LANDTAG
NIEDERSACHSEN

N i e d e r s c h r i f t

über die 10. - öffentliche - Sitzung

des Unterausschusses „Häfen und Schifffahrt“

des Ausschusses für Wirtschaft, Verkehr, Bauen und Digitalisierung

am 19. Dezember 2023

Hannover, Landtagsgebäude

Tagesordnung: Seite:

Anwesend:

Mitglieder des Unterausschusses:

1. Abg. Nico Bloem (SPD), Vorsitzender
2. Abg. Matthias Arends (SPD)
3. Abg. Oliver Ebken (SPD)
4. Abg. Marten Gäde (SPD)
5. Abg. Corinna Lange (SPD) (per Videokonferenztechnik zugeschaltet)
6. Abg. Karin Logemann (SPD) (per Videokonferenztechnik zugeschaltet)
7. Abg. Katharina Jensen (CDU) (per Videokonferenztechnik zugeschaltet)
8. Abg. Hartmut Moorkamp (CDU)
9. Abg. Melanie Reinecke (CDU)
10. Abg. Claus Seebeck (CDU)
11. Abg. Ulf Thiele (CDU)
12. Abg. Sina Maria Beckmann (GRÜNE) (per Videokonferenztechnik zugeschaltet)
13. Abg. Christian Schroeder (GRÜNE) (per Videokonferenztechnik zugeschaltet)

Von der Landtagsverwaltung:

Frau Stürzebecher.

Niederschrift:

Parlamentsredakteur Dr. Zachäus, Stenografischer Dienst.

Sitzungsdauer: 10.31 Uhr bis 11.05 Uhr

Außerhalb der Tagesordnung:

Billigung von Niederschriften

Der **Unterausschuss** billigt die Niederschrift über die 9. Sitzung einvernehmlich.

***

Tagesordnungspunkt 1:

Unterrichtungsantrag zur „Kollision von zwei Frachtschiffen am 24. Oktober 2023“

Antrag auf Unterrichtung der Fraktion der SPD vom 27. Oktober 2023

Vors. Abg. **Nico Bloem** (SPD) verweist auf die Unterrichtung des Umweltministeriums vom 1. November 2023 sowie die ergänzende E-Mail vom 6. Dezember 2023. Es sei der Hinweis erfolgt, dass erst nach Abschluss der Ermittlungen unterrichtet werden könne. Aus diesem Grund empfehle er, mit der Entgegennahme der Unterrichtung zu warten.

*

Der **Unterausschuss** beschließt einvernehmlich, dieser Empfehlung zu folgen.

***

Tagesordnungspunkt 2:

Unterrichtungsantrag zur „Resilienzfähigkeit der Niedersächsischen Häfen gegen Hackerangriffe“

Antrag auf Unterrichtung der Fraktion Bündnis 90/Die Grünen vom 17. November 2023

Der **Unterausschuss** billigt den Antrag auf Unterrichtung einvernehmlich.

Unterrichtung

MR **Jacob** (MW): Gerne komme ich der Bitte nach, über die Resilienzfähigkeit der niedersächsischen Häfen gegen Hackerangriffe zu unterrichten. Ich bitte vorab um Ihr Verständnis, dass zu konkreten Schutzmaßnahmen keine Informationen weitergegeben und offengelegt werden können, um die Prozesse in den Unternehmen nicht zu gefährden.

Landeseigene niedersächsische Hafengesellschaften

Die niedersächsischen Hafengesellschaften, die „Niedersachsen Ports GmbH & Co. KG“ (NPorts), die „Container Terminal Wilhelmshaven JadeWeserPort-Marketing GmbH & Co. KG“ (JWP-M) und die „JadeWeserPort Realisierungs GmbH & Co. KG“ (JWP-R), arbeiten eng zusammen und sind netzwerktechnisch in Teilen bereits verbunden, wobei die beiden letzteren sich eine gemeinsame IT-Infrastruktur teilen. Die IT-Infrastruktur ist völlig losgelöst von der des Landes. Das Unternehmen betreibt eine eigene Plattform und eigene Server. Alle Gesellschaften bieten keine physischen Umschlagleistungen an, sind als Terminaleigentümer aber in die Umschlagprozesse eingebunden. Die Sicherheitsmaßnahmen folgen den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Computer Emergency Response Teams der Niedersächsischen Landesverwaltung (N-CERT).

