BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
22. Wahlperiode

Drucksache 22/9253
13.09.22

Schriftliche Kleine Anfrage

des Abgeordneten Sami Musa (fraktionslos) vom 05.09.22

und Antwort des Senats

Betr.: Änderung der Bedrohungslage der Cybersicherheit

Einleitung für die Fragen:

Am 12. Juli 2022 hat die deutsche Bundesinnenministerin ihre „Cybersicherheitsagenda" vorgestellt: Der Angriffskrieg Russlands auf die Ukraine habe die Bedrohungslage vor dem Hintergrund einer sich ohnehin kontinuierlich verschärfenden Cyberbedrohung zusätzlich zugespitzt, erfordere eine strategische Neuausrichtung und damit auch erhöhte Investitionen in die Cybersicherheit unseres Landes. Zu diesem Zweck soll das „Bundesamt für Sicherheit in der Informationstechnik" (BSI) zu einer Zentralstelle im Bund-Länder-Verhältnis, also zu einer „Art BKA" für die Cybersicherheit ausgebaut werden. Dies ziehe auch eine föderale Neuregelung und eine neue Zuordnung der Aufgabenverteilung zwischen Bund und Ländern nach sich. Zu diesem Zweck soll die Zentralstellenfunktion des Bundesamtes für Verfassungsschutz im Verfassungsschutzbund ausgebaut und gestärkt werden. Hierfür möchte die Bundesinnenministerin Nancy Faeser einen neuen gesetzlichen Rahmen schaffen. Sie strebt eine Grundgesetzänderung an, um damit einen größeren Teil der Verantwortung für Cybersicherheit in Bundesverantwortung zu belassen.

Neben der Zunahme von Straftaten, denen einzelne Personen oder Unternehmen zum Opfer fallen, muss der Schutz der sogenannten Kritischen Infrastrukturen aktuell bei politischen Entscheidungsträgern dringend in den Fokus gerückt werden. Gerade mit dem Angriffskrieg Russlands auf die Ukraine ist das Schutzbedürfnis der Kritischen Infrastrukturen offensichtlich geworden. So meldete die Tagesschau am 13. April 2022, dass die Ukraine einen erneuten Cyberangriff auf die Energieversorgung des Landes abwehren konnte. Im Kontext dieser Meldung wurde auch darauf hingewiesen, dass auch Kritische Infrastrukturen in der Bundesrepublik Deutschland für die gegen die Ukraine eingesetzte Schadsoftware anfällig sein könnten. Als Beispiel kann hier die Störung der Fernwartung von über 5.800 Windkraftanlagen seit dem 24. Februar 2022, dem Tag des russischen Angriffs auf die Ukraine, genannt werden. Mutmaßlich hatten russische Hacker das Satellitennetzwerk angegriffen, über das unter anderem mit den Windkrafträdern kommuniziert wird.

Vor diesem Hintergrund frage ich den Senat:

Einleitung für die Antworten:

Der Cyberraum bietet ein weites Feld für die Vorbereitung und Durchführung von Spionage- oder Sabotageaktivitäten. Die Ausforschung und Instrumentalisierung der eigenen Internet-Infrastruktur durch fremde Nachrichtendienste stellt für Unternehmen, Forschungseinrichtungen, Behörden oder auch Privatpersonen eine hohe, konstant zunehmende Gefährdung dar. Im Jahr 2021 schätzte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Lage der deutschen IT-Sicherheit als „besorgniserregend" ein.

Die Cyber-Spionageabwehr des Landesamtes für Verfassungsschutz (LfV) Hamburg ist für die Aufklärung und Abwehr von Aktivitäten im Cyberraum zuständig, die ausschließlich der Cyberspionage und -sabotage mit mutmaßlich staatlich-nachrichtendienstlichem oder extremistischem Hintergrund zuzuordnen sind. Die Bekämpfung der Cyberkriminalität, der Schutz der Behördennetze und der Schutz Kritischer Infrastrukturen (KRITIS) einschließlich ihrer IT-Infrastruktur sind nicht Teil der gesetzlich geregelten Aufgaben des LfV Hamburg.

Cyberaktivitäten mit mutmaßlich staatlich-nachrichtendienstlichem Hintergrund können in tatsächlich durchgeführte Angriffe zum Zweck der Ausspähung beziehungsweise der Ausleitung von Daten (Cyberspionage) oder zur Störung der Netze und Arbeitsprozesse (Cybersabotage) einerseits und vorbereitende beziehungsweise ausforschende Aktivitäten (zum Beispiel sogenanntes Port Scanning), die der Planung eines solchen Cyberangriffs dienen beziehungsweise die Suche nach einem geeigneten Ziel unterstützen, andererseits eingeteilt werden. Es liegt in der Natur derartiger Cyberaktivitäten, dass sie möglichst lange unentdeckt bleiben sollen. Dies erschwert die zeitnahe Erkennung beziehungsweise Attribution des Angriffes zu einem bestimmten Land oder fremden Nachrichtendienst durch die Verfassungsschutzbehörden. Im Sinne der nachrichtendienstlichen Aufklärung der Cyberaktivitäten erfolgt die Zusammenarbeit des LfV Hamburg mit Zielen mutmaßlich staatlich gesteuerter Cyberangriffe grundsätzlich immer auf vertraulicher Basis.

Dies vorausgeschickt, beantwortet der Senat die Fragen wie folgt:

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

Antwort zu Frage 1:

Kritische Infrastrukturen sind gemäß KRITIS-Strategie des Bundes „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." (BMI, 2009).

