BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 20/7821**
20. Wahlperiode **24.05.13**

Große Anfrage

der Abgeordneten Karl-Heinz Warnholz, Kai Voet van Vormizeele, Dennis Gladiator, Ralf Niedmers, Christoph Ahlhaus (CDU) und Fraktion vom 29.04.13

und Antwort des Senats

Betr.: Cybersicherheit in Hamburg

„Cyber-Angriffe werden immer größer, immer folgenreicher und immer professioneller. Dieser Trend wird sich fortsetzen.“, so der Viren-Experte Eugene Kaspersky auf der Innovationskonferenz 2013 in München.

Unsere Gesellschaft ist hoch technologisiert und der technische Fortschritt – und damit auch die technische Abhängigkeit – nimmt dabei zu. „Deutschland wird – wie jedes Land – immer mehr abhängig von der Funktionsfähigkeit von Netzen“, sagt der Bundesminister des Inneren, Dr. Hans-Peter Friedrich. Im Kampf gegen Angriffe auf staatliche wie private Computernetzwerke sind sowohl Regierungen und Behörden wie auch die Wirtschaft gefordert, ihre Netze gegen Angriffe zu schützen. Dies gilt insbesondere für die kritischen Infrastrukturen, aber auch für die Datennetze der Sicherheitsbehörden.

Hamburg als Metropole und Wirtschaftsstandort ist dabei im besonderen Fokus möglicher Cyberangriffe. Ein gezielter Cyberangriff mit dem Ziel der Sabotage oder Spionage auf Hamburger Unternehmen, insbesondere Versorgungsunternehmen, auf die Hafenwirtschaft oder die Sicherheitsbehörden hätte katastrophale Auswirkungen auf jeden einzelnen Menschen in unserer Stadt – abgesehen von den unübersichtlichen materiellen und wirtschaftlichen Schäden sowie möglichen Verlusten von Leib und Leben. Im Falle von Spionage könnte sensibles Wissen von Behörden und Unternehmen entwendet werden und hohe wirtschaftliche Schäden verursachen. Aus diesem Grund obliegt dem Hamburger Senat eine besondere Verantwortung zum Schutz unserer IT-Infrastruktur vor Cyberangriffen und dessen Auswirkungen.

Vor diesem Hintergrund fragen wir den Senat:

Die Sicherheit der Datenverarbeitung ist für Privatpersonen, Firmen sowie öffentliche Einrichtungen ein wichtiger Teil von gesellschaftlicher Sicherheit geworden. Identitätsdiebstahl kann für jeden Einzelnen dramatische Folgen haben (zum Beispiel Verlust von Geld oder persönlicher Integrität). Firmen, deren IT nicht störungsfrei funktioniert, können keine Waren ausliefern oder ihnen wird ihr geistiges Eigentum in Form von neuen Produkten oder Ähnlichem gestohlen. Die öffentlichen Einrichtungen müssen nicht nur das Funktionieren der Verwaltung sicherstellen, sondern auch die Sicherheit der ihnen von den Bürgerinnen und Bürgern anvertrauten Daten.

Für die Aufgabenwahrnehmung in der hamburgischen Verwaltung hat daher die Informationssicherheit eine erhebliche und weiterhin zunehmende Bedeutung. Gleichzeitig ist für eine moderne Ausgestaltung der Zusammenarbeit mit Verwaltungskunden eine Integration von neuen Kommunikationswegen erforderlich. Häufig werden Daten

von internen und externen Stellen gemeinsam bearbeitet. Zugriffe von außen können jedoch die Informationssicherheit beeinträchtigen, wenn keine geeigneten Maßnahmen zur Sicherung der Informationsprozesse getroffen werden. Daher hat der Senat am 02. April 2013 die Informationssicherheitsleitlinie (IS-LL) für die Freie und Hansestadt Hamburg (FHH) beschlossen. Mit dieser Leitlinie verfolgt der Senat das Ziel, ein umfassendes Konzept zur Informationssicherheit aufzubauen und umzusetzen, um eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen zu erreichen. Dieses Konzept passt sich nahtlos in die gemeinsamen Anstrengungen von Bund und Ländern auf diesem Feld ein. Der IT-Planungsrat von Bund und Ländern hat im März 2013 eine Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung mit einem entsprechenden Umsetzungsplan beschlossen. Darüber hinaus hat der Bund mit seiner im Jahre 2011 aufgelegten Cyber-Sicherheitsstrategie und der Gründung des Cyber-Sicherheitsrates die Aufgaben beschrieben und organisatorische Maßnahmen getroffen, die die Sicherheit im Cyberraum gewährleisten sollen.

Begriffsdefinitionen

Die in der Anfrage benutzten Begriffe von Cybersicherheit bis Cyberspionage bedürfen einer Definition, damit ein gemeinsames Verständnis bei der Beantwortung der Fragen zugrunde liegt. Die Definitionen sind in Anlehnung an das Dokument „Cyber-Sicherheitsstrategie für Deutschland“ des Bundesministeriums des Innern (BMI) aus dem Jahr 2011 aufgestellt worden.

Cyberraum:

Der Cyberraum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyberraum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. IT-Systeme in einem isolierten virtuellen Raum sind kein Teil des Cyberraums.

Cyberangriff:

Ein Cyberangriff oder eine Cyberattacke ist ein gezielter IT-Angriff im Cyberraum, der sich auf größere, für eine spezifische Infrastruktur wichtige Computernetzwerke von außen richtet und zum Ziel hat, die IT-Sicherheit zu brechen. Die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit können dabei als Teil oder Ganzes verletzt sein.

Cybersicherheit:

Cybersicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyberraums auf ein tragbares Maß reduziert sind. Im Informationssicherheitsmanagements (InSiMa) der Freien und Hansestadt Hamburg werden der Angriff von außen (internetbasiert) und die vorbeugende Gefahrenabwehr unterschieden.

Cyberspionage:

Cyberangriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden, wenn sie von fremden Nachrichtendiensten ausgehen oder gesteuert werden, als Cyberspionage bezeichnet.

Cybercrime/Cyberkriminalität:

Cybercrime umfasst Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden. Cybercrime umschreibt hiernach Kriminalitätsformen, die nicht an konkreten Straftatbeständen, sondern am betroffenen Tatmittel orientiert sind. Das Tatmittel kann nach der Definition sowohl Tatsubjekt als auch Tatobjekt sein. Die Definition ist von der Arbeitsgemeinschaft Kripo im Rahmen der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) im September 2012 beschlossen worden.

Dies vorausgeschickt, beantwortet der Senat die Große Anfrage wie folgt:

I. Zuständigkeiten und Aufgaben – Wer macht was?

1. *Welche Behörden und Ämter befassen sich in welcher Art und Weise mit wie vielen Stellen (bitte mit der jeweiligen Wertigkeit angeben) mit dem Thema Cybersicherheit?*

Mit Beschluss der IS-LL gehört die Befassung mit dem Thema Cybersicherheit zu den Regelaufgaben aller Behörden (siehe auch Antwort zu I. 3.). Im Folgenden werden Aufgaben, die von den Regelaufgaben abweichen, je Behörde dargestellt.

Die Polizei verfügt über eine IT-Sicherheitsorganisation. Diese besteht aus dem IT-Sicherheitsbeauftragten, dem IT-Sicherheitsmanager, dem IT-Sicherheitsmanagement-Team und dem sogenannten CERT (Computer Emergency Response Team).

Das Landesamt für Verfassungsschutz (LfV) befasst sich mit dem Thema in Bezug auf den Schutz von Verschlusssachen (VS) in digitaler Form und Bezug nehmend auf das Arbeitsfeld Wirtschaftsspionage. Im Übrigen siehe Drs. 20/5503.

Zusätzlich wird durch Mitarbeiter des Amtes A der BIS ein autarkes, IP-basiertes Kommunikationsnetz als Rückfallstufe im Katastrophenfall betrieben.

Im Bereich der Zahlstelle der EU-Landwirtschaftsförderung werden nach Vorgaben der Europäischen Kommission PC-Arbeitsplätze mit zusätzlicher hoher Sicherheit betrieben. Hierzu besteht seit 2007 ein IT-Sicherheitsmanagement-Team.

Übersicht der Stellenanteile und -wertigkeit

Behörde/Amt	Stellenanteil/-wertigkeit
BIS	
-----Amt A	anteilig E 11/E 12
-----Polizei	anteilig A 15/1 x A 13
-----Feuerwehr	0
-----LBV	anteilig E 12
-----LfV	Keine Angabe (s. Frage 1. der Drs. 20/5503)
BASFI	anteilig E 14
BGV	anteilig A 12
BSB	anteilig A 13/A 16/E 13/E 14
BSU	0
Bezirksverwaltung	anteilig A 15/A 12/E 11
BWF	anteilig E 12
BWVI	anteilig E 12/E 14
FB	anteilig E 14/E 12
HmbfDI	anteilig A 12
JB	anteilig A 11
KB	anteilig A 10/E 12/E 14
RH	0
SK/PA	anteilig A 12/A 14/A 11
ZPD	anteilig E 11/E 12/A 15

2. *Unterscheidet der Senat beziehungsweise die zuständige Behörde bei dem Thema Cybersicherheit zwischen Cyberangriffen, Cyberspionage und Cyberkriminalität?*

   Wenn ja, wie unterscheiden sich diese nach der Auffassung des Senats beziehungsweise der zuständigen Behörde voneinander und welche Dienststelle nimmt hierbei welche Aufgabe wahr?

   Wenn nein, warum nicht?

Cybersicherheit ist das Aufgabenfeld des Informationssicherheitsmanagements (InSiMa) in der Finanzbehörde. Dort werden die generellen Vorgaben für die Behörden sowie für Dataport zu sicherheitsrelevanten Themen erstellt. Durch die IS-LL ist zudem eine Informationssicherheitsmanagement-Arbeitsgruppe (InSiMa AG) gegrün-

det worden, die den regelmäßigen Austausch zwischen den Beteiligten (InSiMa und behördliche Informationssicherheitsbeauftragte (behördlichen InSiBe)) sicherstellt.

