BREMISCHE BÜRGERSCHAFT
Landtag
19. Wahlperiode

Drs. 19/1993
(zu Drs. 19/1932)
15.01.19

Mitteilung des Senats
an die Bremische Bürgerschaft (Landtag)
vom 15. Januar 2019

„Cybersicherheit in Bremen“

Die Fraktion der FDP hat die im beiliegenden Entwurf der Mitteilung des Senats an die Bürgerschaft zitierte Große Anfrage an den Senat gerichtet:

„Die Sicherheit der Datenverarbeitung ist für Privatpersonen, Firmen sowie öffentliche Einrichtungen ein relevanter Teil gesellschaftlicher Sicherheit geworden. Laut einer repräsentativen Studie im Auftrag des Digitalverbandes „Bitkom“ ist jeder zweite deutsche Internetnutzer innerhalb eines Jahres Opfer von Cybercrime, also im weitesten Sinne Internetkriminalität, geworden. Am Häufigsten kam es dabei zur Infektion mit Schadprogrammen und zum Diebstahl von Zugangsdaten für Online-Dienste und Online-Shops. Cybercrime kann für den Einzelnen dramatische Folgen haben. Dabei spielt vor allem der Verlust von Geld und persönlichen Daten, Privatsphäre und Integrität eine Rolle. Jedes zweite Opfer von Cybercrime gibt an, dass ein finanzieller Schaden, beispielsweise durch das Hinzuziehen eines Reparaturdienstes, den Kauf von Soft- oder Hardware sowie nicht erhaltender Waren, entstanden ist. Laut der Bitkom-Studie erstattet aber nur jeder sechste Betroffene Anzeige gegen den oder die Betrüger. Das Bundeskriminalamt geht in seinem Bundeslagebild Cybercrime für das Jahr 2017 von Schäden in Höhe von mindestens 71,4 Mio. Euro im Bereich Computerbetrug aus. Das entspricht einer Steigerung gegenüber dem Vorjahr von fast 40 Prozent. Kaum vertreten in dieser Statistik sind Schäden von Firmen, denen bei Eindringen in ihre IT-Infrastruktur nicht selten wertvolles Wissen oder Kundendaten gestohlen werden. Schätzungen gehen davon aus, dass Unternehmen in Deutschland 55 Milliarden Euro für die Folgen der Angriffe durch Cybercrime ausgegeben haben.

Besonders wichtig ist die Sicherheit vor Cyberkriminalität bei kritischer Infrastruktur und öffentlichen Einrichtungen. In Erinnerung bleibt die Infizierung von 450 Rechnern bei der Deutschen Bahn, die 2017 zu tagelangen Ausfällen bei Anzeigetafeln und Ticketautomaten geführt hat. Bei öffentlichen Einrichtungen steht ganz besonders die Sicherheit der ihnen zugetragenen Daten und die Funktionsfähigkeit der Verwaltung im Mittelpunkt. Im Sinne der Cyber-Sicherheitsstrategie für Deutschland des Bundesinnenministeriums ist Cybersicherheit ein anzustrebender Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyberraums auf ein tragbares Maß reduziert sind. Dem Bremer Senat obliegt eine besondere Verantwortung zum Schutz der IT-Infrastruktur. Gezielte Cyberangriffe können auf Bremer Unternehmen, auf Versorgungsunternehmen, auf die Hafenwirtschaft, auf die Sicherheitsbehörden, auf die gesamte öffentliche Verwaltung inklusive Justiz und Gesundheitswesen und auf Privatpersonen abzielen. Solche Angriffe haben potenziell eine katastrophale Auswirkung.

Dennoch arbeitet die Bremer Verwaltung immer noch mit anfälligen Closed-Source-Betriebssystemen und proprietären Büroanwendungen vornehmlich auf Microsoft-Basis. Sie ignoriert dabei Sicherheitsbedenken und die massiven Warnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), verstößt dabei mutmaßlich gegen europäisches Wettbewerbs- und Vergaberecht und macht sich abhängig von einem amerikanischen Konzern mit nachgewiesenen Spionage-Hintertüren für den Geheimdienst NSA, die auch gerne von Cyber-Kriminellen ausgenutzt werden.

Vor diesem Hintergrund fragen wir den Senat:

1. Wie viele Cyberangriffe hat es jeweils in den vergangenen fünf Jahren auf die bremische Verwaltung, auf bremische Unternehmen sowie auf kritische Infrastruktur in Bremen gegeben?

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

   b) Welche Schäden haben diese Angriffe jeweils verursacht?

   c) Wie hoch waren die Kosten zur Behebung der Schäden durch den jeweiligen Angriff?

   d) Welche Dauer haben diese Angriffe jeweils verzeichnet?

   e) Welche Störung wurde jeweils durch den Angriff verursacht?
2. Wie hoch schätzt der Senat das Risiko von Cyberangriffen auf die öffentliche Verwaltung bzw. auf die kritische Infrastruktur in Bremen ein, die zu erheblichen Folgen (beispielsweise Ausfall des Stromnetzes oder Ausfall des öffentlichen Nahverkehrs) führen kann?
3. Inwieweit gibt es bei den zuständigen Behörden ein „Worst-Case-Szenario“ für einen Cyberangriff? Wenn ja, wie zeichnet sich dieses aus und liegen entsprechende Abwehrpläne beziehungsweise Einsatzpläne vor? Wenn nein, warum nicht?
4. Inwieweit arbeitet der Senat mit externen Hackern zusammen, die regelmäßig Angriffe („friendly attacks“) auf die Bremer Verwaltung ausüben, um Sicherheitslücken aufzudecken? Wenn ja, wie oft? Wenn nein, plant er dieses?
5. Welche Behörden und Ämter befassen sich mit jeweils wie vielen Stellen mit dem Thema Cybersicherheit und inwieweit wird dabei zwischen Cyberangriffen, Cyberspionage und Cyberkriminalität unterschieden?
6. Welche Qualifikationen haben die Mitarbeiter, die sich in den Behörden und Ämtern mit dem Thema Cybersicherheit beschäftigen und können alle Planstellen mit Fachkräften besetzt werden?
7. Inwieweit sind die bremischen Institutionen nach Ansicht des Senats im Bereich der Cyberkriminalität ausreichend gut aufgestellt und wo sieht der Senat aus welchem Grund welchen Nachholbedarf?
8. Inwiefern hat der Senat beziehungsweise haben welche zuständigen Behörden ein Konzept bezüglich einer sicheren Kommunikation der Behörden und Organisationen mit Sicherheitsaufgaben, welches vor Cyberangriffen geschützt ist?

9. Welche Aufgabe nimmt das Unternehmen Dataport im Bereich der Cybersicherheit wahr und wie gestaltet sich die Zusammenarbeit mit den Behörden und Ämtern?
10. Inwieweit kooperiert Bremen bei dem Thema Cybersicherheit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder mit den zuständigen Behörden anderer Bundesländer?
11. Inwieweit ist Bremen durch welche Institute oder Dienststellen im Bereich der Forschung und Entwicklung zum Schutz vor Cyberangriffen mit welchem Aufwand (Personal und Kosten) tätig beziehungsweise beteiligt?
12. Welche Präventionsmaßnahmen mit der Prävention zum Schutz vor Cyberangriffen nimmt der Senat beziehungsweise die zuständige Behörde vor, insbesondere bei den
    - Sicherheitsbehörden,
    - Dienststellen der öffentlichen Verwaltung,
    - den öffentlichen Versorgungsunternehmen,
    - den öffentlichen Verkehrsunternehmen,
    - der in Bremen angesiedelten Industrie und Wirtschaft sowie
    - den Hochschulen und Forschungsinstituten in Bremen?
13. Inwieweit bieten die zuständigen Behörden Beratungsgespräche für welche Zielgruppen an und in welcher Häufigkeit und von wem bzw. wie wurden diese Beratungsgespräche jeweils in den vergangenen fünf Jahren angenommen?
14. Inwieweit arbeitet der Senat beim Thema Cybersicherheit insbesondere mit kleinsten, kleinen und mittleren Unternehmen zusammen, die häufig nicht über die Ressourcen verfügen, eigene IT-Sicherheitsprogramme aufzulegen?
15. Wie viele Betroffene von Straftaten im Bereich der Cyberkriminalität erstatten jährlich bei der Bremer Polizei Anzeige und welche Schadenssummen werden dabei ermittelt?
16. Welche Erklärungen hat der Senat dafür, dass nur etwa jeder sechste Betroffene Anzeige erstattet und welche Aufklärungsmaßnahmen hält er insoweit für erforderlich?
17. Inwieweit hat der Senat Informationen darüber, ob und in welchem Umfang Geschädigte auf zivilrechtlichem Weg Ersatz der ihnen zugefügten Schäden erhalten (haben)?
18. Wie ist die Polizei Bremen sachlich und personell bei den Ermittlungen zu Cyberkriminalität aufgestellt und hält der Senat hier aufgrund des offensichtlichen Anstiegs der kriminellen Aktivitäten eine Aufstockung der Mittel für notwendig?
19. Wieviel Ermittlungsverfahren hat es im Bereich Cyberkriminalität in den letzten fünf Jahren jeweils bei der Staatsanwaltschaft mit welchem Ausgang gegeben?
20. Wie wird das Personal zur Bearbeitung von Cyberkriminalität bei der Polizei und der Staatsanwaltschaft ausgebildet?

