Orten oder besonderen Merkmalen durch spezielle Internet-Recherchemöglichkeiten);

— Ermittlungen mit Bezug sogenannter Kryptowährungen (keine Abschöpfung) mittels unterstützender Spezialsoftware.

Die aufgeführten Aufgabenstellungen des Abschnittes K134 werden im Anforderungsfalle ebenfalls für die Ortspolizeibehörde Bremerhaven als ermittlungsunterstützende/-begleitende Landeskriminalamt-Aufgabe wahrgenommen.

Verstetigte Kooperationen auf Grundlage von bundesweiten Kooperationsvereinbarungen existieren innerhalb des K13 nicht.

19. Wie viele Stellen sind derzeit bei beim K13 der Kriminalpolizei eingeplant und besetzt? Wie viele Stellen davon sind beim K134 fest tätig? Wie viele sind anlassbezogen oder sporadisch tätig, und wo werden diese gegebenenfalls abgezogen?

    Das Referat K13 ist im Geschäftsverteilungsplan der Polizei Bremen mit 43 Funktionsstellen ausgewiesen. Dabei wird ein SOLL-VZE (Vollzeitäquivalent) von 39 VZE (inklusive acht refinanzierter „Encrochat"-Stellen) verzeichnet.

    Von den 43 Funktionsstellen sind derzeit 29 Stellen mit Mitarbeitenden besetzt. Die aus dem zusätzlichen Personalkörper „Encrochat" stammenden Funktionsstellen befinden sich derzeit im Ausschreibungsprozess des Abschnittes K131-Digitale Forensik.

    Im Abschnitt K134-Cybercrime sind aktuell sieben Funktionsstellen eingerichtet. Davon sind fünf Vollzugsstellen dem Bereich Cybercrime-Ermittlungen zugeordnet. Zwei Funktionsstellen sind als Technische Angestellte für den Bereich OSINT/SOCMINT-Aufgabe ausgewiesen.

    Derzeit wird das K134 im Bereich der Betrugsverfahren durch den Einsatz einer weiteren Vollzugsbeamtin temporär unterstützt.

    Anlassbezogene oder sporadische Aufgabenwahrnehmungen durch Mitarbeitende anderer Referate sind aufgrund der erforderlichen Fachkenntnisse und der Spezialausbildung regelmäßig nicht möglich.

20. Welche Aus- und Fortbildungsmöglichkeiten werden Polizeivollzugsbeamtinnen und -beamten angeboten, um die Aufgaben im Rahmen ihres Einsatzes gegen Cybercrime entsprechend wahrzunehmen?

    Die polizeiliche Ausbildung im Lande Bremen findet im Rahmen des sechssemestrigen dualen Bachelorstudiums „Polizeivollzugsdienst" (Bachelor of Arts) an der Hochschule für Öffentliche Verwaltung Bremen statt, der sich durch seine Interdisziplinarität und ausgeprägte Theorie-Praxis-Verbindung auszeichnet.

    Die Studierenden werden bereits frühzeitig mit Erscheinungsformen von Cybercrime vertraut gemacht.

    So werden in den grundständigen Modulen zu spezifischen Erscheinungsformen der Kriminalität durchgängig auch die Phänomenologie, Deliktstruktur und polizeilichen Handlungsansätze jener Tatbegehungskonstellationen adressiert, bei denen das Internet als Tatmittel eine prominente Rolle spielt beziehungsweise eigenständige Deliktsformen generiert hat. So werden beispielsweise im Modul I. Kriminalitätsbekämpfung: Gewaltdelikte (3. Semester) und Modul N. Kriminalitätsbekämpfung: Tötungsdelikte und sexuelle Gewaltdelikte (5. Semester) phänomenbezogen auch digitale Ausprägungsformen der Gewalt- und Tötungskriminalität adressiert (zum Beispiel Hate Speech im Internet, Cybergrooming zur gezielten Kontaktaufnahme mit Kindern und Jugendlichen im Kontext sexualisierter Gewalt, Cyber-Stalking).