Die Polizei unterscheidet nicht zwischen Cyberangriff, Cyberspionage und Cyberkriminalität. Die Begriffe beinhalten grundsätzlich Sachverhalte, die den Anfangsverdacht von konkreten Straftaten nach dem Strafgesetzbuch oder dem Gesetz gegen den unlauteren Wettbewerb begründen. Bei derartigen Sachverhalten werden kriminalpolizeiliche Ermittlungen im Landeskriminalamt Hamburg geführt.

Aufgaben zur Cybersicherheit im engeren Sinne werden bezüglich der internen polizeilichen Kommunikationsvorrichtungen bei der Polizei in der IT-Abteilung wahrgenommen (siehe auch Antwort zu I. 1.).

Die Verfassungsschutzbehörden des Bundes und der Länder unterscheiden zwischen Wirtschaftsspionage und Konkurrenzausspähung beziehungsweise Industriespionage. Als Wirtschaftsspionage wird die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben bezeichnet. Es handelt sich insoweit um Anwendungsfälle der Wirtschaftsspionage im Sinne des § 4 Absatz 1 Nummer 2 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG). Im Gegensatz dazu wird unter Industriespionage verstanden, dass ein (konkurrierendes) Unternehmen ein anderes ausforscht.

Mittel der Wirtschaftsspionage kann auch ein Cyberangriff in Form der Cyberspionage sein.

Wenden sich Unternehmen mit einem Verdachtsfall an das Landesamt für Verfassungsschutz (LfV), prüft das LfV, ob sich Anhaltspunkte für einen Verdacht auf Wirtschaftsspionage feststellen lassen oder ob es sich um einen Fall von Industriespionage handeln könnte. In Fällen mit einem Verdacht auf Wirtschaftsspionage erfolgt die weitere Bearbeitung im Referat „Spionageaufklärung“ und in enger Abstimmung mit dem Bundesamt für Verfassungsschutz (BfV), das die zentrale Auswertungsfunktion im Bereich der Spionageabwehr hat, sowie dem BSI. Können keine ausreichenden Anhaltspunkte für einen Verdacht auf Wirtschaftsspionage festgestellt werden, so wird dem Unternehmen empfohlen, sich direkt an die Polizei zu wenden. Im Einzelfall vermittelt das LfV auf Wunsch des Unternehmens den Kontakt zur Polizei. Im Übrigen siehe Drs. 20/5758.

Das LfV wirkt beim Schutz von VS in digitaler Form bei den Behörden der Freien und Hansestadt Hamburg mit. Deren Verarbeitung und Übertragung regelt die Verschlusssachenanweisung für die Behörden der Freien und Hansestadt Hamburg (HmbVSA) und die Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) des Bundes.

Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) unterscheidet zwischen den genannten Begrifflichkeiten und legt insoweit die Vorgaben des BSI zugrunde.

3. Welche Aufgaben im Einzelnen nehmen die jeweiligen Behörden und Ämter in Bezug auf das Thema Cybersicherheit wahr? Bitte im Detail angeben.

Die Behörden nehmen Aufgaben zum Betrieb der in ihrer Verantwortung stehenden IT-Arbeitsplätze und lokaler Netzwerkkomponenten entsprechend den IT-Sicherheitsvorgaben aus dem IT-Handbuch der Freien und Hansestadt Hamburg wahr. Die Funktion der/des Informationssicherheitsbeauftragten (InSiBe) wird in jeder Behörde gemäß der IS-LL wahrgenommen. Zu den wesentlichen Aufgaben der/des behördlichen InSiBe gehören:

1. Beratung der mit Informationsprozessen befassten Stellen der Behörde (zum Beispiel Organisationsleitungen, IT-Beauftragte, IT-Leitungen) in Fragen der Informationssicherheit durch Unterstützung und Information.
2. Erstellung eines Sicherheitskonzepts, das die Rahmenvorgaben des zentralen Sicherheitskonzepts erfüllt und alle weiteren erforderlichen Maßnahmen zur Informationssicherheit in der jeweiligen Behörde beschreibt, Planung und Erarbei-

tung von behördenspezifischen Vorgaben und Konzepten im Rahmen der Informationssicherheit.

3. Prüfung, ob in der Behörde alle vorgeschriebenen Maßnahmen zur Informationssicherheit umgesetzt werden und wirksam sind, Controllingmaßnahmen im Rahmen der übergeordneten und behördenspezifischen Vorgaben.

4. Teilnahme am regelmäßigen Informationsaustausch beziehungsweise an der Arbeitsgruppe des zentralen InSiMa, Mitwirkung bei der Erarbeitung von Handlungsempfehlungen.

5. Unterrichtung der Beschäftigten in Fragen der Informationssicherheit, das heißt Beratung der Beschäftigten, Sensibilisierungsmaßnahmen durchführen, Information über gegebenenfalls auftretende Sicherheitsprobleme, Hilfestellung bei Aus- und Fortbildungsmaßnahmen.

In der Behörde für Wirtschaft, Verkehr und Innovation (BWVI) werden im Bereich Zahlstelle-Landwirtschaftsförderung vom IT-Sicherheitsmanagement-Team der BWVI folgende Aufgaben wahrgenommen:

- Erstellung und Pflege der Dokumentation (Leitlinienpapiere, Nutzer, Geräte, laufender Betrieb)
- Erstellung und Pflege des IT-Verbundes (GS-Tool)
- Interne Audits und Begleitung von externen Audits (zum Beispiel Kontrolle der festgelegten Maßnahmen/Abläufe bei Dataport)

4. Stehen in den jeweiligen Behörden qualifizierte Mitarbeiter für die Wahrnehmung der Aufgaben der Cybersicherheit zur Verfügung? Bitte nach Behörden und Ämtern angeben. Ist die derzeitige Personalausstattung aus Sicht des Senats beziehungsweise der zuständigen Behörde ausreichend?

Wenn ja, wie kommt der Senat beziehungsweise die zuständige Behörde zu dieser Einschätzung?

Wenn nein, wie will der Senat beziehungsweise die zuständige Behörde dieses Personal rekrutieren? Welche Dienststellen sind davon betroffen und welche Konzepte liegen hierfür vor? Mit welchen Kosten rechnen die jeweiligen Dienststellen, um diesen Personalbedarf abzudecken?

Die in der Antwort zu I. 1. angegebene Personalausstattung ist nach Einschätzung der zuständigen Behörden dem heutigen Bedrohungsniveau angemessen. Diese Einschätzung leitet sich daraus ab, dass die Abwehr von Angriffen und die Prävention bisher erfolgreich bewältigt wurden.

5. Welche Aufgaben nimmt das Unternehmen Dataport im Einzelnen mit wie vielen Stellen bei der Cybersicherheit wahr?

Dataport (Träger sind die Länder Schleswig-Holstein, Hamburg, Bremen, Niedersachsen, Mecklenburg-Vorpommern und der kommunale „IT-Verbund Schleswig-Holstein“) nimmt die folgenden Aufgaben wahr, die unmittelbar der Cybersicherheit zuzurechnen sind:

1. Zentrales Anti-Virenmanagement für die Freie und Hansestadt Hamburg (4,5 MA),

2. Firewallbetrieb für die Freie und Hansestadt Hamburg (9 MA),

3. Zentrales Sicherheitsmanagement, insbesondere IT-Sicherheitsvorfallmanagement in Zusammenarbeit mit den betroffenen Kunden (2 MA).

Darüber hinaus werden eine Reihe betrieblicher Aufgaben wahrgenommen, die mittelbar der Cybersicherheit dienen:

1. Betrieb und Ausbau der Infrastruktur- und Netzarchitektur unter IT-Sicherheitsgesichtspunkten,

2. Sichere Konfiguration und Härtung[1] von Systemen (Clients, Server, Netzwerkkomponenten et cetera) und Fachanwendungen,
3. Bearbeitung von Sicherheitslücken in Hard- und Software sowie Patchmanagement (Einspielen von Sicherheitsupdates),
4. Systemmonitoring und Überwachung,
5. Sicherheitsmanagement auf Basis von IT-Grundschutz (ISO 27001) insbesondere mit den Teilaufgaben Sicherheitskonzeption, Sicherheitsüberprüfungen (Sicherheitsrevision), Notfallvorsorge und Notfallmanagement.

In diesen Aufgabenfeldern sind die beschäftigten Mitarbeiter meist nur anteilig in Verbindung mit anderen IT-betrieblichen Aufgaben tätig, sodass eine Benennung der effektiven Personalstellen im Einzelnen nicht möglich ist. Nach einer qualifizierten Schätzung sind in der Summe mehr als 100 Beschäftigte für derartige Aufgaben tätig.

6. Wie gestaltet sich die Zusammenarbeit zwischen den Behörden und Ämtern der Freien und Hansestadt Hamburg (FHH) und dem Unternehmen Dataport in Sachen Cybersicherheit? An welchen Stellen gibt es Optimierungsbedarf und wann wird dieser vollzogen beziehungsweise umgesetzt?

Dataport betreibt das Netz der FHH, die Serversysteme im Rechenzentrum sowie die unmittelbar von Dataport administrierten Endgeräte. Dataport bietet diese Infrastrukturen in den BSI-Schutzstufen „normal“ und „hoch“ an.

Die Infrastrukturen werden überwacht. Beim Auftreten von Unregelmäßigkeiten werden die betroffenen Stellen informiert und entsprechende Gegenmaßnahmen eingeleitet. Größere Störungen/Angriffe werden gegebenenfalls nach einer Entscheidungsmatrix als Sicherheitsvorfälle eingestuft und je nach Kritikalität und Ausmaß werden die notwendigen Maßnahmen ergriffen. Dataport hat für Notfälle komplette Beschreibungen von Prozessen in Notfallhandbüchern hinterlegt.

Die Zusammenarbeit gestaltet sich auch in den Bereichen, in denen Dataport nicht mit dem Endgerätebetrieb betraut ist, insbesondere bei Feuerwehr und Polizei sowie Gerichten und Steuerverwaltung, problemlos und sachgerecht.