21. Wie häufig hat man sich in den vergangenen fünf Jahren für die sachgerechte Ermittlungsarbeit externer Sachverständiger bedient, welche Kosten sind dabei jeweils entstanden und wird dies gegebenenfalls zukünftig (weiter) für notwendig erachtet?
22. Wie stellt sich die Bearbeitungssituation (bezogen auf Anzahl der Verfahren, die durchschnittliche Bearbeitungsdauer und die Rückstände) bei der KTU für Ermittlungsverfahren im Zusammenhang mit IT-Sicherheit dar?“

Der Senat beantwortet die Große Anfrage wie folgt:

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein“ (so die Definition des BSI auf seiner Homepage). Die Komplexität dieses Themas kann angesichts der Vernetzung der FHB mit vielen regionalen Akteuren einerseits im Rahmen einer Großen parlamentarischen Anfrage kaum hinreichend abgebildet werden. Andererseits verlangt sie nach einer Eingrenzung und Strukturierung in der Beantwortung. Es ist zwischen Störungen im IT Betrieb, ungerichteten Angriffen (die die FHB nur zufällig treffen) und zielgerichteten Angriffen auf die FHB zu unterscheiden, wobei eine klare Abgrenzung nur sehr eingeschränkt möglich ist. In diesem Sinne wird der Begriff „Informationssicherheit“ in der FHB einen wesentlichen Teil der Cybersicherheit abbilden. Bei der Informationssicherheit geht es darum, die IT insgesamt gegen alle Arten von Beeinträchtigungen zu schützen. So würden Stromausfälle oder Naturkatastrophen auf den ersten Blick die Informationssicherheit berühren, sie würden jedoch nicht als Beeinträchtigungen der Cybersicherheit gewertet werden, sondern als „normales“ Betriebsrisiko.

Informationssicherheit ist somit eine Voraussetzung für Cybersicherheit. Intransparente IT Infrastrukturen, unklare Meldewege bei Störungen und Nutzerinnen und Nutzer, die sich ihrer Verantwortung für die Informationssicherheit nicht bewusst sind, stellen ein nicht kalkulierbares Risiko dar. Dies gilt sowohl für die Verwaltung als auch für andere kritische Infrastrukturen. In diesem Grundverständnis beantwortet der Senat die nachfolgenden Fragen. In den Antworten sind auch die Angaben aus Bremerhaven enthalten.

1. Wie viele Cyberangriffe hat es jeweils in den vergangenen fünf Jahren auf die bremische Verwaltung, auf bremische Unternehmen sowie auf kritische Infrastruktur in Bremen gegeben?

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

b) Welche Schäden haben diese Angriffe jeweils verursacht?

c) Wie hoch waren die Kosten zur Behebung der Schäden durch den jeweiligen Angriff?

d) Welche Dauer haben diese Angriffe jeweils verzeichnet?

e) Welche Störung wurde jeweils durch den Angriff verursacht?

a) Für die Verwaltung gilt: Gerichtete Angriffe, die Bremen getroffen haben und treffen sollten, wurden in den letzten fünf Jahren mit einer Ausnahme (s.u.) nicht beobachtet. Ungerichtete Angriffe waren dagegen sehr zahlreich, sie wurden vor allem im SPAM-Schutz, im zentralen Virenschutz und im Firewallmanagement beobachtet.

b) und c) Bei den Auswirkungen und Schäden können zunächst betriebliche Aufwände bei Dataport (bzw. Unterauftragnehmern) ermittelt werden, die der Abwehr dienten. Diese Aufwände sind im Rahmen der bestehenden Aufträge abgegolten. Hinzu kam in vielen Fällen ein Arbeitsausfall beim Anwenderinnen und Anwendern in der Verwaltung. Hierüber liegen keine zentralen Daten vor. Gleiches gilt auch für evtl. immaterielle Auswirkungen (Reputationsschäden etc.). Grob geschätzt werden durch Dataport 1800h/Jahr für Bremen zur Schadensbehebung aufgewandt (gemittelter Aufwand über die gesamte betreute Infrastruktur). Einzelfallbezogen kann es Schwankungen nach oben und unten geben.

Prognostisch werden die Kosten steigen, da die Vorfälle häufiger und deren Behandlung komplizierter und langwieriger werden. Die aktuelle Spam-Welle ist ein gutes Beispiel dafür.

d) und e) Ergänzend gab es 12242 Schadsoftwarebereinigungen für die im zentralen Mail System CCMS bei Dataport angeschlossenen Ressorts in den letzten 30 Tagen.

Für die netznahen Dienste der bremischen Verwaltung erfolgte für die vergangenen Jahre eine Abschätzung der internen Aufwände anhand von Dataport gelieferter verdichteter Daten. Angaben dazu enthält die Tabelle im Anhang, die auch präventive Aufwände, Fälle der Datenherausgabe und der Unterstützung polizeilicher Ermittlungen beinhaltet.

Für den täglichen Kampf gegen Spam gibt es Durchschnittswerte für ein Jahr, die einen Eindruck vermitteln. Konkrete Zahlen auf Jahresbasis werden nicht erhoben, die folgenden Zahlen für das vergangene Jahr sind daher aus täglichen Durchschnittswerten abgeleitet:

Ca. 35 Millionen E-Mails wurden durch Grey-Listing (siehe https://de.wikipedia.org/wiki/Greylisting) behandelt.

Ca. 6,5 Millionen E-Mails wurden als SPAM erkannt.

Es gab mindestens einen Angriff auf die bremische Verwaltung, bei welchem eine technische Manipulation zum Nachteil einer Subdomain der URL „bremen.de“ ausgeübt wurde. Es entstand kein Schaden für die bremische Verwaltung. Es gibt zudem kontinuierliche Angriffe auf bremische Unternehmen, diese sind mangels Unterscheidungsmerkmalen im polizeilichen Vorgangsbearbeitungssystem jedoch nicht auswertbar. Für die kritische Infrastruktur liegt keine Anzeige im Sinne des IT-Sicherheitsgesetzes vor.

2. Wie hoch schätzt der Senat das Risiko von Cyberangriffen auf die öffentliche Verwaltung bzw. auf die kritische Infrastruktur in Bremen ein, die zu erheblichen Folgen (beispielsweise Ausfall des Stromnetzes oder Ausfall des öffentlichen Nahverkehrs) führen kann?

Der Senat schätzt das Risiko für gezielte und ungezielte Cyberangriffe auf die Öffentliche Verwaltung mit „mittlerer“ Eintrittswahrscheinlichkeit ein. Maßnahmen, welche dieses Risiko minimieren sind an geeigneten Stellen des Bremer Landesnetzes getroffen worden.

Kritische Infrastrukturen in Bremen werden vom IT-Sicherheitsgesetz erfasst, sobald sie durch Rechtsverordnungen des Bundes (BSI-KritisV) bestimmte Schwellenwerte überschreiten. Der Schwellenwert legt fest, ab wann eine Anlage oder Teile davon als bedeutend für die Daseinsvorsorge einzuordnen sind.

Derzeit sind in Bremen 13 Unternehmen und Einrichtungen vom IT-Sicherheitsgesetz betroffen. Die Betreiber dieser kritischen Infrastrukturen werden durch dieses Gesetz verpflichtet, standardisierte und branchenspezifische Maßnahmen oder branchenspezifische Sicherheitsstandards zur Reduktion von Cybersicherheitsrisiken anzuwenden. Die branchenspezifischen Sicherheitsstandards werden unter der Bezeichnung „B3S“ vom BSI abgenommen und veröffentlicht. Diese Maßnahmen werden von unabhängigen Auditoren überprüft. Das BSI behält sich vor, die Ergebnisse dieser Audits wiederum einer weiteren Überprüfung zu unterziehen.

In Bezug auf Energie- und Wasserversorgung sowie Logistik und Verkehr verweist der Senat auf die sektorspezifischen Vorgaben aufgrund des IT Sicherheitsgesetzes, die auch eine eigene Risikobewertung und -behandlung von den Betreibern verlangen.

Zu weiteren kritischen Infrastrukturen bei eigenen Beteiligungen zählt der Senat insbesondere das öffentliche Gesundheitswesen und den ÖPNV:

Die Gesundheit Nord ist an das Internet angebunden und nutzt dieses in vielfältigen Szenarien zur Erfüllung der Aufgaben der Gesundheitsversorgung. Insofern ist die Gesundheit Nord von den Risiken des Internets wie jedes andere mit dem Internet verbundene Unternehmen berührt. Dieses Risiko wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) quartalsweise bewertet. Für das 3. Quartal 2018 (mit Ausblick auf das 4. Quartal) wird das Risiko für Ransomware als gleichbleibend hoch, das Risiko von DDOS (Distributed Denial of Service) Angriffen (d.h. Angriffe auf Webdienste, so dass diese nicht mehr verfügbar sind), Malware und Identitätsdiebstahl als steigend eingeschätzt. Das Risiko der Gesundheit Nord von ungerichteten Cyberangriffen getroffen zu werden, wird von ihr als hoch eingeschätzt. Das Risiko von zielgerichteten Cyberangriffen getroffen zu werden, wird als niedrig eingeschätzt.