Beim JWP als Arbeitgeber des niedersächsischen Port Cyber Security Officers (PCSO) werden derzeit auch noch weitere Maßnahmen - quasi aus einer Vorbildfunktion heraus - umgesetzt. Wir haben den zuständigen Port Cyber Security Officer bei der JWP-M angesiedelt, die dabei federführend für alle drei Gesellschaften agiert. Der PCSO ist im ständigen Austausch mit den Sicherheitsbehörden - Niedersächsischer Verfassungsschutz, Landeskriminalamt, Bundesverfassungsschutz - und den Fachkollegen in den übrigen norddeutschen Häfen - Hamburg und Bremen seien hier benannt - sowie den zuständigen IT-Kollegen in den Häfen.

Neben einer redundant aufgebauten, modernen und ständig gewarteten Firewall verfügen die niedersächsischen Hafengesellschaften über einen wirksamen Spam- und Antivirusschutz sowie heuristische Erkennungsmaßnahmen von Schadsoftware und ihrer Aktivitäten. Als Dienstleister für Web-Services - unter anderem für NPorts - verfügen die redundanten Internetzugänge des JWP über einen leistungsfähigen DDoS-Schutz seitens des Providers.

NPorts und die JWP-IT weisen die Mitarbeiter zeitnah auf aktuelle Angriffsversuche hin und versuchen im persönlichen Gespräch die Aufmerksamkeit und die Wachsamkeit der Kolleginnen und Kollegen zu erhöhen. Beim JWP sorgt eine zentrale Softwareverteilung für ständige Updates der Betriebs- und Clientsoftware. NPorts verwendet Terminal-Server und kann so zentral die

Aktualität der Software sicherstellen. Für die E-Mail-Sicherheit verfügt jeder Mitarbeiter der JWP-Gesellschaften über eine persönliche Signatur über SwissSign und hat auch die Möglichkeit, Inhalte verschlüsselt zu übermitteln. Eine ausgefeilte Backup-Strategie ermöglicht die zeitnahe Wiederherstellung von Daten, Datenbankinhalten und ganzen Systemen an allen Standorten. Im Falle eines Cyberangriffs greifen die Notfallprozesse mit niedergeschriebenen Meldeketten und Maßnahmen.

Das zuständige Fachreferat aus dem MI - Referat 36 Katastrophenschutz, Kompetenzzentrum Großschadenslagen - hat uns darüber hinaus mitgeteilt, dass das MI kein Mandat zum Schutz der Cybersicherheit der Wirtschaft hat und es diesbezüglich auch keine besonderen Vorgaben gibt. Für die Cybersecurity von Unternehmen und Einrichtungen, die unter das BSI-Gesetz fallen, gelten die Anforderungen aus dem BSI-Gesetz und der BSI-Kritisverordnung. Laut MI - das ist uns aber auch bekannt - fallen die Häfen unter die KRITIS-Einstufung. Alle diesbezüglichen Informationen sind als „Verschlusssache - Nur für den Dienstgebrauch“ (VS-NfD) eingestuft. Die aktuellen Listen mit den Einrichtungskriterien wurden uns vom MI zur Verfügung gestellt und können bei uns im für den Datenschutz zuständigen Referat eingesehen werden. Ich habe sie für die heutige Unterrichtung nicht zur Verfügung gestellt bekommen.

Informationen der Hafensicherheitsbehörde

Dieser Aufgabenbereich treibt die Umsetzung der internationalen Regelungen für den Hafenzugang und der internationalen Hafensicherheitsvorschriften voran. Die Aufgaben der Hafensicherheitsbehörde bestehen in der Umsetzung von europäischen Verordnungen sowie Richtlinien, die im Kern einen rechtswidrigen Angriff auf Häfen bzw. Hafenanlagen verhindern sollen. Als Cyberangriff wird auch das widerrechtliche virtuelle Eindringen in eine Hafenanlage über deren IT angesehen.