Dataport unterstützt das LfV mit Beratungsleistungen, Kalkulation und Umsetzung von baulich-technischen Maßnahmen in Bezug auf die IT-Sicherheit.

Im Aufbau des Digitalfunknetzes wurde Dataport von der Projektgruppe BOS Digitalfunk Hamburg mit der Konzeption, dem Ausbau und dem Betrieb des Zugangsnetzes (Festnetzanbindung) für die Basisstationen beauftragt. In der Ausführung unterliegt Dataport ebenfalls den von der BDBOS definierten und bundeseinheitlich vorgegebenen Sicherheitsstandards.

Für die wissenschaftlichen Aufgaben betreiben die Hochschulen derzeit eigene Wissenschaftsnetze. Aufgrund der immer engeren Integration aller Aufgaben auch im Wissenschaftsbereich sollen künftig in den Hochschulen integrierte Netze gebildet werden, in denen die administrativen und wissenschaftlichen Aufgaben wahrgenommen werden können. Wegen der mit dieser sogenannten Netzkoppelung verbundenen besonderen Herausforderungen, auch im Bereich der IT Sicherheit, bedarf es dabei einer engen Abstimmung mit dem Dienstleister Dataport und des InSiMa.

Zwischen dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) und der Finanzbehörde sowie Dataport hat es bislang keine Zusammenarbeit in Sachen Cybersicherheit gegeben. Künftig erwartet der HmbBfDI eine engere Zusammenarbeit durch die Teilnahme des InSiBe des HmbBfDI an der AG InSiMa.

[1] Serverhärtung bedeutet, dass alle Betriebssystem-Grundfunktionen, die bei der vorgesehenen Aufgabe des Servers nicht benötigt werden, deaktiviert oder deinstalliert werden. Server mit minimal benötigten Betriebssystem-Grundfunktionen sind durch Schadsoftware oder Hacker deutlich weniger verwundbar beziehungsweise angreifbar als Standardinstallationen.

Zurzeit wird an der Optimierung der Darstellung der aktuellen Sicherheitslage (zum Beispiel Darstellung der Patchstände oder auch Sicherheitsvorfälle in den Behörden) gearbeitet, um diese den zuständigen InSiBes noch schneller zur Verfügung stellen zu können.

7. Auf welcher Grundlage besteht die Zusammenarbeit zwischen der FHH und Dataport?

Grundlage für die Zusammenarbeit zwischen Dataport und der Freien und Hansestadt Hamburg in Bezug auf Cybersicherheit sind die Gründungsdrucksache Dataport zum Gesetz zum Staatsvertrag über die Errichtung von Dataport AöR (siehe Drs. 17/3236) sowie die Änderungsdrucksachen zum Beitritt des Landes Mecklenburg-Vorpommern und der Freien Hansestadt Bremen zum Staatsvertrag (Drs. 18/3061) und zum Beitritt des Landes Niedersachsen zum Staatsvertrag (Drs. 19/6234) sowie die Drucksache zum Gesetz über das „Sondervermögen Hamburgisches Telekommunikationsnetz“ (Drs. 17/3304). Darauf aufbauend wird die Zusammenarbeit in der Benutzungsordnung Dataport vom 16. Januar 2004, der Dataport Sicherheitsleitlinie vom 28. Juni 2006 und der Grundsatzvereinbarung über Kooperation, Auftragsdatenverarbeitung und den Betrieb des Hamburgischen Telekommunikationsnetzes vom 04. Dezember 2009 konkretisiert.

a) Welche Kosten folgen aus der Zusammenarbeit für die FHH? Bitte jeweils nach Behörden und Ämtern gliedern.

Gemäß den oben angeführten Grundlagen der Zusammenarbeit ist Dataport verpflichtet, Maßnahmen zum Datenschutz und zur Datensicherheit zu beachten und umzusetzen. Dies betrifft auch die Umsetzung der Richtlinien aus dem IT-Handbuch der Freien und Hansestadt Hamburg. Dazu sind keine gesonderten Verträge abgeschlossen, die eine Leistungserbringung auflisten. Die bereitgestellte zentrale Infrastruktur (zum Beispiel für Netzzugriff, Mailnutzung, Intranet, Schutztechnologien gegenüber dem Internet et cetera) wird anteilig je Arbeitsplatz durch den Preis je Endgerät abgerechnet. Der Anteil der Sicherheitsmaßnahmen (zum Beispiel Firewallbetrieb, zentraler Verzeichnisdienst) wird nicht explizit ausgewiesen, ist jedoch im Endgerätepreis enthalten.

Das InSiMa hat zwei Verträge mit Dataport abgeschlossen:

1. Abrufvertrag für besondere Situationen (50.000 Euro p.a.)
2. Zentraler Datenbankserver für die Sicherheitsdokumentation (GS-Tool; 27.200 Euro p.a.)

b) Welche personellen, materiellen und/oder organisatorischen Folgen hat die Vereinbarung zwischen der FHH und Dataport für den jeweiligen Vertragspartner?

Die personellen und organisatorischen Auswirkungen folgen der beschriebenen Aufgabenteilung zwischen der Freien und Hansestadt Hamburg und Dataport (siehe Antworten zu I. 4., I. 5. und I. 6.). Dataport nimmt diese Aufgaben jeweils für mehrere Länder wahr und kann daher ein sehr viel höheres Spezialistenwissen vorhalten, als es möglich wäre, wenn die Aufgabe mehrfach wahrgenommen würde. Zu den Kosten siehe Antwort zu I. 7. a).

c) Wurde in die Grundlage der Zusammenarbeit auch das Thema Cybersicherheit aufgenommen?

Wenn ja, mit welchem Inhalt, welchen Aufgaben und welcher Zielsetzung?

Wenn nein, warum nicht?

Dataport ist zur Umsetzung der Richtlinien des IT-Handbuch der Freie und Hansestadt Hamburg verpflichtet (siehe Antworten zu I. 7. und I. 7. a)). Die in den Richtlinien getroffenen Festlegungen binden sowohl die Beschäftigten im Umgang mit der IT als auch den Dienstleister bei der technischen Umsetzung und Unterstützung in sicherheitsrelevanten Themen (zum Beispiel die Passwortrichtlinie, die Freigaberichtlinie, die Vorgabe für den Windows-Client-Betrieb).

8. Welche Aufgabe hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bezug auf die Cybersicherheit der FHH?

Das BSI stellt mit den Grundschutzkatalogen auf Basis der Norm ISO27001 eine umfassende Sicherheitskonzeption zur Verfügung und schreibt diese regelmäßig fort. In der IS-LL ist festgelegt, dass sich die Informationssicherheit in der Freien und Hansestadt Hamburg an den BSI-Grundschutz-Konzeptionen orientiert.

Ein wesentlicher Punkt der IS-LL ist der Aufbau eines CERT-Verbundes (Computer-Emergency-Response-Team) für die Gefahrenabwehr und technische Unterstützung bei Sicherheitsvorfällen. Mit dem BSI wurde eine Vereinbarung getroffen, dass die CERTs sich gegenseitig unterstützen, vertrauliche Informationen austauschen und im Krisenfall eng zusammenarbeiten.

9. Wie gestaltet sich die Zusammenarbeit zwischen der FHH, Dataport und dem BSI? An welchen Stellen gibt es Optimierungsbedarf und wann wird dieser vollzogen beziehungsweise umgesetzt?

Die Zusammenarbeit ist vertrauensvoll und durch die Länderübergreifende Krisenmanagementübung (EXercise) (LÜKEX) 2011 2011 intensiviert worden. Dataport hält ständigen operativen Kontakt zum BSI. Dataport nimmt diese Aufgabe für Bremen, Schleswig-Holstein und Hamburg wahr. In Abhängigkeit von der Bedrohungslage wird diese Zusammenarbeit fortentwickelt.

10. Bestehen aus der Zusammenarbeit mit dem BSI Kosten zulasten der FHH?

Wenn ja, welche und aus welchem Titel werden diese aufgewandt?

Wenn nein, wie werden die anfallenden Kosten gedeckt?

Das BSI stellt für die Zusammenarbeit keine Rechnungen.

11. Kooperiert die FHH außer mit dem BSI im Bereich der Cybersicherheit mit anderen Bundesbehörden?

Wenn ja, mit welchen, welchem Inhalt, welchen Aufgaben und welcher Zielsetzung?

Wenn nein, warum nicht? An welchen Stellen gibt es Optimierungsbedarf und wann wird dieser vollzogen beziehungsweise umgesetzt?

12. Kooperiert die FHH im Bereich der Cybersicherheit mit anderen Bundesländern?

Wenn ja, mit welchen, welchem Inhalt, welchen Aufgaben und welcher Zielsetzung?

Wenn nein, warum nicht? An welchen Stellen gibt es Optimierungsbedarf und wann wird dieser vollzogen beziehungsweise umgesetzt?

Die Organisation der Sicherheitsbehörden in der BIS hat Kontakte zum BMI über den ständigen Ausschuss V der Innenministerkonferenz. Die FHH ist im IT-Planungsrat von Bund und Ländern vertreten.

Für den Verfassungsschutz gilt ergänzend, dass das LfV sowohl im Bereich der Prävention von Wirtschaftsspionage als auch zum Schutz von Verschlusssachen in digitaler Form mit den Verfassungsschutzbehörden des Bundes und der Länder kooperiert. Die Kooperation erfolgt sowohl anlassbezogen als auch anlassunabhängig.

Durch diese Kooperation wird sichergestellt, dass das angestrebte IT-Sicherheitsniveau erreicht, dauerhaft gewährleistet und fortlaufend verbessert wird. Jede im IT-Verbund der Verfassungsschutzbehörden beteiligte Behörde realisiert ihre Sicherheitsanforderungen in eigener Verantwortung auf Grundlage gemeinsamer Sicherheitsforderungen.

Vergleiche auch Vorbemerkung sowie Antworten zu I. 8. und I. 9.