Gegen diese Risiken betreibt die Gesundheit Nord eine IT-Sicherheitsinfrastruktur. Die monatlich erfolgte Bewertung des Status der IT-Sicherheit der Gesundheit Nord durch einen IT-Sicherheitsdienstleister stuft

diese als gut bis sehr gut ein. Insofern wird das Risiko der Gesundheit Nord durch einen Cyberangriff einen erheblichen Schaden zu erleiden als eher gering eingeschätzt.

Die IT-technischen Schutz- und Vorsorge-Maßnahmen der BSAG zur Risiko-Minimierung von Cyberangriffen sind state-of-the-art und entsprechenden den Empfehlungen des BSI. Diese Schutzmaßnahmen werden durch sogenannte Penetrationstests auf ihre Wirksamkeit getestet.

Das Risiko eines kompletten Ausfalls des öffentlichen Nahverkehrs allein durch einen Cyberangriff ist als gering einzuschätzen, da selbst bei Ausfall zentraler IT-systeme ein Fahrbetrieb auf Basis entsprechender Rückfallebenen möglich ist.

In Bezug auf Cybersicherheit der Stromversorgung sind zwei Aspekte von besonderer Bedeutung:

1. Auswirkungen eines Stromausfalls auf die IT, insbesondere der kritischen Infrastrukturen: Ein Stromausfall ist ein Szenario, dass jedem Rechenzentrumsbetreiber bekannt ist. Dataport hat hierfür im Rechenzentrums-Betrieb die nötigen Vorkehrungen getroffen. Auch die Telekommunikationsinfrastruktur steht über einen überschaubaren Zeitraum durch entsprechende Systeme zur Herstellung einer unterbrechungsfreien Stromversorgung zur Verfügung. Auch dezentral betriebene Rechenzentren verfügen regelhaft über derartige Vorkehrungen. Unterbrechungsfreie Stromversorgungen müssen in diesem Kontext jedoch weiter betrachtet werden. Auf eine kurzzeitige Batterieabstützung erfolgt ein Notstromaggregat, dieses muss mit Kraftstoffen versorgt werden, welches u.a. die Verfügbarkeit der Verkehrsinfrastrukturen voraussetzt (Interdependenzen).

2. Risiken, dass die IT eines Stromversorgers angegriffen wird, um einen großflächigen und langanhaltenden Stromausfall auszulösen: Dies ist eine Situation, die explizit in den branchenspezifischen Regelungen des IT-Sicherheitsgesetzes und des Energiewirtschaftsgesetzes vorgesehen sind. Energieversorger haben hier entsprechende Verpflichtungen. Dazu gehört auch die Einschätzung des Risikos, in welchem Umfang der Versorger Ziel einer Cyberattacke werden kann. Zur Abmilderung dieser Cyberrisiken gehören Audits mit speziell für das BSI Gesetz geschulten Auditoren. Die Audits zur IT-Sicherheit bedeuten, dass sowohl die Prozesse des KRITIS-Unternehmens dokumentiert werden müssen, als auch, dass mindestens alle zwei Jahre entsprechende Audits, Prüfungen oder Zertifizierungen nachgewiesen werden müssen. In diesen Unternehmen sind die üblichen Mechanismen der Risikoüberwälzung auf Versicherungen und Akzeptanz des Risikos nur eingeschränkt zugelassen.

Aufgrund der immer weiterwachsenden Bedeutung der Digitalisierung und der damit einhergehenden Vernetzung kommt es zu einer stärkeren Abhängigkeit kritischer Infrastrukturen von IT- und Kommunikationssystemen.

Durch Interdependenzen (Abhängigkeiten zwischen einzelnen Sektoren oder Branchen) wird das Risiko von Ausfällen als Auswirkung von Angriffen noch

verstärkt. Diese Ausfälle in einem Sektor können zu Ausfällen in anderen Sektoren führen und auf diese Weise einen Dominoeffekt auslösen.

Der Senat geht davon aus, dass es künftig weiterer Anstrengungen, auch von Seiten der Unternehmen, bedarf, um die Auswirkungen eines möglichen Stromausfalls auf Bremen transparent zu machen und ihnen aktiv entgegenzusteuern.

Für die Krisenkommunikation der kritischen Infrastrukturen hat der Senat das bei Dataport angesiedelte Computer Emergency Response Team (CERT-Nord, vgl. Antwort zu Frage 9) beauftragt, als koordinierende Stelle zu wirken. Des Weiteren hat sich der Senator für Inneres als „Single Point of Contact“ (SPOC) -gemäß IT Sicherheitsgesetz- dem BSI gegenüber erklärt. Dies soll die Krisenkoordination im eigenem Zuständigkeitsbereich ermöglichen.

Für den Bereich des Senators für Inneres gibt es darüber hinaus differenzierte Einzelbetrachtungen:

Inneres	Das Risiko wird als gering eingestuft. Der weitaus größte Teil der PC-Arbeitsplätze sind BASIS-PCs (Support durch den Dienstleiter Dataport AöR).
Polizei Bremen	Das Risiko wird relativ gering eingestuft. Umfangreiche Sicherheitsmaßnahmen sind bereits umgesetzt: - Ein abgeschlossenes Netz. - Aufwändig abgesicherte Netzgrenzen. - Kein direkter Internetzugriff.
Ortspolizei-behörde Bremerhaven	Das Risiko von Cyberangriffen auf die öffentliche Verwaltung und auf kritische Infrastrukturen wird nur als latente Gefahr gesehen. Die Bewertung ergeht auf Grundlage der Informationen, die aus den Sachverhalten zu Frage 15 dargestellt sind.
Feuerwehr Bremen	Die kritischsten Systeme der Feuerwehr Bremen werden in der Feuerwehr- und Rettungsleitstelle genutzt. Hierzu zählen insbesondere die Funk- und Notrufabfrage und das Einsatzleitsystem. Nach Einschätzung der Feuerwehr besteht ein geringes bis mittleres Risiko mit einer geringen Wahrscheinlichkeit, aber hohen Gefahr für den Brand- und Hilfeleistungsdienst sowie den Rettungsdienst in der Stadt Bremen.
Ordnungsamt, Bürgeramt, Migrationsamt	Das Risiko wird gering eingestuft. Der weitaus größte Teil der PC-Arbeitsplätze sind BASIS-PCs (Support durch Dataport).

3. Inwieweit gibt es bei den zuständigen Behörden ein „Worst-Case-Szenario“ für einen Cyberangriff? Wenn ja, wie zeichnet sich dieses aus und liegen entsprechende Abwehrpläne beziehungsweise Einsatzpläne vor? Wenn nein, warum nicht?

Soweit eine bremische Behörde selbst zur kritischen Infrastruktur gehört, sind Maßnahmen auf Basis des Grundschutzes (BSI) für die Kontinuität des Geschäftsbetriebes durchzuführen. Einschlägig sind hier die Standards des Notfallmanagements.

Für die Kernverwaltung ist der IT-Betrieb weitestgehend an die Dataport AöR ausgelagert, es gelten Abwehrpläne und Prozesse bei Dataport. Darüber hinaus gibt es dort neben den Konzepten zur Datensicherung und Wiederherstellung keine Konzepte.

Bei der Polizei Bremen ist ein ISMS (Informationssicherheitsmanagement-system) etabliert, die Behandlung von Sicherheitsvorfällen ist geregelt. Zur Kontrolle finden länderübergreifende Audits / Revisionen statt.

Bei der Ortspolizeibehörde Bremerhaven liegt im Bereich der DV-Systemtechnik der Ortspolizeibehörde Bremerhaven zurzeit kein konkretes „Worst-Case-Szenario“ vor. Möglichen Ausfällen wird durch teilweise Redundanz, Backup und „cold-standby-Systemen“ begegnet.

Die Feuerwehr sieht derzeit kein spezielles Szenario für einen Cyberangriff vor. Allerdings ist sie auf vielfältige Ausfallszenarien vorbereitet und verfügt über einen jederzeit einsetzbaren Krisenstab.

Die Gesundheit Nord verfügt über ein Notfallkonzept und einen Alarmplan für die Informationstechnik. Dieses schließt Ausfallszenarien auf Grund von Cyberangriffen ein. Inhalt des Notfallkonzeptes sind u. a. ein Backupkonzept und Wiederanlaufpläne für die Systeme sowie Kommunikations- und Eskalationsprozesse. Für besonders aktuelle Cyberangriffe (z. B. Ransomware) bestehen spezifische Regelungen.

Die Gesundheit Nord setzt zudem besonders auf präventive Maßnahmen wie aktuelle IT-Sicherheitssysteme, eine IT-Sicherheitsorganisation und die Information der Beschäftigten der Gesundheit Nord über aktuelle IT-Sicherheitsbedrohungen.

Ein „worst-case“ Szenario für einen Cyberangriff aus ÖPNV-Sicht wäre der Totalausfall sämtlicher interner IT-und Kommunikationssysteme. Ein Fahrbetrieb der Straßenbahnen wäre unter diesen Bedingungen zu stoppen, während ein Bus-Fahrdienst auch ohne IT-Unterstützung eingeschränkt möglich wäre. Entsprechende vorsorgliche Abwehrmaßnahmen und Notfallpläne liegen vor.