Die hiesigen Seehäfen verfügen über keine anlagenübergreifenden Computersysteme. Erfolgreiche Hackerangriffe auf einzelne Hafenanlagen haben daher keine direkten Auswirkungen auf den gesamten Hafen. Jede Hafenanlage im Sinne des Niedersächsischen Hafensicherheitsgesetztes wird vor erstmaligem Anlauf eines Seeschiffes von der Hafensicherheitsbehörde einer umfangreichen Risikobewertung nach dem Hafensicherheitsgesetz unterzogen. Diese beinhaltet auch den Punkt Cybersecurity bzw. Cyberangriff. Aufgrund dieser Risikobewertung fertigt der oder die Beauftragte für die Gefahrenabwehr - der oder die PFSO - in der jeweiligen Hafenanlage den Gefahrenabwehrplan - den PFSP - an, welcher nach sorgfältiger Prüfung durch die Hafensicherheitsbehörde gemäß Hafensicherheitsgesetz genehmigt wird.

Die PFSP beinhalten im Kontext von Cybersecurity auszugsweise die Punkte Meldeverpflichtung an einschlägige Behörden, jährliche Unterweisungen/Schulungen der Beschäftigten, Einrichtung einer Firewall, redundante Datenspeicherung und auch eine IT-Benutzerordnung. Die Gefahrenabwehrpläne sind vor Offenlegung zu schützen. Die Einsichtnahme ist nur Personen mit einer Zuverlässigkeitsüberprüfung gestattet.

In jährlich stattfinden Audits wird die Einhaltung und Umsetzung dieser Gefahrenabwehrpläne durch die Hafenbehörde geprüft. Diese Audits beinhalten ebenfalls das Thema Cybersecurity.

Ein Ausfall von behördlichen computergestützten Systemen - zum Beispiel das National Single Window oder Thetis - würde die behördliche Kontrolle der Abläufe zwar erschweren, hätte aber auf den eigentlichen Umschlagbetrieb keine Auswirkungen.

Das Thema Cybersecurity ist fester Bestandteil der jährlich stattfindenden PFSO-Workshops - also Workshops für die Personen, die für die Gefahrenabwehr in den Häfen und auf den Terminals zuständig sind -, wo die Teilnehmenden auf entsprechende Schwachstellen und Risiken in den Hafenanlagen durch interne wie externe Fachreferenten sensibilisiert werden.

Auszugsweise möchte ich einzelne Maßnahmen im Falle eines Cyberangriffs darstellen.

- Zunächst sind die Vorfälle gemäß den Gefahrenabwehrplänen zu melden.

- Des Weiteren ist eine Vielzahl von präventiven Sicherheitsmaßnahmen in den Gefahrenabwehrplänen hinterlegt und genehmigt.

- In der Risikobewertung werden die Folgen und Auswirkungen eines Cyberangriffs analysiert, und gemeinsam mit dem entsprechenden Hafensicherheitsbetreuer - dem PFSO - wird nach zielführenden Abwehrmaßnahmen recherchiert.

- Bei einem möglichen externen Angriff würde durch die Hafensicherheitsbehörde dieses meldepflichtige Ereignis an die entsprechenden Behörden - zum Beispiel die Zentralen Ansprechstellen Cybercrime der Polizeien - kommuniziert. Alle anderen potenziell betroffenen Betriebe werden bedarfsgerecht ebenfalls in Kenntnis gesetzt.

- Die Gefahrenabwehrpläne beinhalten dementsprechend alle präventiven Maßnahmen zur Gefahrenabwehr in den Häfen bzw. in den Hafenanlagen.

- Bei der Bekämpfung von Cyberangriffen arbeitet die Hafensicherheitsbehörde sehr eng mit den zuständigen Ministerien und Behörden zusammen.

Unternehmen der AG Seehäfen

Wir haben in Vorbereitung des heutigen Termins über die AG Seehäfen und die Mitglieder dieser bei den entsprechenden Umschlagunternehmen angefragt. Soweit es hier veröffentlicht werden kann, haben diese uns mitgeteilt, dass einige der angefragten Unternehmen vom BSI als kritische Infrastruktur eingestuft wurden und dementsprechend gemäß BSI-Anforderungen aufgestellt sind. Andere Unternehmen fallen unter das Hafensicherheitsgesetz. Hierzu habe ich im vorherigen Abschnitt bereits erläutert. Details zur Umsetzung sind gemäß dem genannten Gesetz nicht öffentlich. Nach Aussage der Unternehmen können bei einem Cyberangriff die Umschlagaktivitäten weitestgehend autark durchgeführt werden. Da es sich um ein hochsensibles, sicherheitsrelevantes Thema handelt, werden von den Unternehmen keine näheren Details und Daten offengelegt.