13. Das BSI empfiehlt, IT-Objekte (Anwendungen, IT-Systeme, Räumlichkeiten, Netze) nach den sogenannten BSI-Grundschutzkatalogen zu überprüfen und zu sichern. Stehen qualifizierte Mitarbeiter für die Wahrnehmung der Aufgaben nach BSI-Grundschutz zur Verfügung? Bitte nach Behörden und Ämtern angeben. Wie viele dieser Mitarbeiter sind hauptamtlich mit dem Schutz der IT-Objekte in den jeweiligen Behörden befasst? Ist die derzeitige Personalausstattung aus Sicht des Senats beziehungsweise der zuständigen Behörde ausreichend?

Wenn ja, wie kommt der Senat beziehungsweise die zuständige Behörde zu dieser Einschätzung?

Alle von Dataport betriebenen Infrastrukturen orientieren sich an den Grundschutz-Konzeptionen des BSI. Darüber hinaus erarbeitet das InSiMa zurzeit ein Vorgehenskonzept, in dem mittels eines Differenz-Sicherheitschecks die Anwendungen (Software) und die Infrastruktur (Gebäude, dezentrale Technik) einem Basis-Sicherheits-Check unterzogen werden. Hierfür werden die behördlichen InSiBes fortgebildet. Eine Initialschulung ist durch die Finanzbehörde geplant. Zu den Kapazitäten und Qualifikationen siehe Antworten zu I. 4. und I. 5.

Die Bedrohungslage (siehe auch Antwort zu II. 1.) lässt nach Einschätzung der zuständigen Behörde sowie Dataport aktuell nicht erkennen, dass für die oben angeführten Aufgaben zusätzliches Personal benötigt wird. Im Rahmen der AG InSiMa werden Anforderungen, auch an personelle Ressourcen, kontinuierlich hinterfragt und gegebenenfalls den Erfordernissen angepasst.

II. Beurteilung der Lage

1. Wie beurteilt der Senat beziehungsweise die zuständige Behörde die Gefahr eines Cyberangriffes auf die IT-Netze der FHH?

Ein Cyberangriff auf die IT-Netze der Freien und Hansestadt Hamburg kann nach Einschätzung der zuständigen Behörde grundsätzlich nicht ausgeschlossen werden, allerdings wird die Wahrscheinlichkeit eines Angriffs derzeit eher als gering eingeschätzt. Der Schwerpunkt der Cyberangriffe liegt zurzeit in der Erreichung finanzieller Vorteile (zum Beispiel Trojaner zum Zugriff auf Onlinebanking) und im Bereich der Wirtschaftsspionage. Angriffe auf Behörden und Verwaltungen scheinen bisher nicht im Fokus von potenziellen Angreifern zu liegen.

2. Wie beurteilt der Senat beziehungsweise die zuständige Behörde die Gefahr eines Cyberangriffes auf die IT-Netze öffentlicher Versorgungsunternehmen?

Nach Kenntnis der zuständigen Behörde bewerten HAMBURG WASSER und die HAMBURG ENERGIE GmbH die Eintrittswahrscheinlichkeit eines Angriffsversuches als gering. Das potenzielle Schadensausmaß wird von HAMBURG WASSER als nicht unerheblich eingeschätzt. Daher sind entsprechende Gegenmaßnahmen umgesetzt worden. Es werden im Rahmen der unternehmensweiten Risikomanagementsysteme die Risiken Datensicherheit und IT-Systeme gesondert betrachtet. Die Trinkwasserproduktion unterliegt dabei der höchsten Sicherheitsstufe, daher ist die Steuerung der Werke nicht über das Internet möglich. Alle Produktionsprozesse müssen lokal gesteuert werden. Ein Cyberangriff wird so ausgeschlossen.

3. Wie beurteilt der Senat beziehungsweise die zuständige Behörde die Gefahr eines Cyberangriffes auf die IT-Netze öffentlicher Verkehrsunternehmen?

Die öffentlichen Verkehrsunternehmen haben diesbezüglich entsprechende Abwehrmaßnahmen in ihren IT-Infrastrukturen implementiert.

4. Wie beurteilt der Senat beziehungsweise die zuständige Behörde die Gefahr eines Cyberangriffes auf die IT-Netze der Hochschulen und Forschungsinstitute in Hamburg?

Grundsätzlich gilt, dass IT-Netze von Hochschulen einer Bedrohung durch Angriffe, die als sehr gefährlich einzustufen wären, ausgesetzt sind, sofern keine Vorkehrungen zur Abwehr getroffen werden. Hochschulen sind nach Einschätzung der zuständigen Behörde hinsichtlich der Kritikalität ihrer Daten (etwa in Verbindung mit integrierten Prozessen wie Campus-Management und Forschungs-Management) vergleichbar mit Einrichtungen der Kernverwaltung und ihre gesamte IT-Infrastruktur muss entsprechend hohen technischen Sicherheitsanforderungen ebenso genügen wie den Anforderungen der Datenschutzgesetzgebung. Zu den schutzbedürftigen Prozessen in der Wissenschaft gehören insbesondere die Speicherung und Verarbeitung personenbezogener Daten – bezüglich der Studierenden zum Beispiel prüfungsrelevante Daten – und die Speicherung, Verarbeitung und Kommunikation von forschungsbezogenen Daten – zum Beispiel Drittmittelanträge und Primärdaten sowie zum Beispiel patentierungswürdige Ergebnisse bei Forschung und Entwicklung.

Eine fundierte Einschätzung der konkreten Gefahrenlage ist ohne detaillierte Erhebung der an die IT-Netze der Hochschulen und Forschungsinstitute in Hamburg angeschlossenen Systeme nur sehr allgemein möglich. Generell muss von einer Gefahr von Angriffen ausgegangen werden, da sensible Daten aus der Forschung (auch gemeinsam mit öffentlichen Einrichtungen und Unternehmen) zu wissenschaftlichen Grundlagen und Anwendungen in diesen Netzen verarbeitet werden und zum Teil kritische Infrastrukturen wie Krankenhäuser angeschlossen sind.

Hinsichtlich der im IT-Sicherheitsbereich üblichen Unterscheidung nach den drei Grundwerten (Schutzzielen) Vertraulichkeit, Integrität und Verfügbarkeit ergibt sich:

Gefahren für die Vertraulichkeit (das heißt Verhinderung von unbefugtem Informationsgewinn) von Daten betreffen insbesondere neue Theorien, Methoden und Technologien sowie Software, die im Rahmen von Forschungsprojekten entwickelt werden, darüber hinaus sensible Daten, die von Unternehmen zu Studienzwecken erhoben werden, und schließlich auch personenbezogene Daten. Vor dem Hintergrund des internationalen „Race of Science and Innovation“ muss zudem davon ausgegangen werden, dass Spionage in der internationalen Spitzenforschung weiter ansteigen wird.

Bezüglich der Integrität (das heißt Verhinderung von unbefugten Veränderungen) von Daten besteht insbesondere die Gefahr, dass Systeme, die in Zusammenarbeit mit den Hochschulen und Forschungsinstituten entwickelt werden und etwa in der Wirtschaft und im öffentlichen Dienst eingesetzt werden, so manipuliert werden, dass eine unkontrollierte Steuerung oder gar Abschaltung durch einen Angriff möglich ist. Darüber hinaus könnten Datensätze gezielt manipuliert werden, sodass die Auswertungen der Daten, die als Entscheidungsgrundlage für Wirtschaft und Politik dienen, zu falschen Rückschlüssen beziehungsweise Entscheidungen führen kann.

Hinsichtlich Verfügbarkeit (das heißt Sicherstellung, dass eine Ressource verwendet werden kann, wenn sie benötigt wird) sind insbesondere die IT-Netze von Forschungseinrichtungen, Universitätsklinika und Krankenhäusern zu nennen.

Folgende Tatbestände kennzeichnen die besondere Situation der Hochschulen hinsichtlich der Cyberkriminalität:

- Die hohe Dynamik im Wissenschaftsbereich bildet die Basis für ein besonderes Gefährdungspotenzial. Hierzu weist zum Beispiel die Universität Hamburg auf die besondere Situation einer Hochschule hin, die darin besteht, dass ständig wechselnde große Anzahlen von Studierenden (ein Vielfaches der Mitarbeiter/-innen) für einige Jahre Teil der Organisation werden und über zahlreiche Anwendungs- und Kommunikationssysteme in Lehre, Forschung sowie Verwaltung mobil mitwirken und in wissenschaftliche Projekte eingebunden sind. Daneben werden gerade durch Studierende IT-Innovationen eingefordert und genutzt. Zudem bewegen sich die Hochschulen aufgrund der Anforderungen aus der Wissenschaft technologisch auch bei der IT-Technik an der „Spitze der Innovation“, was besondere Sicherheitsvorkehrungen erfordert.
- Die Hochschulen verfügen nicht nur über leistungsfähige Rechnersysteme, sondern auch über äußerst leistungsfähige Netze mit regionaler und nationaler sowie internationaler Anbindung. So sieht die HafenCity Universität Hamburg die größte

Gefahr in der IT-Sicherheit darin, dass leistungsfähige Systeme betrieben werden, die gut an das Internet angebunden sind. Diese Systeme sind somit für Cyberkriminelle als Hilfsmittel für ihre Angriffe interessant. Diese Systeme würden daher besonders gesichert und überwacht.

5. Wie schätzt der Senat beziehungsweise die zuständige Behörde die Sicherheit der Hamburger IT-Netze ein? Wo sieht der Senat beziehungsweise die zuständige Behörde Bedarf der Optimierung?

Die zuständige Behörde hat bereits im Jahre 2007 eine Prüfung des FHH-Netzes durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein veranlasst. Es wurde ein Basis-Sicherheits-Check des FHH-Netzes auf der Grundlage der BSI-Grundschutzanforderungen durchgeführt. Aufgrund der Ergebnisse sind eine Reihe von Sofortmaßnahmen ergriffen worden. Seit 2007 wird das Projekt „Zentralarchitektur für Basisinfrastruktur“ bei Dataport umgesetzt. Mit diesem Projekt wurden die Leistungsfähigkeit des Netzes und die Robustheit gegen Störungen und Angriffe erhöht. Der erste Teil des Projekts wurde 2010 erfolgreich abgeschlossen und findet im grundschutzkonformen Rechenzentrum bei Dataport seine Fortsetzung. Das Projekt orientiert sich insgesamt an den Prinzipien des Grundschutzkataloges des BSI.

