BREMISCHE BÜRGERSCHAFT **Drucksache 20/1550**
Landtag **19.08.22**
20. Wahlperiode

Große Anfrage der Fraktion der FDP

Änderung der Bedrohungslage in der Cybersicherheit: Bremische IT in Großkrisenlagen

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.

Bereits 2018 hat die Fraktion der FDP in der Bremischen Bürgerschaft eine umfassende Große Anfrage zum Thema Cybersicherheit im Lande Bremen an den Senat gerichtet (Drucksache 19/1932), welche mit der Mitteilung des Senats vom 15. Januar 2019 an die Bürgerschaft (Landtag), (Drucksache 19/1993) beantwortet wurde. Seitdem ist die Digitalisierung unserer gesamten Gesellschaft erheblich fortgeschritten. Die Coronapandemie hat diese Entwicklung zusätzlich beschleunigt, indem Homeoffice, Onlineshopping und Videokonferenzen in der breiten Mitte der Gesellschaft zum Alltag gehören. Dadurch haben wir nicht allein eine Modernisierung unserer Lebens- und Arbeitswelt erreicht, sondern diese auch neuen Risiken ausgesetzt. So können wir zum Beispiel aus den polizeilichen Kriminalstatistiken ablesen, dass während der Coronapandemie die Zahl der Betrugsdelikte im Internet sowie die Erpressungen durch Ransomware weiter zugenommen haben.

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 fragen wir den Senat:

1. Welche Infrastrukturen im Land Bremen stuft der Senat als sogenannte Kritische Infrastrukturen ein? (Bitte sowohl private als auch staatliche Infrastrukturen aufzählen)
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?
3. Von wie vielen Cyberattacken im Land Bremen 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)?
4. Inwiefern hat sich nach Auffassung des Senats seit 2019 die Gefährdungslage für Kritische Infrastrukturen, Behörden und Unternehmen im Land Bremen Opfer von Cyberattacken zu werden, insbesondere auch vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine, verändert?
5. Welche zusätzlichen Maßnahmen sind seit 2019 ergriffen worden, um dem Ausfall kritischer Infrastrukturen, beispielsweise Strom-, Gas-, Fernwärme- und Wasserversorgung, durch Cyberattacken vorzubeugen?
6. Welche zusätzlichen Präventionsmaßnahmen zum Schutz vor Cyberattacken sind durch den Senat, beziehungsweise die jeweiligen Behörden, seit 2019 eingeführt und/oder verstetigt worden, insbesondere bei den
   a) Sicherheitsbehörden,
   b) Dienststellen der öffentlichen Verwaltung,
   c) den öffentlichen Versorgungsunternehmen,
   d) den öffentlichen Verkehrsunternehmen,
   e) der in Bremen angesiedelten Industrie und Wirtschaft sowie
   f) den Hochschulen und Forschungsinstituten in Bremen?
7. Wie sind die für die Cybersicherheit zuständigen Behörden im Land Bremen personell und finanziell ausgestattet? Ist diese Ausstattung im Angesicht der gegenwärtigen Bedrohungslage noch ausreichend, wenn ja, warum, wenn nein, wo muss mit welchen Geldern nachgebessert werden?
8. Inwiefern werden diese Präventionsmaßnahmen regelmäßig einer Evaluation in Bezug auf ihre Wirksamkeit unterzogen?
9. Inwieweit gibt es mittlerweile bei den zuständigen Behörden ein „Worst-Case-Szenario“ für Cyberattacken, insbesondere vor dem Hintergrund, dass im Jahr 2019 weder die Ortspolizeibehörde Bremen, noch die Feuerwehr Bremen im Besitz entsprechender Notfallpläne waren? Inwiefern

wurden entsprechende Abwehr- oder Einsatzpläne seit 2019 bei den anderen Behörden vor dem Hintergrund der veränderten Bedrohungslage angemessen angepasst? Inwiefern gibt es im Land Bremen weiterhin Behörden, die keine entsprechenden Abwehr- und Einsatzpläne haben?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Birgit Bergmann, Dr. Magnus Buhlert,
Lencke Wischhusen und Fraktion der FDP