    Zusätzlich über diese rein phänomenologische Betrachtungsweise hinausgehend erhalten die Studierenden im Rahmen des Moduls R „Digitale Spuren und Datenschutz" (6. Semester) einen Überblick über aktuelle Kriminalitätsphänomene im Kontext von Cybercrime einschließlich der kriminalistischen, taktischen und rechtlichen Besonderheiten. Konkret werden unter anderem die Themen Identitätsdiebstahl, Phishing, Warenkreditbetrug, Ransomware und das Manipulieren von Webseiten ebenso angesprochen wie die Bedeutung des Cybercrime in den unterschiedlichen Phänomenbereichen. Ergänzend werden Kenntnisse im Datenschutzrecht wiederholt und vertieft. Das Modul findet im 6. Semester statt und umfasst 3 SWS beziehungsweise 45 Lehrveranstaltungsstunden.

Im Rahmen der polizeilichen Fortbildung wird das Thema „Cybercrime“ bereits seit vielen Jahren in unterschiedlichen didaktischen Formaten adressiert, wobei die didaktischen Formate sukzessive ausdifferenziert und mit Blick auf unterschiedliche Zielgruppen weiterentwickelt wurden.

Regelmäßig wird zudem für Mitarbeitende der Polizei im Lande Bremen, die im Rahmen der operativen beziehungsweise weiterführenden Ermittlungen Bezug zum Internet haben, das Fortbildungsseminar „Internet – Ermittlungsmöglichkeiten“ angeboten, das anhand konkreter Praxisfälle aktuelle Kriminalitätsphänomene und das Spektrum geeigneter (auch) digitaler Ermittlungs-, Analyse- und Sicherungsmaßnahmen vorstellt und vertieft. Zudem ist das Thema Cybercrime in den Seminaren Qualifizierung zum/zur Polizeilichen Ermittler:in seit dem Jahr 2010 als Pflichtveranstaltung im Umfang von jeweils acht Lehrveranstaltungsstunden curricular verankert.

21. Ist es mittlerweile, wie 2019 angekündigt, zur Einstellung „ergänzender Fachkräfte außerhalb der Laufbahn des Polizeivollzugsdienstes“ im Bereich Cybercrime bei der Polizei Bremen gekommen, und wenn ja, welche Qualifikationen bringen diese Fachkräfte mit, und wo haben sie diese erworben?

    Seit Anfang des Jahres 2022 sind im K134 Cybercrime zwei technische Angestellte für die spezialisierte Internetrecherche tätig. Die Mitarbeiter:innen verfügen über eine IT-Ausbildung beziehungsweise ein IT-Studium und werden durch spezielle polizeiinterne und externe Fortbildungen für die Aufgabe kontinuierlich spezialisiert. Die Mitarbeiter:innen arbeiten auftragsbasiert für alle ermittelnden Dienststellen der Polizei Bremen.

22. Wie viele Stellen sind bei der Kriminalpolizei der Ortspolizeibehörde Bremerhaven für den Kampf gegen Cybercrime geplant und wie viele davon sind besetzt?

    Im zuständigen Fachkommissariat (Betrug & Internetkriminalität) der Ortspolizeibehörde Bremerhaven werden derzeit sechs Sachbearbeiter:innen eingesetzt, die interdisziplinär das gesamte Phänomenfeld bearbeiten. 0,5 VZE sind derzeit nicht besetzt. Im Bedarfsfall kann weitere Fachkompetenz bei der „Technischen Einsatzunterstützung“ angefordert werden.

23. Wie viel Ermittlungsverfahren hat es aufgrund welcher Delikte im Bereich Cyberkriminalität seit 2019 bei der Staatsanwaltschaft zusätzlich gegeben? (Sofern die Verfahren abgeschlossen sind, bitten wir zusätzlich um Mitteilung des Ausgangs der jeweiligen Verfahren.)

    In dem Zeitraum von Januar 2019 bis (einschließlich) August 2022 wurden bei der Staatsanwaltschaft Bremen im Bereich der Computerkriminalität 187 Ermittlungsverfahren gegen insgesamt 199 Beschuldigte geführt, davon

    — 79 wegen Computerbetruges (§ 263a Strafgesetzbuch) und Betruges (§ 263 Strafgesetzbuch),

    — vier wegen sonstiger Wirtschaftsstrafsachen,

    — zwei wegen Geldwäsche (§ 261 Strafgesetzbuch),

    — vier wegen Vergehen/Verbrechen nach dem Betäubungsmittelgesetz,

    — 97 wegen des Verdachts verschiedener Taten, unter anderem

        — wegen (versuchter) Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks (§ 152b Strafgesetzbuch)

        — wegen (versuchten) Ausspähens von Daten (§ 202a Strafgesetzbuch)

— wegen (versuchten) Abfangens von Daten (§ 202c Strafgesetzbuch)

— wegen (versuchter) Datenhehlerei (§ 202d Strafgesetzbuch)

— wegen (versuchter) Fälschung beweiserheblicher Daten (§ 269 Strafgesetzbuch)

— wegen (versuchter) Datenveränderung (§ 303a Strafgesetzbuch),

— wegen (versuchter) Computersabotage (§ 303b Strafgesetzbuch).