6. Wie schätzt der Senat beziehungsweise die zuständige Behörde die Rolle von Unternehmen bezüglich ihres Schutzes vor Cyberangriffen ein? Wo sieht der Senat beziehungsweise die zuständige Behörde Optimierungsbedarf?

Private Unternehmen sind für den Schutz ihrer IT-Netzwerke selbst verantwortlich. Die IT-Infrastruktur von Unternehmen und deren Sicherung liegt im ausschließlichen Verfügungsbereich der Unternehmen selbst. Sie bestimmen im Kontext des Unternehmenszieles und ihrer jeweiligen eigenen Möglichkeiten Art und Umfang von IT-Grundschutz und seiner firmeninternen Umsetzung. Den zuständigen Behörden sind entsprechende Unternehmensinterna nicht bekannt.

Im Übrigen siehe Drs. 20/5503.

7. Wie viele Fälle von Cyberangriffen sind dem Senat beziehungsweise der zuständigen Behörde seit dem 1. Januar 2010 bekannt? Um was für Angriffe (beispielsweise Sabotage, Spionage oder Erpressung) hat es sich hierbei gehandelt? Welche Tendenzen sind dabei zu erkennen? Bitte jeweils nach Jahren angeben.

Den zuständigen Behörden sind im oben angeführten Zeitraum keine Cyberangriffe (gemäß Definition in der Vorbemerkung) auf die Infrastrukturen der Stadt bekannt.

Das LfV nimmt allerdings freiwillige Meldungen beziehungsweise Anzeigen von Hamburger Unternehmen entgegen, wenn das Unternehmen der Ansicht ist, einem Cyberangriff ausgesetzt gewesen zu sein. Für den genannten Zeitraum sind diese Meldungen in umfänglichen Akten gesammelt. Alle Akten können in der für die Bearbeitung der Großen Anfrage zur Verfügung stehenden Zeit nicht konkret ausgewertet werden. Daher hat sich das LfV auf den Zeitraum 1. Januar 2012 bis 7. Mai 2013 beschränkt. In diesem Zeitraum hat das LfV im Jahr 2012 vier und vom 1. Januar 2013 bis zum 7. Mai 2013 drei Hinweise auf mögliche Cyberangriffe erhalten. Hierbei handelte es sich in einem Fall möglicherweise um Cyberspionage. Mangels abschließender Untersuchung durch das betroffene Unternehmen sind weiter gehende Einschätzungen nicht möglich.

III. Prävention und Information

1. Welche Priorität misst der Senat beziehungsweise die zuständige Behörde dem Thema Cybersicherheit, insbesondere der Prävention und der Aufklärung, zu?

Dem Thema Cybersicherheit und der Information der Anwenderinnen und Anwender kommt eine hohe Priorität zu.

2. Welche Maßnahmen der Prävention zum Schutz vor Cyberangriffen nimmt der Senat beziehungsweise die zuständige Behörde vor, insbesondere bei

a) den Sicherheitsbehörden?

Grundsätzlich werden die für die Hamburger Verwaltung festgelegten Standards zur IT-Sicherheit eingehalten. Aufgrund betriebsbedingter Einflüsse (hier insbesondere Einsatzlenkungssystem) können in wenigen Ausnahmefällen nicht alle Regeln vollumfänglich eingehalten werden. Diesbezüglich gibt es folgende Zusatzmaßnahmen:

Für die Feuerwehr gilt:

1. Die Feuerwehr ist seit einigen Jahren in das Virenmanagement von Dataport eingebunden, obwohl die Feuerwehr ausschließlich über nicht zentral administrierte PCs verfügt.
2. Alle externen Zugänge (USB, Kartenlesegeräte et cetera) sowie DVD-Laufwerke sind grundsätzlich gesperrt. Die Freischaltung erfolgt für einzelne Personen und Geräte auf Antrag nach Prüfung. Dazu wird eine zentrale Softwarelösung genutzt.
3. Soweit externe Daten über USB-Sticks und DVD bei der Feuerwehr eingelesen werden sollen, geht dies nur über sogenannte Datenschleusen in Verbindung mit besonderen Arbeitsplätzen, die über einen speziellen Virenscanner verfügen.
4. Für einen Großteil der Arbeitsplätze (insbesondere Feuer- und Rettungswachen) ist der Zugang ins Internet nur über einen eigenen Proxyserver der Feuerwehr möglich. Für unterschiedliche Benutzergruppen gibt es, abhängig vom möglichen Risiko, unterschiedliche Beschränkungen (beschränkter Zugriff, Ausführungssperre, Download-Begrenzungen).
5. Der Betrieb der sogenannten operativen Arbeitsplätze (Zugangsterminals zum Einsatzlenkungssystem an den Feuer- und Rettungswachen) erfolgt in einer eigenen Domain außerhalb des FHHNET.

Die Polizei hat – unabhängig von technischen Vorkehrungen neben allgemeinen Sensibilisierungsmaßnahmen – frühzeitig damit begonnen, die Mitarbeiterinnen und Mitarbeiter auf einschlägige Fachinformationen des BSI und der TU Berlin hinzuweisen und ein zusammenfassendes internes Informationsfaltblatt „Online-Sicherheit“ herausgegeben.

Die bei der Polizei seit Januar 2010 eingerichtete Zentrale Ansprech-, Clearing- und Koordinierungsstelle für Computer- und Netzwerkkriminalität (ZAC) steht Hamburger Unternehmen und Institutionen für Präventionsgespräche als Ansprechpartner zur Verfügung.

Darüber hinaus siehe Vorbemerkung.

Für das LfV: Siehe Antworten zu I. 2. und I. 3. sowie zu I. 11. und I. 12.

Die BDBOS greift bei eingesetzten Werkzeugen/Systemen auf Empfehlungen und Zulassungen des BSI zurück.

b) den Dienststellen der öffentlichen Verwaltung?

Die Behörden und ihre nachgeordneten Dienststellen und Einrichtungen orientieren sich an den IT-Grundschutz-Empfehlungen des BSI. Die wichtigste Präventionsmaßnahme ist die laufende Ertüchtigung der IT-Infrastrukturen, um so Angriffe abwehren zu können. Daher werden die Anforderungen aus dem Bereich der Cybersicherheit bei der Planung, Umsetzung und dem Betrieb der IT-Infrastrukturen durch das InSiMa eingebracht.

Im Übrigen siehe Antworten zu I. 13. und II. 5.

c) den öffentlichen Versorgungsunternehmen?

HAMBURG WASSER und die HAMBURG ENERGIE GmbH haben nachfolgende Prävention umgesetzt:

- Entkopplung der Trinkwasserproduktionsprozesse vom Internet

- Sicherheitssoftware auf Workstations, Laptops und Servern mit täglicher Aktualisierung durch automatische Updates und zentralem Virenmanagement
- wöchentliche vollständige Untersuchung (Scan) des Systems
- Personal Firewalls und Intrusion-Schutz
- Durchführung von regelmäßigen Sicherheitsaudits mit Penetrationstest durch unterschiedliche externe Dienstleister
- hohe Sicherheit durch strenge Passwortrichtlinien
- Regelmäßige Schulungen der Mitarbeiter im Bereich Informationssicherheit
- Zugangskontrolle und -beschränkung zum Rechenzentrum
- Beschränkung der Möglichkeiten zur Installation von Programmen an den Workstations.
- Diverse weitere Maßnahmen für Netzwerke und Server, die aus Sicherheitsgründen nicht genauer dargelegt werden können.

d) den öffentlichen Verkehrsunternehmen?

Die Erreichung beziehungsweise Erhaltung eines hohen Maßes an Cybersicherheit wird nach Auskunft der Verkehrsunternehmen als sehr wichtige Aufgabe angesehen. Sie nutzen daher konsequent die technischen Möglichkeiten zum Schutz vor Cyberangriffen wie zum Beispiel Firewalls.

e) der in Hamburg angesiedelten Industrie und Wirtschaft?

Die Sicherheit der IT in Industrie und Wirtschaft ist von größter Bedeutung und kann im Falle von Missbrauch weitreichende Konsequenzen für ein Unternehmen haben. Die Unternehmen sind selber für ihre Cybersicherheit verantwortlich. Spezielle Maßnahmen sind hier auch bisher nicht nachgefragt worden.

Im Rahmen des Wirtschaftsschutzes begegnet das LfV der Gefährdung durch Cyberspionage mit einem Informations- und Beratungsangebot für Hamburger Unternehmen, welches präventiv ausgerichtet ist. Im Übrigen siehe Drs. 20/5503 und Drs. 20/5758.

f) den Hochschulen und Forschungsinstituten in Hamburg?

Soweit die Hochschulen und Forschungsinstitute in ihrer Aufgabenerfüllung den Leitlinien und Vorgaben unterliegen, die auch für die „Kernverwaltung“ der Freien und Hansestadt Hamburg gelten, sind die entsprechenden Sicherheitsmaßnahmen aus dem IT-Handbuch der Freien und Hansestadt Hamburg und der IS-LL durch die Hochschulen beziehungsweise durch den Dienstleister Dataport, soweit dieser die technische Infrastruktur bereitstellt (zum Beispiel für zentrale Administrationsverfahren), zu gewährleisten.

Ansonsten liegt die Gewährleistung der entsprechenden Schutzmaßnahmen für die von den Hochschulen selbst betriebenen Rechnersysteme, Netze und Anwendungen in deren Verantwortung. Aufgrund des Gefährdungspotenzials ergreifen die Hochschulen umfangreiche Schutzmaßnahmen zur Abwehr und Verhinderung vor Cyberangriffen.

Alle staatlichen Hamburger Hochschulen haben Zugang zum DFN, das die notwendige nationale Kommunikation mit höchsten Sicherheitsstandards sicherstellt und die Anbindung an europäische und internationale Netze gewährleistet. Das DFN-CERT mit seinen IT-Sicherheitsfachleuten wird von den Hochschulen in Anspruch genommen. Das DFN-CERT warnt frühzeitig bei Bekanntwerden neuer Sicherheitslücken, Viren oder Spams und unterstützt bei der Behebung/Lösung von Sicherheitsproblemen.