Eine unmittelbare Gefahr für Menschenleben besteht nicht. Mögliche Auswirkungen wären vor allem monetärer Art.

4. Inwieweit arbeitet der Senat mit externen Hackern zusammen, die regelmäßig Angriffe („friendly attacks“) auf die Bremer Verwaltung ausüben, um Sicherheitslücken aufzudecken? Wenn ja, wie oft? Wenn nein, plant er dieses?

Im Rahmen der gemeinsamen Leitlinie für Informationssicherheit von Bund und Länder haben sich die Beteiligten über ein gemeinsames Awareness-Programm für die Beschäftigten in den Ländern verständigt. Seit 2013 werden regelmäßige Roadshows „Die Hacker kommen“ in Bremen und Bremerhaven für alle Beschäftigten mit großem Erfolg und entsprechender Resonanz angeboten.

Auch bei der Überprüfung der Sicherheit der bei Dataport betriebenen Infrastrukturen bedient man sich externer Unterstützung durch Beratungsleistungen bzw. „white hat“ Hackern.

Durch die vertiefte Kooperation zwischen dem BSI und der Freien Hansestadt Bremen wird es zukünftig möglich sein, Ressourcen - insbesondere Hacker - des Bundes in Anspruch zu nehmen und einen kontinuierlichen Verbesserungsprozess zu initiieren. Die Cyber-Sicherheitsstrategie des Bundes bildet dabei den strategischen Rahmen für Länder und Wirtschaft.

5. Welche Behörden und Ämter befassen sich mit jeweils wie vielen Stellen mit dem Thema Cybersicherheit und inwieweit wird dabei zwischen Cyberangriffen, Cyberspionage und Cyberkriminalität unterschieden?

Mit dem Thema Cybersicherheit in Gänze befassen sich mehrere Dienststellen im Land Bremen.

Im Geschäftsbereich der Senatorin für Finanzen wird das Thema „Cyber- und Informationssicherheit“ durch den CIO (Chief Information Officer), das zentrale IT Management in der Abteilung 4 und den CISO (Chief Information Security Officer) bearbeitet.

Im Geschäftsbereich des Senators für Inneres befassen sich der Landesverfassungsschutz, das Landeskriminalamt und der Katastrophenschutz mit den Themen Cyberspionage und Cyberkriminalität.

Der Informationssicherheitsbeauftragte (ISB) des Senators für Inneres befasst sich mit einer vollen Stelle mit dem Thema Cybersicherheit.

Das Fachkommissariat K 15 der Polizei Bremen umfasst die Aufgabengebiete IT-Forensik, Telekommunikationsüberwachung, Video Forensik sowie den Abschnitt Cybercrime-Ermittlungen mit dem Schwerpunkt Cybercrime im engeren Sinne. Dabei beinhaltet der Begriff Cybercrime solche Straftaten, die sich gegen das Internet, weitere Datennetze und informationstechnische Systeme richten. Cybercrime im engerem Sinne meint dabei Straftaten, die sich gegen deren Daten richten sowie solche Straftaten, die mittels dieser Informationstechnik begangen werden. Durch das Fachkommissariat werden neben den zugewiesenen eigenen Ermittlungsverfahren auch Phänomen

bedingte Unterstützungsleistungen für andere Ermittlungsdienststellen wahrgenommen.

Die Abteilung für Staatsschutzangelegenheiten ist zuständig für das Themenfeld der sog. Spionage.

Neben den Landeskriminalämtern befassen sich mit dem Themenfeld der Spionage sowohl im Bereich der Strafverfolgung als auch im Bereich der Spionageabwehr weitere Sicherheitsbehörden, darunter der Generalbundesanwalt beim Bundesgerichtshof, das Bundeskriminalamt (BKA), der Bundesnachrichtendienst, die Verfassungsschutzämter des Bundes und der Länder, das Zollkriminalamt, das Bundesamt für Wirtschaft und Ausfuhrkontrolle und das Bundesamt für Sicherheit in der Informationstechnik.

Spionagetätigkeiten von privaten Organisationen oder Unternehmen untereinander können unter dem Begriff der allgemeinen Cyberkriminalität subsumiert werden. Ein sog. Cyberangriff eines ausländischen Geheimdienstes in Bremen wurde in den letzten Jahren nicht registriert.

In der Ortspolizeibehörde Bremerhaven gibt es bei der Kriminalpolizei eine Ermittlungsabteilung „Internetkriminalität“. Im Bereich der DV-Systemtechnik ist keine Stelle explizit mit dem Themenkomplex befasst.

Bei der Staatsanwaltschaft Bremen haben zwei Staatsanwälte ein Sonderdezernat „Internet- Kriminalität“ mit einem Pensum von jeweils 0,25 VZÄ. Zwischen Cyberangriffen, Cyberspionage und Cyberkriminalität wird hier nicht unterschieden.

Weitere betroffene Ressorts sind anlassbezogen involviert.

6. Welche Qualifikationen haben die Mitarbeiter, die sich in den Behörden und Ämtern mit dem Thema Cybersicherheit beschäftigen und können alle Planstellen mit Fachkräften besetzt werden?

Die Freie Hansestadt Bremen hat - wie auch alle anderen Bundesländer - die Herausforderung bei der Personalgewinnung erkannt. Alle Länder sind sich darüber einig, dass hier neue Wege beschritten werden müssen.

Die Qualifikationen der Mitarbeiter sind bei den ihnen zugewiesenen Aufgaben höchst unterschiedlich, jedoch jeweils angemessen. Bei den ermittelnden Dienststellen werden Informatikerinnen und Informatiker, Wirtschaftsinformatikerinnen und Wirtschaftsinformatiker, Ingenieure, Ingeneurinnen sowie Verwaltungswirtinnen und –wirte in verschiedenen beamtenrechtlichen Laufbahnen und im Tarifbereich beschäftigt. Vakanzen sind nicht bekannt.

Bei der Staatsanwaltschaft Bremen ist einer der beiden Sonderdezernenten bereits seit etwa sieben Jahren mit dieser Rechtsmaterie befasst. Er hat in dieser Zeit zahlreiche Fortbildungsveranstaltungen im Bereich Cybercrime wahrgenommen und regelmäßig an bundesweiten und niedersächsischen

Fachtagungen teilgenommen. Er wird die Behörde allerdings am 01.01.2019 verlassen. Für ihn wird im Geschäftsjahr 2019 ein Staatsanwalt auf diesem Dezernat nachrücken, der sich ab dann in diese Materie einarbeiten muss.

Der zweite Dezernent bearbeitet dieses Sonderdezernat seit etwa einem halben Jahr. Es ist vorgesehen, dass sowohl dieser Dezernent als auch der ab dem Geschäftsjahr 2019 nachrückende Staatsanwalt zukünftig regelmäßig an entsprechenden Fortbildungsveranstaltungen und Fachtagungen teilnehmen werden.

Die Informationssicherheitsbeauftragten (ISB) beim Senator für Inneres und der Bremer Polizei erlangen ihre Qualifikation durch länderübergreifende Schulungen unter Federführung des BKA und durch Qualifikationsmaßnahmen z.B. in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der BAKÖV (Bundesakademie für öffentliche Verwaltung).

Bei der Ortspolizeibehörde Bremerhaven ist im Bereich DV-Systemtechnik für das Fachgebiet niemand ausgebildet.

Bei der Feuerwehr Bremen gibt es keine Planstelle für Cybersicherheit. Die in den Fachreferaten der IuK (Information und Kommunikation) eingesetzten Mitarbeiter und Mitarbeiterinnen haben keine gesonderte Qualifikation in diesem Spezialbereich.

7. Inwieweit sind die bremischen Institutionen nach Ansicht des Senats im Bereich der Cyberkriminalität ausreichend gut aufgestellt und wo sieht der Senat aus welchem Grund welchen Nachholbedarf?

Die Fachdienststelle K 15 bei der Polizei nimmt die zugewiesenen Aufgaben mit gut ausgebildetem Personal zuverlässig wahr. Aufgrund des stark wachsenden Aufwandes zur Bearbeitung von Ermittlungsverfahren der Cyberkriminalität sowie der Wahrnehmung der Zentralstellenaufgaben für das Land – einschließlich der Unterstützung der Ortspolizeibehörde Bremerhaven – ist in den kommenden Jahren ein erheblicher personeller Aufwuchs der Dienststelle einschließlich der technischen Ausstattung erforderlich. Entsprechende Planungen sind gegenwärtig Teil der perspektivischen Personalplanung der Polizei Bremen. Der Senator für Inneres sieht hier eine Schwachstelle in der quantitativen Ausstattung der Personalressourcen.

Aufgrund des aktuell sehr geringen Fallaufkommens ist die sachgerechte Bearbeitung der Ermittlungs- und Strafverfahren im Bereich Cyberkriminalität mit dem aktuellen Personalansatz bei der Staatsanwaltschaft Bremen noch gewährleistet.

8. Inwiefern hat der Senat beziehungsweise haben welche zuständigen Behörden ein Konzept bezüglich einer sicheren Kommunikation der Behörden und Organisationen mit Sicherheitsaufgaben, welches vor Cyberangriffen geschützt ist?