Aussprache

Abg. **Sina Maria Beckmann** (GRÜNE): Durch Ihre Erläuterungen habe ich das Gefühl erhalten, dass wir relativ gut geschützt sind. Ich habe dennoch zwei Nachfragen. Erstens. Gab es bereits

einen Hacking-Angriffsversuch in Niedersachsen? Zweitens. Habe ich Sie richtig verstanden, dass das Land Niedersachsen bei einem Cyberangriff gar nicht viel unternehmen kann, weil das im Zuständigkeits- und Aufgabenbereich der einzelnen Hafengesellschaften liegt?

MR **Jacob** (MW): Zur ersten Frage. Mir ist bekannt - das ist auch kommuniziert worden -, dass es Angriffe durch massenhaft versendete E-Mails gab. Dabei wird versucht, Systeme durch sehr viele E-Mails zu verlangsamen. Diese Angriffe haben aber keine Folgen gehabt.

Zur zweiten Frage. Eingangs sagte ich bezüglich der Beeinträchtigung von Prozessen, dass die einzelnen Hafenstandorte einzelne Hafensicherheitsbehörden besitzen, die die Prozesse vor Ort betreuen und überwachen. Wenn ein Standort angegriffen wird, dann kann es passieren, dass dieser Standort vom Netz genommen wird. Damit wäre die Kommunikation untereinander nicht mehr möglich. Allerdings werden bei der Hafenbehörde, bei NPorts und beim JWP im Wesentlichen allgemeine Daten über Schiffe - Schiffsankünfte, Abrechnungsdaten und Ähnliches - verwaltet, betreut und verarbeitet.

In Ihrem Unterrichtungsantrag haben Sie ein Beispiel aus Australien geschildert, bei dem - so habe ich es verstanden - insbesondere die Technik beeinträchtigt wurde. Die Unternehmen der AG Seehäfen haben sehr allgemein geschildert, dass sie diesbezüglich entsprechende Abwehrmechanismen besitzen. Mir liegen allerdings keine weiteren Detailinformationen darüber vor, inwieweit die Umschlaganlagen oder -techniken beeinträchtigt werden können bzw. welche Schutzmechanismen vorhanden sind.

Abg. **Matthias Arends** (SPD): Der Unterrichtungsantrag von Frau Beckmann war sehr berechtigt. Auch wenn die Situation in Australien am Ende aufgrund der Struktur hier in Niedersachsen nicht mit der hiesigen Situation vergleichbar ist, ist es nichtsdestotrotz wichtig darzustellen, wie einzelne Komponenten ineinandergreifen, wie man sich aufeinander verlassen kann und wie Szenarien durchdacht worden sind.

Ich war 17 Jahre lang Soldat. Es war immer gut, wenn man erkennen konnte, dass es Strukturen gibt und jeder in seiner Struktur weiß, was er wann zu tun hat. Durch diese Unterrichtung habe ich den Eindruck gewonnen, dass sich aus den Gedanken, die man sich darüber, was passiert, wenn etwas passiert, zu Recht im Vorfeld gemacht hat, durchaus verfestigte Strukturen ergeben haben. Auch wenn Vieles durch den Geheimhaltungsgrad VS-NfD verständlicherweise geschützt und daher nicht im Detail darstellbar ist, habe ich den Eindruck, dass dies gut durchdacht ist. Hoffentlich werden durch unsere Kleinteiligkeit - diese kann manchmal auch ein Vorteil sein - Vorkommnisse, wie sie Frau Beckmann in ihrem Beispiel dargelegt hat, in Niedersachsen nicht in so dramatischer Art und Weise Auswirkungen haben.

Abg. **Hartmut Moorkamp** (CDU): Sie haben über die Gefahrenabwehrpläne in den Häfen gesprochen und über meldepflichtige Ereignisse. Wie viele meldepflichtige Ereignisse gab es im Laufe des Jahres 2023 oder auch in den letzten Jahren hier in Niedersachsen?

MR **Jacob** (MW): Das kann ich nicht beantworten; die Hafensicherheitsbehörde hat uns dazu nichts weiter mitgeteilt. Ich kenne aus dem letzten Jahr ein paar Fälle, nicht nur aus dem Bereich der IT, sondern es gab zum Beispiel auch unberechtigte Zugänge in die Hafenanlagen. Dabei sind Personen mit falschen ID-Karten aufgefallen. Wenn Sie diesbezüglich weitere Informationen wünschen, dann können wir gerne nachfragen.