Außer den damit verbundenen Maßnahmen müssen die Netz-, Hardware- und Softwareinfrastruktur auf einem technologisch möglichst aktuellen Stand mit entsprechenden Sicherheitsvorkehrungen gehalten werden. Hierzu gehören unter anderem auch Identifizierungsverfahren.

Für die IT-Sicherheit im Universitätsklinikum Hamburg-Eppendorf (UKE) ist der Geschäftsbereich Informationstechnologie (GB IT), dort der Abschnitt Infrastruktur, verantwortlich. Der GB IT verfügt über eine durch das BSI zertifizierte Sicherheitsorganisation. Die betriebswichtigen Bereiche des UKE und insbesondere die Krankenversorgung wären grundsätzlich auch ohne Internetverfügbarkeit arbeitsfähig.

3. Welche Maßnahmen der Prävention zum Schutz vor Cyberangriffen unternimmt das Unternehmen Dataport?

Dataport betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 auf Basis der IT-Grundschutz-Empfehlungen des BSI. In diesem Rahmen werden die Anforderungen aus dem Bereich der Cybersicherheit bei der Planung, Errichtung und dem Betrieb der IT-Infrastrukturen berücksichtigt. Die Freie und Hansestadt Hamburg nutzt die Leistungen des ISMS von Dataport bedarfsgerecht auch für die Absicherung ihrer Infrastrukturen und Verfahren im Rahmen der Auftragsdatenverarbeitung.

4. Bestehen eine Kooperation oder mehrere zwischen der FHH und Unternehmen in Hamburg bezüglich der Zusammenarbeit im Bereich der Beratung und/oder zum Schutz vor Cyberangriffen?

Wenn ja, mit welchen Unternehmen und welchem Inhalt und Umfang?

Wenn nein, warum nicht?

Nein.

5. Sind in Dienststellen der FHH, zum Beispiel den Kundenzentren der Bezirke, Informationsmaterialien des BSI zum Thema Cybersicherheit zu erhalten?

Wenn ja, welche und in welchen Dienststellen?

Wenn nein, warum nicht?

Für die Dienststellen der BIS siehe Antwort zu III. 6.

Das Jugendinformationszentrum (JIZ) bietet jungen Menschen im Informationsladen ein umfängliches Angebot an Infomaterialien zu Themen an, die für sie von Interesse sind. Im Rahmen der Zuständigkeit für Fragen des gesetzlichen Jugendmedienschutzes und der Medienkompetenzförderung werden auch Infomaterialien zu den Risiken und Chancen der Internetnutzung bereitgehalten.

Außerdem bietet die Hamburger Volkshochschule unterschiedliche Kurse zum Thema Cybersicherheit an (zum Beispiel Rechtsicherheit im Internet, Download und Sicherheit beim Surfen, Sicherheit in lokalen Netzwerken).

Im Übrigen: Nein, da die Sensibilisierung der Bürgerinnen und Bürger in Sachen Cybersicherheit nicht zu den Kernaufgaben der Bezirksverwaltung gehört.

6. Inwieweit informiert der Senat beziehungsweise die zuständige Behörde über das Thema Cybersicherheit? Bitte nach Informationsangebot, Zielgruppe und Umfang, sowie gegebenenfalls mit Kosten angeben.

Die Polizei informiert in den örtlichen Polizeikommissariaten. Darüber hinaus informiert die Polizei seit 2007 unter dem Gesichtspunkt von Prävention und Opferschutz über „Sicherheit in den Neuen Medien“ und ist mit diesem Thema auf Verbrauchermessen, Sicherheitstagen und Ähnlichem und auch im Rahmen von Vorträgen vertreten. Bestandteil dessen sind beispielsweise Präventionsmedien aus dem bundesweiten Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) wie „Sicherung von Hardware gegen Diebstahl und unbefugte Nutzung“ (November 2012), „Vorauszahlungsbetrug/betrügerische Angebote im Internet, überzahlte Schecks, „Nigeria-Briefe““ (Oktober 2011) und eigene Veröffentlichungen wie „Sicherheit für Hamburger Unternehmen“ (November 2012).

Für das LfV siehe Antwort zu III. 7. Im Übrigen: nein.

7. Welche Angebote bietet der Senat beziehungsweise die zuständige Behörde der Industrie, insbesondere den kleinen und mittelständischen Unternehmen, an, um sich vor Cyberangriffen, Cyberspionage und vor Cyberkriminalität zu schützen?

Die Polizei steht mit ihrem allgemeinen kriminalpolizeilichen Beratungsangebot sowohl der Allgemeinheit als auch der Industrie oder mittelständischen Unternehmen zur Verfügung. Insbesondere Unternehmen werden hinsichtlich des Zusammenspiels von personellen, organisatorischen und technischen Rahmenbedingungen und über mögliche Schwachstellen beraten. Dabei steht bei der Betrachtung des Phänomens „Cybercrime“ der technische Aspekt im Vordergrund.

Das LfV bietet den Unternehmen zum Schutz vor Wirtschaftsspionage ein umfassendes Informations- und Beratungsangebot an. Im Übrigen siehe Drs. 20/5503.

a) Welche Seminare, Schulungen, Kurse oder Lehrgänge bieten die zuständigen Behörden an? Welchen zeitlichen Umfang haben diese jeweils und mit welchen Kosten müssen die Teilnehmer jeweils rechnen?

Der Senat bietet keine festen Seminare, Schulungen, Kurse oder Lehrgänge an. Im Übrigen siehe Antworten zu III. 6. und III. 7.

b) Wie viele Stellen und wie viele Beschäftigte halten jeweils welche Behörden für die Beratung und die Schulung zum Schutz vor Cyberangriffen, Cyberspionage und vor Cyberkriminalität vor?

In der Projektgruppe BOS Digitalfunk beschäftigt sich ein Mitarbeiter mit den für die Mitarbeiterinnen und Mitarbeiter wesentlichen Fragen zum Thema Cyberkriminalität als ein Teil seines Aufgabenfeldes.

Im Übrigen siehe Drs. 20/5503.

c) Was für Publikationen hält der Senat beziehungsweise die zuständige Behörde vor, um vor Cyberangriffen, Cyberspionage und vor Cyberkriminalität zu warnen und um Hinweise zum Schutz vor Cyberangriffen, Cyberspionage und vor Cyberkriminalität zu geben?

Die Polizei stellt die Broschüre „Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime“ zur Verfügung, die auch in elektronischer Form über die Internetpräsenz der Polizei Hamburg verfügbar ist. Im Übrigen siehe Antworten zu III. 5. und 6.

Für das LfV siehe Antwort zu III. 5. Im Übrigen siehe Drs. 20/5758.

Die BDBOS führt regelmäßig eine Awareness-Kampagne zur IT-Sicherheit durch und stellt den Mitarbeitern der BDBOS Informationsmaterial zur Verfügung. Aufgrund ihres gesetzlichen Aufgabenbereiches sowie des gesetzlich beschränkten Nutzerkreises des Digitalfunks BOS stellt die BDBOS keine Publikationen für Dritte zum Thema Schutz vor Cyberangriffen, Cyberspionage und Cyberkriminalität bereit.

d) Bieten die zuständigen Behörden Beratungsgespräche an?

Wenn ja, welche, in welcher Häufigkeit und von wem werden diese Beratungsgespräche jeweils in Anspruch genommen? Wie viele Beratungsgespräche wurden in den Jahren 2010, 2011 und 2012 geführt? Bitte nach Jahren und Arten gliedern.

Wenn nein, warum nicht?

Die zuständigen Behörden führen keine entsprechende Statistik.

Im Rahmen des Informations- und Beratungsangebotes Wirtschaftsschutz bietet das LfV Hamburg Beratungsgespräche an. Die für eine Beantwortung der Frage nach der Anzahl und Art der Beratungsgespräche im Zeitraum 1. Januar 2010 bis Mai 2013 über die Nutzung der genannten Angebote erforderlichen Zahlen hat das LfV nicht statistisch erfasst.

Insofern müsste das LfV insgesamt 371 Akten händisch auf durchgeführte Beratungsgespräche durchsehen. Dies ist in der für die Bearbeitung dieser Großen Anfrage zur Verfügung stehenden Zeit vollumfänglich nicht leistbar. Das LfV hat sich daher auf eine händischen Auswertung auf den Zeitraum 1. Januar 2012 bis 7. Mai 2013 beschränkt. Im Jahr 2012 wurden

- 38 Sensibilisierungsgespräche mit Sicherheitsverantwortlichen oder den Geschäftsführungen, davon elf Gespräche mit Geheimschutzberatungen, geführt sowie fünf Informations- und Vortragsveranstaltungen für Mitarbeiterinnen und Mitarbeiter eines Unternehmens und 16 Informations- und Vortragsveranstaltungen im Rahmen von Multiplikatoren-Veranstaltungen durchgeführt.

Im Zeitraum 1. Januar 2013 bis 7. Mai 2013 wurden

- 22 Sensibilisierungsgespräche mit Sicherheitsverantwortlichen oder Geschäftsführungen, davon 17 Gespräche mit Geheimschutzberatungen, geführt sowie zwei Informations- und Vortragsveranstaltungen für Mitarbeiterinnen und Mitarbeiter eines Unternehmens und zehn Informations- und Vortragsveranstaltungen im Rahmen von Multiplikatoren-Veranstaltungen durchgeführt.

e) Welche Kosten fallen für den jeweiligen Ratsuchenden an?

Keine.

8. Welche Angebote bietet der Senat beziehungsweise die zuständige Behörde der Industrie, insbesondere den kleinen und mittelständischen Unternehmen, an, wenn diese angegriffen wurden?

Für den Bereich der Polizei siehe Antwort zu III. 9.

Für das LfV siehe Antworten zu I. 2. und I. 3. sowie III. 6. und III. 7. Im Übrigen siehe Drs. 20/5503. Darüber hinaus: keine.