Der wichtigste Kommunikationsweg der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Bremen ist der Digitalfunk, an dem die Feuerwehr Bremen angeschlossen ist. Die Feuerwehr verfügt über ein eingeschränktes Redundanznetz und über ein separates Alarmierungssystem.

Darüber hinaus erfolgt die Kommunikation innerhalb der Länder-/Bundespolizeien über ein separates, nach dem Schutzbedarf der zu versendenden Daten ausgerichtetes Sondernetz der Polizeien. Dieses Netz befindet sich in der Hoheit des Bundeskriminalamtes (BKA).

9. Welche Aufgabe nimmt das Unternehmen Dataport im Bereich der Cybersicherheit wahr und wie gestaltet sich die Zusammenarbeit mit den Behörden und Ämtern?

Dataport ist kein Unternehmen in privater Rechtsform, sondern eine Anstalt öffentlichen Rechts. Träger sind die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein (Land und Kommunalverbund). Sitz der Anstalt ist Altenholz in Schleswig-Holstein. Für vier dieser Länder ist Dataport ein zentraler IT-Dienstleister, so auch für Bremen. Für Bremen umfassen die Aufgaben den zentralen Rechenzentrumsbetrieb, das Management von dezentralen IT-Systemen sowie die Bereitstellung von Netz- und Telekommunikationsdienstleistungen. In allen seinen Bereichen hat sich Dataport zur Aufrechterhaltung der Informationssicherheit verpflichtet. Damit ist auch eine wesentliche Voraussetzung für die Abwehr von Cyberangriffen gegeben, nämlich IT ordnungsgemäß zu betreiben. Die Abwehr von Cyberangriffen und ihre Prävention ist daher unmittelbar Teil der Dienstleistungen von Dataport. Dataport verfügt über leistungsfähige und effektive Strukturen zur Aufrechterhaltung der Informationssicherheit und leistet daher einen unerlässlichen direkten Beitrag für die Cybersicherheit der bremischen Verwaltung. Die Kommunikation zu den Anwendern in der bremischen Verwaltung verläuft insbesondere dort, wo der Systembetrieb vollständig an Dataport übertragen wurde, reibungslos.

Darüber hinaus betreiben die Länder ein gemeinsames CERT (Computer Emergency Response Teams) bei Dataport. Dort sind vier Personen gemeinsam für die Bewertung von Software-Schwachstellen, Empfehlung von Abwehrmaßnahmen und für allgemeine Informationsarbeit tätig. Das CERT-Nord stellt auch die Kommunikation zu den CERTs der anderen Länder und des Bundes im Rahmen des Verwaltungs-Cert-Verbunds (VCV, vgl. Frage 10) her. Das CERT-Nord seinerseits erhält Warn- und Störungsmeldungen aus den IT Bereichen und ermittelt daraus ein Lagebild. Dieses wird durch Newsletter zurück in die bremische Verwaltung gespiegelt.

Dataport meldet Sicherheitsvorfälle an das Zentrale Informationssicherheitsmanagement bei der Senatorin für Finanzen.

Bremerhaven ist in die Kommunikation dieser Stellen einbezogen, so dass Land und Kommunen vollständig und einheitlich Dienstleistungen des CERT-Nord nutzen. Das CERT-Nord informiert auch die Betriebsbereiche bei Dataport über seine Erkenntnisse, so dass hier sehr schnell reagiert werden kann.

10. Inwieweit kooperiert Bremen bei dem Thema Cybersicherheit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder mit den zuständigen Behörden anderer Bundesländer?

Die koordinierte Zusammenarbeit mit weiteren Trägern von Dataport, den Ländern und dem Bund ist über die jeweiligen Informationssicherheits-managements der Trägerländer gegeben. Der Austausch über gezielte und ungezielte Bedrohungsszenarien wird auf dem Weg über das CERT-Nord zum VerwaltungsCERT Verbund (VCV) des Bundes und der Länder gewährleistet.

Die Innenministerkonferenz und der IT-Planungsrat widmet den Themen Cyber- und Informationssicherheit jeweils eine eigene Arbeitsgruppe, die sich inhaltlich koordinieren.

Im Bereich kritischer Infrastrukturen (KRITIS) beim Senator für Inneres erfolgt die Kooperation im Rahmen der KritisV zwischen dem zentralen Ansprechpartner beim Senator für Inneres und dem BSI, das wiederum Kontakt zu den anderen Ansprechstellen der Länder hält. Die Polizeien des Landes Bremen kooperieren mit dem BSI in Form von länderüberreifenden Gremien, an denen auch das BSI selbst beteiligt ist.

11. Inwieweit ist Bremen durch welche Institute oder Dienststellen im Bereich der Forschung und Entwicklung zum Schutz vor Cyberangriffen mit welchem Aufwand (Personal und Kosten) tätig beziehungsweise beteiligt?

Die Senatorin für Finanzen, der Senator für Inneres und die Polizei Bremen sind in länderübergreifenden Gremien und Arbeitsgruppen vertreten.

An der Forschung und Entwicklung zum Schutz vor Cyberangriffen besteht hier keine Beteiligung.

Zur Verbesserung der Informationssicherheit in der Verwaltung gibt es eine Kooperation der bremischen Verwaltung mit dem Technologiezentrum Informatik (TZI). Der Senator für Wirtschaft, Arbeit und Häfen und die Senatorin für Finanzen tragen im Volumen einer Stelle beim TZI gemeinsamen den Aufwand für die Evaluation und Verbesserung der Informationssicherheit in bremischen Einrichtungen, die ihren IT Betrieb nicht oder nur teilweise an Dataport übertragen haben.

Das TZI beteiligt sich u.a. an der Entwicklung und Weiterentwicklung von Standards für Cybersicherheit, der Erkennung und Validierung von Security Patterns oder der Entwicklung sicherer mobiler Anwendungen zur Steuerung von Smarthome-Systemen.

Forschungsfragen zu Cybersicherheit werden im Land Bremen am Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI Standort Bremen), am Institut für Seeverkehrswirtschaft und Logistik (ISL) sowie der Universität Bremen (primär Technologiezentrum Informatik an der Universität Bremen - TZI), z. T. unter Hinzuziehung weiterer bremischer Forschungspartner adressiert.

In der Grundlagenforschung war das DFKI u.a. maßgeblich an der Initiierung und Durchführung des Deutsche Forschungsgemeinschaft (DFG)-Schwerpunkts 1496 "Zuverlässigkeit sichere Softwaresysteme" beteiligt (2010-2017).

Der Schwerpunkt am ISL liegt besonders auf Sicherheitsfragen in Häfen und Offshore-Windparks.

Derzeit laufen in Bremen neben Einzelförderungen (DFG, Bundesministerien) mehrere größere Forschungsverbundprojekte im Bereich IT-Sicherheit u.a. in Kooperation mit lokalen (Bremer) Firmen, bei denen Fragen der Cybersicherheit im Mittelpunkt stehen. Insgesamt wurde für 2018 von den genannten Forschungseinrichtungen in Bremen eine Fördersumme von etwa 2 Mio. € eingeworben.

Cybersicherheit spiegelt sich auch in den Inhalten in Lehrveranstaltungen der Hochschulen. Beispielhaft ist die Veranstaltung „Informationssicherheit“ an der Universität Bremen zu nennen, in der pro Jahr ca. 100 Studierende der Informatik und benachbarter Studiengänge die Grundlagen der Informationssicherheit erlernen.

Beispiele für größere derzeit laufende Forschungsverbundprojekte mit Projektpartnern:

- SecProPort (BMVI, IHATEC) Skalierbare Sicherheitsarchitekturen für die Geschäftsprozesse in deutschen Häfen (2018-2021, Projektpartner: DFKI, ISL, Universität Bremen, dhb, BLG, Hapag-Lloyd, datenschutzCert, Duisburger Hafen AG)
- SATISFy (BMBF) Validierung von SAfeTy- und Security-Anforderungen in autonomen Fahrzeugen (2018-2021, DFKI, Projektpartner: DFKI, Concept Engineering GmbH, HOOD GmbH, Kasper & Oswald GmbH, Robert Bosch GmbH, Universität Tübingen, Volkswagen AG)
- SECRC (BMBF) Security by Reconfiguration - Physikalische Sicherheit durch dynamische Hardware-Rekonfiguration (2017-2019, Projektpartner: DFKI, Robert Bosch GmbH, Forschungszentrum Informatik (FZI), Mixed Mode GmbH, TU Hamburg-Harburg)
- PortSec: IT-Risikomanagement in der Hafentelematik (BMBF, Laufzeit 09/2016-08/2018; Koordination durch ISL; ISL-Fördersumme 547.672 €; weitere bremische Partner: dbh Logistics IT AG, datenschutz cert GmbH, Universität Bremen).

Im Übrigen wird auf Frage 14 verweisen.

12. Welche Präventionsmaßnahmen mit der Prävention zum Schutz vor Cyberangriffen nimmt der Senat beziehungsweise die zuständige Behörde vor, insbesondere bei den

- Sicherheitsbehörden,
- Dienststellen der öffentlichen Verwaltung,
- den öffentlichen Versorgungsunternehmen,
- den öffentlichen Verkehrsunternehmen,
- der in Bremen angesiedelten Industrie und Wirtschaft sowie
- den Hochschulen und Forschungsinstituten in Bremen?