Ein ebenen-, sektor- und gefahrenübergreifendes „Gesetz zum Schutz Kritischer Infrastrukturen" gibt es in Deutschland nicht. Dennoch gibt es sektorspezifische Hinweise auf eine Systemrelevanz der Funktionsfähigkeit zur Sicherstellung der Versorgung der Bevölkerung. Die Freie und Hansestadt Hamburg (FHH) nimmt gemäß der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) folgende Einteilung vor:

- Energie: Elektrizität, Gas, Mineralöl, Fernwärme (§ 2),
- Wasser: öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung (§ 3),
- Ernährung: Ernährungswirtschaft, Lebensmittelhandel (§ 4),
- Informationstechnik und Telekommunikation (§ 5),
- Gesundheit: medizinische Versorgung, Arzneimittel und Impfstoffe, Labore (§ 6),
- Finanz- und Versicherungswesen: Kreditinstitute, Börsen, Versicherungen, Finanzdienstleister (§ 7),
- Transport und Verkehr: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik (§ 8).

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

Antwort zu Frage 2:

Nach dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme gehören zukünftig folgende Unternehmen und Zulieferer zu der Kategorie „Unternehmen im besonderen öffentlichen Interesse" (UBI):

- Hersteller von Rüstung und Produkten für staatliche Verschlusssachen (VS), da deren Ausfall Sicherheitsinteressen Deutschlands gefährden würde,

- Unternehmen von erheblicher volkswirtschaftlicher Bedeutung, weil Störungen gesamtgesellschaftliche Bedeutung hätten,
- Betreiber Betriebsbereiche der oberen Klasse mit gefährlichen Stoffen – Chemie und produzierende Industrie nach der Störfall-Verordnung.

Zu den Unternehmen von erheblicher volkswirtschaftlicher Bedeutung gehören auch Zulieferer, wenn sie für die oben genannten Unternehmen von wesentlicher Bedeutung sind.

Konkret wenden sich Unternehmen zur Prüfung ihrer Eigenschaft als Kritische Infrastruktur nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) in Verbindung mit §§ 2 bis 8 der BSI-Kritisverordnung (BSI-KritisV) direkt an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Frage 3: *Von wie vielen Cyberattacken im Land Hamburg hat der Senat im Zeitraum von Januar 2019 bis Juni 2022 Kenntnis erhalten?*

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

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

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

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

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

f) Wie lange war die Wirkdauer der jeweiligen Angriffe?

g) Welche Störungen wurden jeweils durch die Angriffe verursacht?

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

Antwort zu Fragen 3 bis 3 h):

Statistische Daten im Sinne der Fragestellung werden nicht zentral erfasst.

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

Antwort zu Frage 4:

Der russische Angriffskrieg auf die Ukraine erhöht das Risiko für Cyberangriffe mutmaßlich russischen Ursprungs gegen deutsche und hamburgische Einrichtungen. Die intensivierte Unterstützung der Ukraine und die umfassende Sanktionierung Russlands durch die Bundesregierung können zu verstärkter Cyberspionage und Cybersabotage führen.

Der Senat teilt daher die Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Demnach hat sich infolge des Russland-Ukraine-Krieges die Cyber-Bedrohungslage für Deutschland erhöht, was grundsätzlich auch für Kritische Infrastrukturen gilt. Generell ist festzustellen, dass sich die Angriffsmethoden stetig weiterentwickeln.

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

Antwort zu Frage 5:

Dataport hat als zentraler Dienstleister für die Infrastrukturen der Hamburger Verwaltung bereits im Jahr 2019 begonnen, im Zuge des Auf- und Ausbaus des Cyber-Defense-Centers eigene Expertise im Bereich „White Hacking“ und Penetrationstests aufzubauen und die Angriffserkennung auszubauen. Seit 2020 wurde eine Reihe von Penetrationstests durchgeführt. Seit 2021 steht auch ein Dienst zur Angriffssimulation bei Dataport zur Verfügung, der genutzt wird, um die intern ergriffenen, auf IT-Grundschutz basierenden Sicherheitsmaßnahmen auf Wirksamkeit zu überprüfen.

Im Übrigen haben die Betreiber Kritischer Infrastrukturen in der FHH für Cyberattacken entsprechende Notfallpläne vorgesehen, um einem Ausfall vorzubeugen. Diese orientieren sich an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik.

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

a) den Sicherheitsbehörden,

b) den Dienststellen der öffentlichen Verwaltung,

c) den öffentlichen Versorgungsunternehmen,

d) den öffentlichen Verkehrsunternehmen,

e) der in Hamburg angesiedelten Industrie und Wirtschaft sowie

f) den Hochschulen und Forschungsinstituten in Hamburg?

Antwort zu Fragen 6 a) bis 6 f):

Siehe Antwort zu 5.

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

Antwort zu Frage 7:

Aufseiten der FHH werden steuernde und ministerielle Aufgaben wahrgenommen. Die operativen Aufgaben wurden dem zentralen IT-Dienstleister übertragen. Die Ausstattung ist nach Einschätzung der zustehenden Behörden ausreichend, wird jedoch fortlaufend überprüft.

Im Übrigen siehe Vorbemerkung.

Frage 8: *Inwiefern werden diese Präventionsmaßnahmen regelmäßig einer Evaluation in Bezug auf ihre Wirksamkeit unterzogen?*

Antwort zu Frage 8:

Eine zentral gesteuerte, regelmäßige Evaluation im Sinne der Fragestellung erfolgt nicht.

Im Übrigen siehe Vorbemerkung.