9. Wie viele Stellen und wie viele Beschäftigte halten jeweils welche Behörden für die Unternehmen, die angegriffen wurden, vor?

Das allgemeine kriminalpolizeiliche Beratungsangebot der Polizei ist präventiv ausgerichtet. Jedes Unternehmen kann sich aber auch nach einem Cyberangriff an die Polizei wenden, um für die Zukunft Vorsorge treffen zu können. Im Übrigen siehe Antworten zu I. 2., III. 7. und III. 7. b).

Für das LfV: siehe Drs. 20/5503.

IV. Strategien und Schutz

1. Welche Strategie verfolgt der Senat beziehungsweise die zuständige Behörde in Bezug auf die Abwehr von Cyberangriffen auf die IT-Netze der FHH, insbesondere auf die der Sicherheitsbehörden?

Zur Abwehr von Cyberangriffen werden sowohl technische als auch organisatorische Maßnahmen getroffen. Konkret wurde mit dem Inkrafttreten der IS-LL ein Informationssicherheitsmanagementsystem aufgebaut, welches sich an IT-Grundschutz anlehnt. Die Mitarbeiterinnen und Mitarbeiter werden schrittweise für das Thema Cybersicherheit sensibilisiert, da die Erfahrung zeigt, dass auch dort ein großer Angriffsvektor für Cyberkriminelle besteht. Durch die Errichtung neuer Rechenzentren bei Dataport wird eine nach IT-Grundschutz zertifizierte Infrastruktur aufgebaut und betrieben, die noch größeren Schutz vor Angriffen bietet.

Im Übrigen siehe Vorbemerkung.

2. Welche Strategie verfolgt der Senat beziehungsweise die zuständige Behörde in Bezug auf die Abwehr von Cyberangriffen auf die IT-Netze der Versorgungsunternehmen?

HAMBURG WASSER hat die Angriffsflächen für Cyberattacken durch Entkoppelung der Trinkwasserproduktionsprozesse vom Internet, Reduzierung der Administratorenrechte und Freiheitsgrade der Computer-Konfiguration sowie konsequente Firewall-Strategien reduziert. Ein Schwerpunkt der Abwehrstrategie liegt auf dem Schutz der

Server und Netzwerkverbindungen, die aus Sicherheitsgründen hier nicht genauer dargelegt werden (siehe Antwort zu III. 2 c)).

3. Welche Strategie verfolgt der Senat beziehungsweise die zuständige Behörde in Bezug auf die Abwehr von Cyberangriffen gegen Unternehmen?

Die Abwehr von Cyberangriffen liegt nach Auffassung der zuständigen Behörde in erster Linie in der Eigenverantwortung der Unternehmen. Im Übrigen siehe Antwort zu III. 7. Polizei und LfV bieten den Unternehmen kostenfrei Beratungen an.

Im Übrigen siehe für das LfV Drs. 20/5758.

4. Welche Schutzziele hat der Senat beziehungsweise die zuständige Behörde zum Thema Cyberangriffe?

Die Schutzziele entsprechen den Vorgaben des BSI.

5. Welche Einsatzkonzepte und Abwehrpläne hat der Senat beziehungsweise die zuständige Behörde im Fall eines Cyberangriffs? Wie sind in diese Pläne/Konzepte die öffentlichen Versorgungsunternehmen, die Verkehrsbetriebe und das Gesundheitssystem eingebunden und welche Rolle füllen sie dabei aus?

6. Welche Vorkehrungen hat der Senat beziehungsweise die zuständige Behörde getroffen für den Fall eines Cyberangriffes, insbesondere auf die FHH und/oder die öffentlichen Versorgungsunternehmen?

Die Einsatzkonzepte zur Abwehr von Cyberangriffen sind Bestandteil des Betriebs der IT-Infrastruktur der FHH. Sie liegen in Form von Notfallkonzepten und Einsatzplänen bei Dataport vor. Öffentliche Versorgungsunternehmen, Verkehrsbetriebe und Gesundheitssysteme sind in diese Konzepte nicht eingebunden. Diese betreiben ihre eigene IT-Infrastruktur und haben entsprechende Sicherheits-Krisenmanagement-maßnahmen implementiert.

Bei einem Ereignis im Umfeld des Einsatzlenkungssystems von Polizei und Feuerwehr werden die zu treffenden Maßnahmen durch die Polizei vorgegeben. Im Fall einer Eigenentdeckung wird der Vorgang umgehend an das InSiMa oder die zuständige Stelle bei der Polizei (Einsatzlenkungssystem) gemeldet und die zu treffenden Sofortmaßnahmen entsprechend abgestimmt. Weiter gehende Pläne bestehen bei der Feuerwehr nicht.

Die BDBOS baut gegenwärtig ein entsprechendes Informations-Sicherheitsmanagement und Notfallmanagement für das BOS-Digitalfunknetz auf.

7. 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?

Siehe grundsätzliche Anmerkungen zu IV. 5.

Seitens der Feuerwehr gibt es verschiedene Einsatzpläne und Rollen, um auf den Ausfall technischer Infrastruktur zu reagieren.

Die Polizei hat eine mehrstufige technische Vorsorge getroffen, um bei einem Angriff auf die IT-Systeme sicherzustellen, dass polizeiliche Daten einschließlich des gemeinsamen Einsatzlenkungssystems mit der Feuerwehr nicht eingesehen werden und abfließen können. Dadurch ist die Funktionsfähigkeit der Polizei dauerhaft gewährleistet ist. Darüber hinaus siehe Vorbemerkung und Antwort zu I. 1.

Im Rahmen des Aufbaus des Notfallmanagements für das BOS-Digitalfunknetz werden diese Szenarien betrachtet.

Die durch die BIS betriebene Netzinfrastruktur für die Belange des Katastrophenschutzes ist als „Worst-case-Szenario“ zu verstehen. Als isolierte IT-Struktur ist sie nicht Bestandteil des Cyberraumes und insoweit weitestgehend geschützt gegen Cyberangriffe.

8. Ist das BSI in die Abwehrpläne der jeweiligen Behörde eingebunden?

Wenn ja, wie und in welchem Umfang?

Wenn nein, warum nicht?

Bisher bestand diesbezüglich keine Notwendigkeit. Bei Bedarf wird das BSI in einem abgestuften Verfahren vornehmlich über Dataport in die Abwehr von Cyberangriffen einbezogen.

Die BDBOS arbeitet bei ihrer Planung eng mit dem BSI zusammen und berücksichtigt bei ihren Maßnahmen wesentlich die von dortiger Seite vorgegebenen Standards.

9. Hat der Senat beziehungsweise die zuständige Behörde ein Konzept bezüglich einer sicheren Kommunikation der Behörden und Organisationen mit Sicherungsaufgaben (BOS; Funk, Mobiltelefon, Mailverkehr, Videokonferenzen/-übertragungen, Alarmierungstechniken), welches vor Cyberangriffen geschützt ist?

Wenn ja, welches und welchen Dienststellen und Organisationen steht es seit wann zur Verfügung?

Wenn nein, warum nicht?

Aufgrund der großen Abhängigkeit der Feuerwehr und Polizei von einer funktionierenden Kommunikation bestehen seit jeher Bestrebungen, Rückfallstufen zu betreiben beziehungsweise auf unterschiedliche technische Plattformen zurückgreifen zu können. Eine detaillierte Systembeschreibung ist an dieser Stelle aufgrund der Vertraulichkeit nicht möglich. Genutzt werden folgende Technologien/Systeme:

- FHHNET (Datennetz)
- FHH-Telefonnetz
- Telefonnebenstellenanlagen
- Telefonanschlüsse privater Anbieter
- Mobiltelefone (unterschiedliche Vertragspartner)
- Mobile Datenübertragung mittels unterschiedlicher Standards und mit unterschiedlichen Vertragspartnern
- Digitalfunk TMO (Trunk Mode Operation)
- Digitalfunk DMO (Direct Mode Operation)
- Analogfunk 4 m
- Analogfunk 2 m

Sämtliche Kommunikationsmittel und -wege der Polizei sind so ausgelegt, dass sie nach jeweils technisch aktuellem Stand nicht durch Cyberangriffe gefährdet werden können.

Das LfV nutzt zur Erfüllung seiner gesetzlichen Aufgaben voneinander separierte Infrastrukturen und Netzzugänge.

Dabei handelt es sich einerseits, als Teil der hamburgischen Verwaltung, um das FHH-Netz. Für dieses Netz gelten die durch die Finanzbehörde für die Freie und Hansestadt Hamburg festgelegten Regularien.

Vor dem Hintergrund der besonderen Anforderungen des Geheim -und Datenschutzes wird daneben von den Ämtern für Verfassungsschutz (BfV/LfV) ein besonders geschütztes Netz betrieben. Die Regularien dieses Netzes unterliegen der Geheimhaltung. Sie werden vom BSI in Zusammenarbeit mit den IT-GSV des Bundes und der

Länder festgelegt und überwacht. Dieses Netz ist zur Verarbeitung und Speicherung von Daten bis zum Verschlussgrad VS-Geheim zugelassen.

Die BDBOS errichtet und betreibt den Digitalfunk für die BOS. Dieser wurde entsprechend der bestehenden Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität konzipiert und wird entsprechend realisiert. Ein wesentlicher Vorzug des Digitalfunks BOS basierend auf dem Tetra-Standard ist unter anderem die Abhörsicherheit.

Der Tetra-Standard beinhaltet als Sicherheitsfunktion bereits eine Luftschnittstellenverschlüsselung. Diese schützt den Übertragungsabschnitt zwischen Endgerät und Basisstation und ist im Digitalfunk BOS immer aktiv. Für die wirksame netzweite abhörsichere Übertragung, die innerhalb der Netzinfrastruktur auch leitungsgebunden erfolgen kann, wird in Deutschland im Digitalfunk BOS zusätzlich die sogenannte Ende-zu-Ende-Verschlüsselung gemäß BSI-Spezifikation eingesetzt. Unabhängig von sämtlichen genutzten Übertragungswegen wird somit sichergestellt, dass der Informationsaustausch zwischen den Kommunikationspartnern im Digitalfunk BOS von Endgerät zu Endgerät verschlüsselt stattfindet. Bund und Länder haben sich darauf verständigt, die Ende-zu-Ende-Verschlüsselung flächendeckend einzusetzen. Die Ende-zu-Ende-Verschlüsselung ist mit Beginn des erweiterten Probebetriebes im Funktionsumfang des BOS-Digitalfunknetzes enthalten.