Das zentrale IT-Sicherheitsmanagement bei der Senatorin für Finanzen arbeitet im Bereich der Prävention für die Dienststellen der öffentlichen Verwaltung auf verschiedenen Ebenen:

- „Awareness“ Maßnahmen:

  In Zusammenarbeit mit der Bundesakademie für Öffentliche Verwaltung (BAKÖV) finden in Bremen regelmäßig (mehrfach jährlich) für die Zielgruppe „alle Beschäftigten der gesamten Verwaltung“ Aufklärungsveranstaltungen zu den Themen IT-Sicherheit/Cybersicherheit: „Die Hacker kommen“ statt. Auf diesen u.a. mit „Life Hacking“ speziell auf die Verwaltungen zugeschnittenen Veranstaltungen werden die Beschäftigten in Hinblick auf spezielle Gefährdungen für die Öffentliche Verwaltung sensibilisiert.

- Erstellung und Bereitstellung von themenbezogenen „Flyern“, „Türhängern“ u.ä. zur Aufklärung zu Informationssicherheits- und Cybersicherheitsgefährdungen.

- Aus- und Fortbildung von neuen IT-Sicherheitsbeauftragten der bremischen Verwaltung der Eigenbetriebe und anderer bremischer Einrichtungen und Betriebe im Aus- und Fortbildungszentrum für den bremischen Öffentlichen Dienst (AfZ) und bei der BAKÖV in Zusammenarbeit mit und durch Spezialisten im Auftrag der BAKÖV.

- In der Aus- und Fortbildung neuer Mitarbeiterinnen und Mitarbeiter im AfZ ist die Sensibilisierung für das Thema IT-/Cybersicherheit inzwischen ein Baustein der regulären Ausbildungsmaßnahmen.

- Die Senatorin für Finanzen stellt im Intranet das „BITS“ (Behörden IT Sicherheitstraining -> https://www.bits-training.de/) für alle Beschäftigten bereit, ein Selbstlernprogramm zu Themen und Zielen der IT-Sicherheit.

- Im Intranet der bremischen Verwaltung (Mitarbeiterportal) werden lageabhängig an prominenter Stelle (Startseite) kurze Hinweise zum Umgang mit aktuellen Bedrohungslagen geschaltet.

- Zu den laufenden organisatorischen Prozessen gehören:

- Regelmäßige Treffen und Videokonferenzen der IT-Sicherheitsmanager der Dataport Trägerländer und des CERT-Nord zum Austausch und zur Abstimmung gemeinsamer Maßnahmen, in Lagen auch regelmäßig bis zu täglich.
- Regelmäßige Treffen der Informationssicherheitsbeauftragten der bremischen Verwaltung („Jour Fixe ISM“) zum Austausch und zur Abstimmung von Maßnahmen.
- Technische Maßnahmen erfolgen durch den zentralen IT-Dienstleister Dataport. Durch die zentralen ISM der Dataport-Trägerländer, das CERT-Nord sowie das Sicherheitsmanagement von Dataport werden in Regelprozessen die technisch organisatorischen Maßnahmen zur Abwehr von Cyberangriffen regelmäßig nachgeschärft und weiterentwickelt. Das betrifft die Durchführung von Sofortmaßnahmen aber auch die regelmäßige Weiterentwicklung der technischen IT-Infrastruktur auf dem Stand der Technik, um ein möglichst hohes Maß an Resilienz in diesem Bereich zu erzielen.
  Konkrete Maßnahmen in diesem Bereich können hier aus Sicherheitsgründen nicht beschrieben werden.

Darüber hinaus entwickeln einzelne Bereiche – oft in Zusammenarbeit mit spezialisierten Dienstleistern - spezifische IT-Sicherheitskonzepte und Amtsanweisungen für ihre speziellen Aufgaben und Infrastrukturen, z.B. das ASV.

Auch bei der Polizei ist ein Informationssicherheitsmanagementsystem (ISMS) etabliert. Die Behandlung von Sicherheitsvorfällen ist dort systematisch geregelt.

Umfangreiche Sicherheitsmaßnahmen sind umgesetzt:

- Ein abgeschlossenes Netz
- Aufwändig abgesicherte Netzgrenzen
- Kein direkter Internetzugriff
- Sicherstellung durch länderübergreifende Audits / Revisionen.

In weiteren originären Aufgabenbereich der Cybercrime-Ermittlungen der Fachdienststelle K 15 ist die „Zentrale Ansprechstelle Cybercrime für die Wirtschaft“ (ZAC) abgebildet. Im Jahr 2018 haben die Beschäftigten der Fachdienststelle an bislang 22 Veranstaltungen der Wirtschaft teilgenommen, um dort über aktuelle Gefahren und Risiken im Rahmen von Vorträgen zu informieren. Die Anzahl der Termine nimmt über die Jahre kontinuierlich zu. Neben den Vortragsterminen sind Mitarbeitende als ZAC-Vertretende in unterschiedlichen Vereinigungen als permanenter Gast/Behördenvertretung beteiligt.

Für die Bereiche der öffentlichen Versorgungsunternehmen und Verkehrsunternehmen wird auf die Antwort zu Frage 2 verwiesen, in Bezug

auf die in Bremen angesiedelte Industrie und Wirtschaft auf die Antwort zu Frage 14.

Angaben zu Hochschulen und Forschungsinstituten in Bremen enthält die Antwort zu Frage 11.

13. Inwieweit bieten die zuständigen Behörden Beratungsgespräche für welche Zielgruppen an und in welcher Häufigkeit und von wem bzw. wie wurden diese Beratungsgespräche jeweils in den vergangenen fünf Jahren angenommen?

Für den Bereich der Öffentlichen Verwaltung sind solche Gespräche ein laufender, kontinuierlicher Prozess, so dass die Anzahl solcher Gespräche im Innenverhältnis nicht quantifizierbar ist.

Ansonsten wird auf die Antwort zu Frage 12 verwiesen.

14. Inwieweit arbeitet der Senat beim Thema Cybersicherheit insbesondere mit kleinsten, kleinen und mittleren Unternehmen zusammen, die häufig nicht über die Ressourcen verfügen, eigene IT-Sicherheitsprogramme aufzulegen?

Der Senat unterstützt vielfältige Angebote für Bremer und Bremerhavener Unternehmen. Viele dieser Angebote sind für die Unternehmen kostenfrei. Die nachfolgend aufgeführten Institutionen bieten nicht nur Angebote zur IT- und Datensicherheit, sondern weitere umfangreiche Angebote rund um die digitale Transformation an:

- Mittelstand 4.0-Kompetenzzentrum Bremen
  - Innovationsforen und Innovationwerkstätten
- Maritimes Cluster Norddeutschland
  - Innovationsforen und Innovationwerkstätten
- DigiLab
  - Dialogplattform, Innovationswerkstätten
- Metropolregion Nordwest
  - Information, Veranstaltungen
- Freies Institut für IT-Sicherheit (ifit)
  - Dialogforen, Workshops, Beratungen, Notfalltelefon.
- TZ
  - Live Hackings und Sicherheit mobiler Anwendungen, Informationsveranstaltungen.
- Webseite Digitalisierung in Bremen (www.digitalisierung-bremen.de)
  - Unter der Rubrik „Beratungsförderung“ sind 10 Unternehmen zur einzelbetrieblichen Förderung für IT Sicherheitskonzepte aufgelistet.

- Datenschutz Nord
    - Auf der Webseite Datenschutz Nord gibt es diverse Informationen zur IT-Sicherheit. Seminare für IT-Sicherheit

- Bremen digitalmedia
    - Veranstaltungen, Workshops
- I2B
    - Meetups rund um das Thema Digitalisierung
- BIS Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung mbH
    - Innovationswerkstätten, Veranstaltungen, Beratung, Förderung.

Im Weiteren gibt es in Bremen und Bremerhaven für Kleine und Mittlere Unternehmen (KMU) folgende Förderungsmöglichkeiten:

- Mit dem Digitalisierungsberaterpool besteht seit 2017 ein Angebot zur Förderung von Beratungsdienstleistungen rund um Digitalisierung und Arbeit 4.0. Die Förderung beträgt 50% bis zu 5.000 €.
- Der Verein „Impulsgeber Zukunft“ berät über das Programm „Unternehmenswert Mensch“ beim Thema Arbeit 4.0. Gefördert werden Beratungen bis max. 10 Tage zu Tagesätzen bis 1.000,- €, der nicht rückzahlbare Zuschuss beträgt 80 % bei Kleinstunternehmen bis 9 MA und bei Betrieben 10-249 Beschäftigen 50 %.
- Im Bundesprogramm „Go Digital“ gibt es einen Fördersatz von 50 Prozent auf einen maximalen Beratertagesatz von 1.100 Euro (akkreditierte Berater). Der Förderumfang beträgt maximal 30 Tage in einem Zeitraum von einem halben Jahr.