Durch die Staatsanwaltschaft Bremen wurden für die einzelnen Deliktsarten folgende – seitens des IT-Fachverfahrens ausgewiesene – Erledigungsarten mitgeteilt:

Computerbetrug, § 263a Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 4 |
| Verbindung mit einem anderen Verfahren | 18 |
| Anklagen | 0 |
| Einstellungen,<br>davon gemäß: | 14 |
| § 170 Absatz 2 StPO | 6 |
| § 153 Absatz 1 StPO | 1 |
| § 153a Absatz 1 StPO | 1 |
| § 154 Absatz 1 StPO | 6 |
| § 154 f StPO | 0 |

Betrug, § 263 Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 1 |
| Verbindung mit einem anderen Verfahren | 31 |
| Anklagen | 1 |
| Einstellungen<br>davon gemäß: | 10 |
| § 170 Absatz 2 StPO | 5 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 4 |
| § 154 f StPO | 1 |

Ausspähen von Daten, § 202a Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 4 |
| Anklagen | 0 |
| Einstellungen<br>davon gemäß: | 8 |
| § 170 Absatz 2 StPO | 5 |
| § 153 Absatz 1 StPO | 1 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 1 |
| § 45 JGG | 1 |

Datenhehlerei, § 202d Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 0 |
| Anklagen | 1 |
| Einstellungen<br>davon gemäß: | 5 |
| § 170 Absatz 2 StPO | 0 |
| § 153 Absatz 1 StPO | 2 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 3 |

Nötigung, Erpressung, §§ 240, 253 Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 57 |
| Anklagen | 0 |
| Einstellungen<br>davon gemäß: | 4 |
| § 170 Absatz 2 StPO | 4 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 0 |

Computersabotage, Datenveränderung, §§ 303a, 303b Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 0 |
| Abgabe an andere Staatsanwaltschaft | 3 |
| Anklagen | 1 |
| Einstellungen<br>davon gemäß: | 0 |
| § 170 Absatz 2 StPO | 0 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 0 |

Urkundenfälschung, Fälschung beweiserheblicher Daten, §§ 267, 269 Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 7 |
| Anklagen | 0 |
| Einstellungen<br>davon gemäß: | 3 |
| § 170 Absatz 2 StPO | 3 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 0 |

Geldwäsche, § 261 Strafgesetzbuch:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 0 |
| Verbindung mit einem anderen Verfahren | 0 |
| Anklagen | 0 |
| Einstellungen<br>davon gemäß: | 4 |
| § 170 Absatz 2 StPO | 2 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 0 |
| § 154 Absatz 1 StPO | 2 |

Sonstige Delikte:

| Erledigungsart: | Anzahl Beschuldigte: |
|---|---|
| Verfahren noch anhängig | 4 |
| Verbindung mit einem anderen Verfahren | 2 |
| Anklagen | 0 |
| Einstellungen<br>davon gemäß: | 3 |
| § 170 Absatz 2 StPO | 2 |
| § 153 Absatz 1 StPO | 0 |
| § 153a Absatz 1 StPO | 1 |
| § 154 Absatz 1 StPO | 0 |

Im gleichen Zeitraum wurden bei der Staatsanwaltschaft Bremen im Bereich der Cyberkriminalität außerdem 52 Ermittlungsverfahren gegen (zunächst) unbekannte Täter geführt, davon

— vier wegen (versuchten) Betruges,

— 19 wegen (versuchten) Computerbetruges,

— elf wegen (versuchter) Computersabotage,

— sechs wegen (versuchten) Ausspähens von Daten,

— zwei wegen (versuchter) Fälschung beweiserheblicher Daten,

— vier wegen (versuchter) Erpressung,

— zwei wegen (versuchter) Datenveränderung,

— zwei wegen (versuchter) Urkundenfälschung,

— eines wegen (versuchter) Sachbeschädigung und

— eines wegen (versuchten) Abfangens von Daten.