Sollten Cyberangriffe darauf abzielen, auch die Stromversorgung zu stören, dient eine vorgehaltene Notstromversorgung der Sicherstellung der Infrastruktur. Eine grundsätzliche Forderung an die Standorte des Digitalfunks BOS besteht daher darin, dass das BOS-Digitalfunknetz auch bei einem Ausfall der elektrischen Energieversorgung weiter betrieben werden kann. Dies ist in den Konzepten entsprechend berücksichtigt. Die FHH legt fest, auf welche Art die Versorgung der Basisstation über eine Unterbrechungsfreie Stromversorgung (USV-Anlage) hinaus sichergestellt wird und realisiert die Lösung im Rahmen ihrer Verantwortlichkeit.

Die von der BIS betriebene Netzinfrastruktur für die Belange des Katastrophenschutzes verbindet als isolierte IT-Infrastruktur die Leitstellen beziehungsweise Krisenstäbe der beteiligten Dienststellen miteinander. Somit sind innerhalb des autarken Netzwerkes Datenkommunikation, Videokonferenz und Mailverkehr zwischen den angeschlossenen Dienststellen (Zentraler Katastrophendienststab der BIS, Polizei, Feuerwehr, Fachbehörden und -ämter sowie Bezirksämter, Hamburg Port Authority und das Landeskommando Hamburg der Bundeswehr) möglich.

V. Forschung und Entwicklung

1. Ist die FHH im Bereich der Forschung und Entwicklung zum Schutz vor Cyberangriffen tätig beziehungsweise beteiligt?

Wenn ja, welche Dienststelle/Organisation ist mit welchem Auftrag an der Forschung und/oder Entwicklung zum Schutz vor Cyberangriffen mit welchem Ziel und Aufwand (Personal, Material, Kosten) beteiligt?

Wenn nein, warum nicht?

Die Universität Hamburg (UHH), die Technische Universität Hamburg-Harburg (TUHH) und die Hochschule für Angewandte Wissenschaften Hamburg (HAW) sind mit Einzelprojekten in Forschung und Entwicklung zum Schutz vor Cyberangriffen tätig. Dies erfolgt nur zum Teil über Auftragsforschung, ein Großteil der Forschung erfolgt durch Mittel der FHH über die Grundfinanzierung der Hochschulen. Die Hochschulen führen dazu folgendes aus:

UHH

- Der Arbeitsbereich „Sicherheit in Verteilten Systemen“ am Fachbereich Informatik der Universität Hamburg ist derzeit an keinen Projekten mit dem konkreten Ziel „Schutz vor Cyber-Angriffen“ beteiligt. Jedoch wird sowohl Grundlagenforschung zur IT-Sicherheit und zum technischen Datenschutz in verteilten Systemen als auch anwendungsorientierte Forschung in den Bereichen mobile Sicherheit und Sicherheitsmanagement durchgeführt. Die Forschungsergebnisse dienen mittelbar

auch dem Schutz vor Cyberangriffen und bringen dieses Thema auch in die universitäre Lehre ein.

TUHH

- Auftragsforschung, zum Beispiel ein Unternehmen beauftragt die Entwicklung einer Sicherheitsmaßnahme, wird an der TUHH nur in Einzelfällen durchgeführt. Im Jahr 2012 war die TUHH an einem Entwicklungsprojekt für Airbus beteiligt, das die Sicherheit der IT-Infrastruktur in Flugzeugkabinen zum Inhalt hatte. Der Auftragswert betrug 100.000 Euro.

HAW mit derzeit folgenden fünf Forschungsprojekten:

- Cyber Threat Assessment; Fakultät Technik und Informatik – Department Informatik; Ziel ist die Analyse der Risiken für nationale kritische Infrastrukturen durch IT-Bedrohungen; der Aufwand wird über Fördersumme abgegolten, Fördersumme: 50.000 Euro.
- SKIMS: Schichtenübergreifendes kooperatives Immunsystem für mobile, mehrseitige Sicherheit; TI/Department Informatik – AG Internet Technologies; Ziel ist die Erhöhung der Sicherheit auf Mobilgeräten (Smartphones); Aufwand: 1,5 Mitarbeiter und Ausstattung für drei Jahre; Fördersumme: 290.470 Euro.
- SMARTPower Hamburg; TI/Department Informatik – AG Internet Technologies; Ziel ist die Datensicherheit und Schutz der Privatsphäre in Smart Grids; Aufwand: 0,5 Mitarbeiter für drei Jahre; Fördersumme: 120.000 Euro.
- Verbundprojekt Safest: Social-Area Framework for Early Security Triggers at Airports – Teilvorhaben: Ende-zu-Ende-Sicherheit für die Flughafensensorik durch intelligente Kommunikation; TI/Dept Informatik – AG Internet Technologies; Ziel ist die Erhöhung der zivilen Sicherheit durch intelligente Sensorik an öffentlichen Plätzen; Aufwand: zwei Mitarbeiter und Ausstattung für drei Jahre; Fördersumme: 530.700 Euro.
- Peeroskop: Peering-Monitor und mikroskopische Analyse zum Schutz des deutschen Internets – Teilprojekt: Landesspezifische Internet-Kartografierung und Angriffssicherung; TI/Department Informatik – AG Internet Technologies; Ziel: Analyse und Überwachung des Internet-Backbones in Deutschland zur Entdeckung und Abwendung von Cyberattacks; Aufwand: ein Mitarbeiter und Ausstattung für drei Jahre; Fördersumme: 323.502 Euro.

2. Hat die FHH in Zukunft vor, sich an der Forschung und Entwicklung zum Schutz vor Cyberangriffen zu beteiligen?

Wenn ja, wann und mit welcher Einrichtung und welchem Ziel und Aufwand?

Wenn nein, warum nicht?

Ja. So beabsichtigt zum Beispiel der Arbeitsbereich „Sicherheit in Verteilten Systemen“ am Fachbereich Informatik der UHH die Gründung eines Zentrums für IT-Sicherheit und Datenschutz an der Universität Hamburg, unter anderem um die notwendige fächerübergreifende Forschung zum Thema Cybersecurity in Hamburg weiter voranzubringen. Im Rahmen der Lehre wird der Fachbereich Informatik der Universität Hamburg im Wintersemester 2013 zusammen mit dem Zentrum für Naturwissenschaft und Friedensforschung (ZNF) und dem Institut für Friedensforschung und Sicherheitspolitik (IFSH) die „Carl Friedrich von Weizsäcker Friedensvorlesung“ zum Thema Cybersecurity mit hochrangigen Vortragenden veranstalten.

3. Unterstützt die FHH die Forschung und Entwicklung zum Schutz vor Cyberangriffen?

Wenn ja, welche Organisation und/oder welches Unternehmen wird mit welchem Ziel und Aufwand (Personal, Material, Kosten) unterstützt?

Wenn nein, warum nicht?

4. Hat die FHH in Zukunft vor, die Forschung und Entwicklung zum Schutz vor Cyberangriffen zu unterstützen?

Wenn ja, wann und welche Organisation/welches Unternehmen mit welchem Ziel und Aufwand?

Wenn nein, warum nicht?

Die für Wissenschaft und Forschung zuständige Behörde hat keine speziellen Förderprogramme für Forschung und Entwicklung zum Schutz vor Cyberangriffen aufgelegt und plant auch nicht, dies zu tun. Sie fördert die Forschung an den staatlichen Hamburger Hochschulen über deren Grundfinanzierung. Im Rahmen der grundständigen Forschung können auch die in der Frage genannten Themen durch die Hochschulforschung aufgegriffen werden.

5. Welche hamburgischen Hochschulen sind derzeit an der Forschung und Entwicklung zum Schutz vor Cyberangriffen tätig beziehungsweise forschen in diesem Bereich? Wie werden diese durch den Senat gefördert?

In Ergänzung zu den Antworten zu V. 1. haben die UHH und die TUHH folgende weiteren Angaben gemacht. Fasst man „Schutz vor Cyberangriffen“ etwas allgemeiner als „Sicherheit und Schutz von informationstechnischen Systemen“, finden sich an der UHH Forschungsaktivitäten am Arbeitsbereich „Sicherheit in Verteilten Systemen“ und am DFN-CERT (Deutsches Forschungsnetz – Computer Emergency Response Team).

Die TUHH ist mit einem Institut (Sicherheit in verteilten Anwendungen) an Forschung und Entwicklung zum Schutz vor Cyberangriffen beteiligt. Darüber hinaus befassen sich an der TUHH weitere Institute im Zusammenhang mit IT-Projekten, die einen anderen Fokus haben, am Rande auch mit Fragen der Cybersicherheit. Eine Themenstellung war zum Beispiel die Zugangssicherheit zu Flugzeugsystemen, an der insgesamt vier Institute der TUHH zusammen mit einem Unternehmen der Branche arbeiteten. Der Wert dieses Projekts betrug 210.000 Euro.

Die Einrichtungen erhalten, über die Grundfinanzierung der Hochschulen hinaus, keine direkte Förderung der FHH für Forschung und Entwicklung zum Schutz vor Cyberangriffen.

6. Welche hamburgischen Unternehmen sind derzeit an der Forschung und Entwicklung zum Schutz vor Cyberangriffen tätig beziehungsweise forschen in diesem Bereich? Wie werden diese durch den Senat gefördert?

Im Programm für Innovation werden zwei Unternehmen mit Projekten durch Gewährung von Zuwendungen gemäß den Richtlinien zur Förderung von Forschungs- und Entwicklungsvorhaben Hamburger Unternehmen gefördert, die dem Thema Cybersicherheit zugeordnet werden können: gateprotect AG und Ernst Sicherheits- und Kommunikationstechnik GmbH.