Abg. **Hartmut Moorkamp** (CDU): Ja, es wäre interessant, das zu wissen.

Zum Ende hatten Sie das Thema kritische Infrastruktur und die Umschlagunternehmen angesprochen. Sie hatten auch die AG Seehäfen erwähnt. Wie viele Unternehmen oder Einrichtungen in den Häfen werden als kritische Infrastruktur eingeschätzt?

MR **Jacob** (MW): Die Abgrenzung ergibt sich aufgrund der Umschlagleistungen; hierzu gibt es Schwellenwerte in der Kritisverordnung. Ich kann momentan nicht beantworten, welcher Hafen dazugehört und welcher lediglich unter das Hafensicherheitsgesetz fällt. Auch hierzu können wir aber gerne nachliefern.

Abg. **Hartmut Moorkamp** (CDU): Des Weiteren habe ich eine Frage zu den Kosten. Das Ganze ist bekanntlich mit einem erheblichen Aufwand verbunden. Die Berechtigung ist vorhanden; es ist notwendig. Ich glaube, diesbezüglich sind sich alle einig. Sie haben die Hafensicherheitsbehörde, die EU-Vorgaben und das Thema Cybersicherheit genannt. All das muss gewährleistet sein. Welche Kosten fallen für unsere Häfen an bzw. welche Summen werden für die Erfüllung dieser Maßnahmen ausgegeben?

MR **Jacob** (MW): Die Hafensicherheitskosten werden bekanntlich auf die Entgelte umgelegt. Sie sind also von den Schiffen zu zahlen. Selbst wenn physische Einrichtungen wie Zugangskontrollen oder Zaunanlagen gebaut werden - zum Beispiel werden Zaunanlagen oder Wachgebäude aufgrund regelmäßiger Überprüfungen erneuert -, so werden diese Sicherheitskosten wieder auf die Anlaufentgelte der Schiffe umgelegt. Das ist allgemein üblich. Unterm Strich entstehen für das Land somit keine Kosten. Ich kann Ihnen aber keine Gesamtsumme über die Kosten pro Jahr mitteilen.

Abg. **Hartmut Moorkamp** (CDU): Das Thema wurde häufiger an uns herangetragen. Gerade die EU-Vorgaben - Kameras und alles, was diesbezüglich gemacht werden muss - werden zwar natürlich umgesetzt und akzeptiert, die Erfüllung dieser EU-Vorgaben sorgt aber nicht immer für Begeisterung. Auch wenn dem Land Niedersachsen keine Kosten entstehen, weil sie umgelegt werden, muss am Ende irgendjemand diese Kosten tragen. Daher wäre es interessant zu wissen, wie hoch diese Summe ist.

MR **Jacob** (MW): Auf der einen Seite gibt es die Kosten, die den Unternehmen entstehen. Wenn zum Beispiel ein Umschlagunternehmen sein Terminal sichert, um seine Güter zu sichern, dann ist das eine Aufgabe des Unternehmens. Auf der anderen Seite stehen die Kosten, die aufgrund des allgemeinen Schutzes der Hafenanlage entstehen, also diese sogenannten ISPS-Entgelte. Die werden auf die Schiffsankünfte umgelegt. Nur hierzu können wir etwas zusammentragen, stellen Ihnen diese Informationen aber gerne zusammen.

***

Tagesordnungspunkt 3:

Unterrichtungsantrag zu „Potenziale der Windenergie in den Niedersächsischen Seehäfen“

Antrag auf Unterrichtung der Fraktion der CDU vom 5. Dezember 2023

Der **Unterausschuss** billigt den Antrag auf Unterrichtung einvernehmlich.

*

Das MW stellt in Aussicht, die Unterrichtung in der nächsten Sitzung am 13. Februar 2024 durchzuführen.

***

Tagesordnungspunkt 4:

Terminangelegenheiten

Der **Unterausschuss** legt die Termine für die auswärtigen Sitzungen im Jahr 2024 fest. Diese werden am 30. April 2024 in Wilhelmshaven und am 3. Dezember 2024 in Brake stattfinden.

***

Tagesordnungspunkt 5:

Parlamentarische Informationsreise

Die Fraktionen werden gebeten, der Landtagsverwaltung die gewünschten Stationen und Themen für die parlamentarische Informationsreise nach Portugal bis zum 5. Februar 2024 schriftlich mitzuteilen.

***