Durch die Staatsanwaltschaft Bremen wurden insoweit folgende – seitens des IT-Fachverfahrens ausgewiesene – Erledigungsarten mitgeteilt:

| Erledigungsart: | Anzahl Verfahren: |
|---|---|
| | |
| Verfahren noch anhängig | 3 |
| Verbindung mit einem anderen Verfahren | 5 |
| Abgaben an andere Staatsanwaltschaft | 2 |
| Umtragungen in das Js-Register nach Beschuldigtenermittlung | 20 |
| Einstellungen gemäß § 170 Absatz 2 StPO | 20 |

24. Inwiefern sind von bremischen Behörden, bremischen Unternehmen und/oder der Firma Dataport in den vergangenen fünf Jahren „Lösegelder“ in Form von Kryptowährungen an Hacker gezahlt worden? (Bitte soweit bekannt die Höhe der Forderung in Euro und Art der Kryptowährung angeben)

    Dem Senat sind keine Zahlungen von „Lösegeldern“ in Form von Kryptowährungen an Hacker in seinem Geschäftsbereich bekannt geworden. Auch die AöR Dataport hat keine „Lösegelder“ bezahlt.

25. Wie interpretiert der Senat vor dem Hintergrund der seitens der Bundesinnenministerin avisierten Gesetzesänderung die Aussage, dass „Sicherheit nicht auf Kosten des Datenschutzes geopfert“ werden dürfe? Wo sind die Grenzen, wo ist Handlungsbedarf, und wie ist die Haltung des Senats im Spannungsfeld zwischen Sicherheit und Datenschutz?

    Nach Einschätzung des Senats stehen die Begriffe Cybersicherheit und Datenschutz nicht in sich ausschließender Konkurrenz. Die IT-Sicherheit könnte von strengen datenschutzrechtlichen Anforderungen vielmehr profitieren, da Unternehmen aufgrund drohender datenschutzbezogener Sanktionsmöglichkeiten die unternehmensinterne Cybersicherheit und IT-Infrastruktur gezwungenermaßen anpassen und optimieren. Diese Optimierungen bedingen eine Stärkung der Unternehmenssicherheit und fördern somit den Schutz von Unternehmen vor Cyberangriffen.

26. Wie viele Datenlecks personenbezogener Daten von welchem Ausmaß bei öffentlichen/nicht öffentlichen Stellen hat es im vergangenen Jahr in Bremen gegeben, die der Landesdatenschutzbeauftragten bekannt wurden? Was waren die Gründe hierfür, soweit bekannt?

    Von den 196 im Jahr 2021 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldeten Datenschutzverletzungen können 45 Meldungen (41 aus dem nicht öffentlichen und vier aus dem öffentlichen Bereich) im weitesten Sinne der Cyberkriminalität zugerechnet werden. Diese Meldungen sind insbesondere auf Hackerangriffe (30), das Aufspielen von Schadsoftware und Phishing-Attacken (zusammen zehn) zurückzuführen. Ein Hackerangriff (Hafnium) auf einen Auftragsverarbeiter bewirkte allein 21 Meldungen.

    Die 196 gemeldeten Datenschutzverletzungen verteilten sich im Übrigen wie folgt (nähere Angaben jeweils unter dem jeweiligen ersten Unterpunkt zum entsprechenden Bereich im 4. Jahresbericht nach der Datenschutzgrundverordnung):

    — Inneres: sieben (davon zwei Meldungen von Bürger- und Ordnungsämtern, vier Meldungen der Polizeien Bremen und Bremerhaven),

    — Justiz: zehn Meldungen von Rechtsanwält:innen und Notar:innen,

    — Gesundheit: 39 Meldungen,

    — Soziales: acht Meldungen,

    — Beschäftigtendatenschutz: 33 Meldungen,

    — Wirtschaft/Gewerbe: 31 Meldungen,

    — Kreditwirtschaft: neun Meldungen,

    — Bauen/Wohnen/Verkehr/Umwelt: 29 Meldungen,

    — Telemedien: 29 Meldungen,

    — Vereine: eine Meldung.

    Der überwiegende Teil der gemeldeten Datenschutzverletzungen bezieht sich auf Konstellationen, in denen Dritte ohne Rechtsgrund personenbezogene Daten zur Kenntnis nehmen können beziehungsweise dies bereits

geschehen ist und insofern von einem „Datenleck“ gesprochen werden kann. Die genaue Zahl wird derzeit nicht gesondert erhoben.