Um die Angebote und Unterstützung an die KMU weiter auszubauen, hat der Senator für Wirtschaft, Arbeit und Häfen in dem Maßnahmenpaket „Bremen Digital 2018-2021“ mit dem Thema „Cybersicherheit in der Wirtschaft“ geplant, das Know-how von Instituten und Unternehmen in Bremen und Bremerhaven zur IT- und Datensicherheit der Wirtschaft zugänglich zu machen. Dazu werden geeignete Informationsformate und Demonstrationsmöglichkeiten entwickelt sowie Förderangebote zur Verfügung gestellt.

Folgende Maßnahmen werden geplant:

a) Innovationswerkstätten zur Qualifizierung des Mittelstandes
b) Innovationsforen inkl. Live Hackings zur Information über neue Trends und Technologien in der IT Security

In zahlreichen Projekten wurde und wird bereits das Thema IT Sicherheit bei der Entwicklung der jeweiligen Anwendung berührt, auch wenn es nicht direkt im Mittelpunkt der jeweiligen Entwicklung bzw. Anwendung steht.

Der Senator für Wirtschaft, Arbeit und Häfen unterstützt (wie in allen anderen Clustern auch) zum Beispiel im Cluster Maritime Wirtschaft mit personellem Aufwand die Bildung von Projektkonsortien im Bereich der „zivilen maritimen

Sicherheitsforschung und Entwicklung innovativer Sicherheitstechnologien und neuen Dienstleistungen“. Eingebettet ist dies im Nationalen Masterplan Maritime Technologien- NMMT der Bundesregierung.

Bereits 2018 wurde durch eine Vielzahl an Maßnahmen und Angeboten an die KMU die Cybersicherheit thematisiert und die Unternehmen sensibilisiert.

Für 2019 sind schon diverse Maßnahmen zum Thema IT und Datensicherheit geplant bzw. in der Planung:

Aus der Veranstaltungsreihe „Das digitale Jetzt – spannende Beispiele aus der Praxis“, die in Kooperation mit bremen digitalmedia und SWAH im monatlichen Rhythmus angeboten wird, ist für 2019 die Veranstaltung „Cyberkriminalität- Aktuelle Bedrohungen und Live Hacking“ in Bremerhaven geplant.

In einer Veranstaltung mit dem Mittelstand 4.0 Kompetenzzentrum und der Handelskammer wird im ersten Quartal 2019 ein Programmpunkt die Sensibilisierung der KMU zum Thema IT-Sicherheit sein.

Im Oktober 2019 findet die 2. Maritime Sicherheitskonferenz statt. Das Thema IT Sicherheit wird ein Schwerpunkt der Konferenz sein.

Das ifit (https://www.ifitev.de/) veranstaltet jährlich dreimal das sogenannte BremSecForum und bietet Informationen und Erfahrungsaustausch zu aktuellen Themen der Informations- und IT-Sicherheit an.

15. Wie viele Betroffene von Straftaten im Bereich der Cyberkriminalität erstatten jährlich bei der Bremer Polizei Anzeige und welche Schadenssummen werden dabei ermittelt?

Bei der Polizei Bremen sind bislang keine Anzeigen von bremischen Unternehmen oder kritischen Infrastrukturen eingegangen.

Schadenssummen sind durch die Polizei Bremen nicht bezifferbar, da es sich in der Regel um wirtschaftliche Kollateralschäden handelt, welche nicht regelhaft durch die Polizei Bremen erfasst werden.

Der Interessenverband IT schätzt den bundesweiten jährlichen Gesamtschaden auf ca. 55 Milliarden Euro. Hierbei handelt es sich jedoch um nicht verifizierte Angaben, welche lediglich auf einer Schätzung beruhen.

Im Bereich der Ortspolizeibehörde Bremerhaven waren im Bereich der Cyberkriminalität bisher zwei Unternehmen und 56 Privathaushalte von Angriffen betroffen. Cyberattacken verursachen hier bei Privathaushalten durchschnittlich eine Schadenshöhe von ca. 200 – 300 Euro. Bei den beiden Unternehmen handelte es sich zum einen um eine weltweit agierende Reederei, die 200 bis 300 Millionen Dollar Schäden davontrug. Bei dem zweiten Unternehmen handelte es sich um einen großen Klinikverbund, der nach eigenen Angaben keinen finanziellen Schaden erlitten hat, da das Netzwerk durch das eigene Personal wiederinstandgesetzt werden konnte.

16. Welche Erklärungen hat der Senat dafür, dass nur etwa jeder sechste Betroffene Anzeige erstattet und welche Aufklärungsmaßnahmen hält er insoweit für erforderlich?

Das geringe Anzeigeverhalten resultiert nach Auffassung des Senats aus mehreren Faktoren. Häufig sind die finanziellen Schäden für den „Normalbürger“ bei Straftaten im Bereich Cyberkriminalität im engeren Sinne noch verhältnismäßig gering. Die Anzeige dieser Straftaten ist hingegen mit Aufwand verbunden (Anzeigeerstattung, ggf. [befürchteter] Verzicht auf die infiltrierte Hardware zu Auswertungszwecken durch die Polizei für längere Zeit). Diese stehen voraussichtlich für Bürgerinnen und Bürger nicht im Verhältnis zu den Erfolgsaussichten, die Täter zu ermitteln und zu überführen. In großen Teilen der Öffentlichkeit dürfte der Eindruck vorherrschen, dass die ohnehin nicht gefasst werden und sie ihre finanziellen Schäden niemals ersetzt bekommen werden. Geschädigte Unternehmen sehen auf Grund des Aufwands häufig von einer Anzeigenerstattung ab, insbesondere wenn Schäden abgewendet bzw. Datenverluste durch die eigene IT egalisiert werden konnten. Imageschäden in der Öffentlichkeit werden nicht mehr als Hauptumstand der geringen Anzeigenquote angesehen. Durch die ansteigende Bekanntheit der Zentralen Ansprechstelle Cybercrime für die Wirtschaft (ZAC) nimmt die direkte Kommunikation geschädigter Unternehmen mit der Polizei kontinuierlich zu.

Aufgrund der Vielzahl der Verschleierungsmöglichkeiten sowohl des Daten- als auch des Geldstroms gestaltet sich die Täterermittlung in der Praxis als äußerst schwierig. Je zeitnaher die Anzeige der Tat erfolgt, desto größer sind die Erfolgsaussichten, den Täter noch anhand digitaler Spuren überführen zu können. Insoweit könnte die Einrichtung einer Onlineplattform zur Anzeigenaufnahme in diesem Deliktsbereich mit entsprechender Aufklärung der Bevölkerung die Erfolgsaussichten der Ermittlungen und damit auch die Anzeigemotivation erhöhen.

Auf Grund der hohen Dynamik im Deliktsfeld „Cybercrime“ und der damit verbundenen schnellen Reaktionsnotwendigkeit sind Präventionsangebote nur schwer oder mit erheblichen Aufwänden umzusetzen. Die Polizei Bremen verbreitet geeignete Informationen über ihre Homepage (Link zum Ratgeber Internetkriminalität der Polizei Niedersachsen) und über Pressemeldungen. Damit ist eine schnelle Informationsweitergabe polizeilicher Erkenntnisse an die Bevölkerung gewährleistet. Die Internetseiten des BSI sind ebenfalls eine geeignete Informationsquelle.

Die Aufklärung der Bevölkerung muss jedoch über die polizeilichen Präventionsmöglichkeiten hinaus vollzogen werden. Es bedarf einer verstärkten und frühen Aufklärung der Bevölkerung im Umgang mit digitalen Daten. Bereits im schulischen Bereich müssen hierfür Grundlagen gesetzt werden.

17. Inwieweit hat der Senat Informationen darüber, ob und in welchem Umfang Geschädigte auf zivilrechtlichem Weg Ersatz der ihnen zugefügten Schäden erhalten (haben)?

Hierzu hat der Senat keine Kenntnisse.

18. Wie ist die Polizei Bremen sachlich und personell bei den Ermittlungen zu Cyberkriminalität aufgestellt und hält der Senat hier aufgrund des offensichtlichen Anstiegs der kriminellen Aktivitäten eine Aufstockung der Mittel für notwendig?

Zur personellen Ausstattung wird auf die Antwort zu Frage 7 verwiesen.

19. Wieviel Ermittlungsverfahren hat es im Bereich Cyberkriminalität in den letzten fünf Jahren jeweils bei der Staatsanwaltschaft mit welchem Ausgang gegeben?

Der Beantwortung dieser Frage liegt die Auswertung der Verfahren aus dem Zeitraum vom 01.01.2013 bis einschließlich November 2018 zugrunde.

In dieser Zeit wurden bei der Staatsanwaltschaft Bremen im Bereich Cyberkriminalität insgesamt 91 Ermittlungsverfahren gegen namentlich ermittelte Beschuldigte geführt, davon

- 28 wegen (versuchten) Computerbetruges (§ 263a StGB), von denen 11 gemäß § 153 Abs. 1 StPO eingestellt wurden, 8 gemäß § 170 Abs. 2 StPO eingestellt wurden, 3 mit zusammenhängenden Verfahren verbunden wurden, 3 an auswärtige Staatsanwaltschaften abgegeben wurden, eines gemäß § 154 Abs. 1 StPO eingestellt wurde, eines mit einer rechtskräftigen Verurteilung endete und ein weiteres derzeit noch bei der Staatsanwaltschaft Bremen anhängig ist,
- 21 wegen Ausspähens von Daten (§ 202a StGB), von denen 11 gemäß § 170 Abs. 2 StPO eingestellt wurden, 3 an auswärtige Staatsanwaltschaften abgegeben wurden, 2 mit zusammenhängenden Verfahren verbunden wurden, 2 gemäß § 153 Abs. 1 StPO eingestellt wurden, eines gemäß § 154 Abs. 1 StPO eingestellt wurde, eines nach Anklageerhebung gemäß § 153a Abs. 2 StPO eingestellt wurde und eines mit einer rechtskräftigen Verurteilung endete,
- 20 wegen (versuchten) Betruges (§ 263 StGB), von denen 13 mit zusammenhängenden Verfahren verbunden wurden, 5 gemäß § 170 Abs. 2 StPO eingestellt wurden und 2 an auswärtige Staatsanwaltschaften abgegeben wurden,
- 7 wegen Vorbereitens des Ausspähens und Abfangens von Daten (§ 202c StGB), von denen 3 mit rechtskräftigen Verurteilungen endeten, 2 mit zusammenhängenden Verfahren verbunden wurden, eines gemäß § 170 Abs. 2 StPO eingestellt wurde und eines an eine auswärtige Staatsanwaltschaft abgegeben wurde,

- 5 wegen (versuchter) Computersabotage (§ 303b StGB), von denen 2 gemäß § 170 Abs. 2 StPO eingestellt wurden, eines an eine auswärtige Staatsanwaltschaft abgegeben wurde, eines mit einer rechtskräftigen Verurteilung endete und ein weiteres derzeit bei der Staatsanwaltschaft Bremen anhängig ist,
- 4 wegen (versuchter) Datenveränderung (§ 303a StGB), von denen 2 gemäß § 170 Abs. 2 StPO eingestellt wurden, eines gemäß § 45 JGG eingestellt wurde und eines mit einer rechtskräftigen Verurteilung endete,
- 2 wegen (versuchter) Fälschung beweiserheblicher Daten (§ 269 StGB), von denen eines gemäß § 154 Abs. 1 StPO eingestellt wurde und eines nach Anklageerhebung noch gerichtsanhängig ist,
- 2 wegen (versuchter) Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks (§ 152b StGB), von denen eines an eine auswärtige Staatsanwaltschaft abgegeben wurde und eines mit einem zusammenhängenden Verfahren verbunden wurde,
- eines wegen Nachstellung (§ 238 StGB), das derzeit bei der Staatsanwaltschaft Bremen anhängig ist und
- ein weiteres Ermittlungsverfahren, das gegen einen namentlich ermittelten Beschuldigten geführt, zu dem der Tatvorwurf sich allerdings nicht mehr feststellen ließ, und das gemäß § 170 Abs. 2 StPO eingestellt wurde.

Im Zeitraum vom 01.01.2013 bis einschließlich November 2018 wurden bei der Staatsanwaltschaft im Bereich Cyberkriminalität außerdem 94 Ermittlungsverfahren gegen unbekannte Täter geführt, davon

- 21 wegen (versuchten) Betruges,
- 17 wegen (versuchter) Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks,
- 13 wegen (versuchter) Computersabotage,
- 11 wegen (versuchten) Computerbetruges,
- 9 wegen Ausspähens von Daten,
- 8 wegen (versuchter) Fälschung beweiserheblicher Daten,
- 7 wegen (versuchter) Erpressung,
- 4 wegen (versuchter) Datenveränderung,
- 2 wegen (versuchter) Nötigung und
- eines wegen eines Vergehens gemäß § 108a UrhG.
- ein weiteres, in dem sich der Tatvorwurf nicht mehr feststellen ließ.

Von diesen Verfahren wurden 67 gemäß § 170 Abs. 2 StPO eingestellt, 19 mit zusammenhängenden Verfahren verbunden und 7 an auswärtige Staatsanwaltschaften abgegeben. Ein weiteres ist derzeit bei der Staatsanwaltschaft Bremen noch anhängig.

20. Wie wird das Personal zur Bearbeitung von Cyberkriminalität bei der Polizei und der Staatsanwaltschaft ausgebildet?

Für den Bereich der Staatsanwaltschaft wird auf die Antwort zu Frage 6 Bezug genommen.

Die Ermittlungspersonen des Fachkommissariats K 15 der Polizei und der Ortspolizeibehörde Bremerhaven im Bereich der Cybercrime-Ermittlungen im engeren Sinne nutzen Aus- und Fortbildungsmöglichkeiten anderer Bundesländer und des Bundes. Weiterhin werden in Abstimmung mit der IT-Forensik Spezialausbildungen durch behördenexterne Spezialistinnenen und Spezialisten in Bremen organisiert.

Die Ausbildung der Ermittlerinnen und Ermittlern der Direktion Kriminalpolizei/LKA der Polizei Bremen im Bereich der Cybercrime-Ermittlungen im weiteren Sinne erfolgt durch Mitarbeitende des Fachkommissariats K 15 im Nebenamt an der Hochschule für öffentliche Verwaltung. Es finden vier Veranstaltungen pro Jahr statt.

Perspektivisch wird beabsichtigt, ergänzend Fachkräfte außerhalb der Laufbahn des Polizeivollzugsdienstes einzustellen.

21. Wie häufig hat man sich in den vergangenen fünf Jahren für die sachgerechte Ermittlungsarbeit externer Sachverständiger bedient, welche Kosten sind dabei jeweils entstanden und wird dies gegebenenfalls zukünftig (weiter) für notwendig erachtet?

Bislang war die Beauftragung von externen Sachverständigen im Bereich Cyberkriminalität durch die Staatsanwaltschaft Bremen nicht erforderlich. Besondere Fachfragen konnten in der Vergangenheit durch den Erfahrungsaustausch mit Dezernenten anderer Schwerpunktstaatsanwaltschaften oder auf polizeilicher Ebene mit den Kriminalbeamten anderer Landeskriminalämter geklärt werden.

Der Erfahrungsaustausch mit den Dezernenten von Schwerpunktstaats-anwaltschaften Cybercrime anderer Bundesländer auf den bundesweiten Arbeitstagungen hat jedoch gezeigt, dass in komplexen Ermittlungsverfahren von dort aus im Einzelfall bereits externe Sachverständige (z.B. vom Fraunhofer-Institut) für besondere technische Ermittlungsfragen herangezogen wurden.

Auf externe Sachverständige wurde bislang nicht zurückgegriffen. Durch die organisatorische Zusammenlegung der Cybercrime-Ermittlungen mit der IT-Forensik in einem Kommissariat und die dort angesiedelten IT-Sachver-ständigen besteht eine enge und kontinuierliche Zusammenarbeit inklusive dem fachlichen Austausch.

22. Wie stellt sich die Bearbeitungssituation (bezogen auf Anzahl der Verfahren, die durchschnittliche Bearbeitungsdauer und die Rückstände) bei der KTU für Ermittlungsverfahren im Zusammenhang mit IT-Sicherheit dar?

Bearbeitungsrückstände liegen bei der KTU Bremen im Bereich Cybercrime im engeren Sinne nicht vor. Die Fachdienststelle Cybercrime der Polizei Bremen verfügt über eigene Auswertecomputer in eigenen, von den Polizei- und Verwaltungsnetzen strikt getrennten IT-Netzen, so dass eine zeitnahe Auswertung bislang immer gewährleistet war.

Anhang zu Frage 1.

Kategorie	Angriffsart	Aufwand bei IT-Dienstleister	Dauer	Auswirkung	2018	2017	2016	2015	2014	Summe	Aufwand (Stunden)
Change- / Schwachstellen management	kein Angriff, proaktiv	Durch-schnitlich 3 Stunden je Vorfall	nicht zutref-fend	temporäre Einschrän-kungen der Serviceverfügbarkeit durch SW-Updates. In dringenden Fällen auch außerhalb der geplanten Wartungsfenster.	13	13	16	14	3	59	177
Trojaner-aktivität	Malware, häufig durch ungerichtete Massen-E-Mails	Durch-schnittlich 1 Stunde je Vorfall	1-2 Tage	durch IT-Dienstleister nicht bewertbar*	48	57	78	12	4	199	199
Attacken von Extern	Direkte Angriffe gegen Dienste und Infrastruktur	Durch-schnittlich 24 Stunden je Vorfall	Durch-schnitt-lich 1 Stunde je Vorfall	oftmals temporäre Einschrän-kungen der Serviceverfügbarkeit		1		4	4	9	216
Falscher Alarm / False Positive	kein Angriff	Durch-schnittlich 1 Stunde je Vorfall	nicht zutref-fend	durch IT-Dienstleister nicht bewertbar*	1		3			4	4
Request for Information	kein Angriff	Durch-schnittlich 8 Stunden je Vorfall	nicht zutref-fend	nicht zutreffend	1	2	2	3	1	9	72
Attacken von Intern	Angriffe aus dem BVN heraus gegen Dienste und Infrastruktur im Internet	Durch-schnittlich 2 Stunden je Vorfall	durch IT-Dienst-leister nicht bewert-bar	durch IT-Dienstleister nicht bewertbar		2	2	2		6	12

Gesamter Aufwand: 680

*Auswirkungen auf den Dienstbetrieb kann der DL nicht beurteilen.