Schleswig-Holsteinischer Landtag
Umdruck 20/2981

maritimes cluster norddeutschland

MCN Geschäftsstelle Schleswig-Holstein
c/o WTSH GmbH, Lorentzendamm 24, 24103 Kiel

Herr
Claus Christian Claussen
Vorsitzender des Wirtschafts- und
Digitalisierungsausschusse

Maritimes Cluster Norddeutschland
Geschäftsstelle Schleswig-Holstein
WTSH Wirtschaftsförderung
und Technologietransfer
Schleswig-Holstein GmbH
Lorentzendamm 24
24103 Kiel

Ansprechpartner
Peter Moller
Geschäftsstellenleiter
+49 431 66666-868
peter.moller@
maritimes-cluster.de
www.maritimes-cluster.de

Kiel, 22. März 2024
E-Mail an: wirtschaftsausschuss@landtag.ltsh.de

Bericht über die Cybersicherheit unserer Infrastruktur.
Bericht der Landesregierung. Drucksache 20/1584.

Stellungnahme Maritimes Cluster Norddeutschland (MCN) e. V.,
Geschäftsstelle Schleswig-Holstein

Sehr geehrter Herr Claussen,

ich wurde gebeten zu o. g. Bericht eine Stellungnahme abzugeben. Dies mache ich gerne. Nachfolgend meine Punkte.

Anzuhörende:
Im Themenkomplex der Cybersicherheit unserer Infrastruktur könnten in Zukunft noch folgende Organisationen angefragt werden.

- BSKI, Bundesverband für den Schutz Kritischer Infrastrukturen
- Wasserstraßen- und Schifffahrtsverwaltung des Bundes (verantwortlich für die Bundeswasserstraßen inkl. Nord-Ostsee-Kanal)
- Bundesamt für Seeschifffahrt und Hydrographie (BSH)
- Seehafen Kiel
- Brunsbüttel Ports
- Lübecker Hafengesellschaft
- Betreiber von Onshore- und Offshore-Windanlagen
- Energieversorger
- Netzbetreiber

Vereinsregister
Amtsgericht
Hamburg VR 23003
Steuernummer
17 / 454 / 05734

Bankverbindung
Deutsche Bank
IBAN: DE91 2007
0024 0485 8247 00
BIC: DEUT DE DB HAM

maritimes cluster
norddeutschland

Bericht über die Cybersicherheit unserer Infrastruktur

Ich begrüße ausdrücklich das Vorhaben verstärkter Aktivitäten der Landesregierung Schleswig-Holstein im Bereich der Cyber- und Informationssicherheit.

Aus meiner Sicht sollte darüber hinaus noch auf weitere und wesentlich weitreichendere mögliche Bedrohungsszenarien und deren Konsequenzen eingegangen werden. So heißt es auf Seite 16:

‚Bezogen auf Unternehmen, Behörden und sonstige Institutionen, einschließlich der kritischen Infrastruktur, stellen Erpressungen mittels eingesetzter Ransomware auch weiterhin die Hauptbedrohung dar.‘

Solche Erpressungen sind ernstzunehmende Bedrohungen denen auch maritime Unternehmen ausgesetzt sind, wie z. B. Werften, Hafenbetreiber, Schiffbauzulieferer oder Reedereien. Treten solche Fälle ein, werden einzelbetriebliche Schäden verursacht, die oft auch Auswirkungen auf nachgelagerte Lieferketten haben.

Jedoch birgt Cybersabotage ein wesentlich höheres Gefährdungspotential für unsere Infrastruktur, Volkswirtschaft sowie Bevölkerung und Natur.

Bei wachsenden geopolitischen Spannungen gilt es in Worst-Case-Szenarien zu denken und handlungsbereit in Bezug auf die Vermeidung als auch die Behebung von Schäden aus Cyber-Sabotageakten zu sein.

Es müssen vorrangig mögliche Ausfallszenarien betrachtet werde, welche durch gezielte Cybersabotage zu Ausfällen und Unglücken größeren Ausmaßes führen können.

Hier sollte Fokus auf die Betreiber kritischen Infrastruktur gelegt werden und – unabhängig der Verantwortung von Bund, Land Schleswig-Holstein oder der Unternehmen – Vermeidungs- und Reaktionsszenarien erarbeitet werden, wobei Reaktionsszenarien meist weit über digitale Maßnahmen hinausgehen (Stichwort: Katastrophenschutz). Ebenso gilt es neben den Betreibern auch die Nutzer der kritischen Infrastruktur zu betrachten und was durch gezielte Sabotage dieser Nutzer geschädigt werden kann. Im maritimen Kontext sind das u. a. die Nutzer unserer Wasserwege und Häfen (z. B. Reedereien und deren Schiffe welche den Nord-Ostsee-Kanal befahren und küstennah unterwegs sind).

Feststellung: auch ein Schiff und dessen Navigation kann gehackt werden. Es sind Cybersicherheitsmaßnahmen von Bund und Land zu fordern und müssen von den Schiffsbetreibern nachvollziehbar umgesetzt werden.

Im maritimen Kontext sind u. a. zu betrachten:

- Häfen, sowie die Konsequenzen ihrer Betriebsunfähigkeit und die daran hängenden Transportketten (Straße, Bahn)

- Seewege und Wasserstraßen (u. a. Nord-Ostsee-Kanal – die am meisten befahrene künstliche Wasserstraße der Welt)
- Verkehrsleitsysteme (an Land und im Wasser)

Die Konsequenzen gravierender Beschädigungen oder eines Totalausfalls kritischer Infrastrukturen Schleswig-Holsteins sind zu betrachten. So können Auswirkungen von havarierten Schiffen sein:

- Verstopfung der Wasserwege (Hafenzufahrten, Kanäle)
- Verschmutzung der Umwelt durch Frachtverlust (z.B. Chemikalientanker) oder Treibstoff-Lecks. Im schlimmsten Fall kann dies direkt Personen und die Schleswig-Holsteinischen Küstenabschnitte und unsere Tourismuswirtschaft treffen.

Bei den Auswirkungen auf Infrastruktur, Betriebe, die Bevölkerung sowie Fauna und Flora ist es belanglos ob die Verantwortlichkeiten für die Cybersicherheit beim Bund, beim Land SH oder bei den Unternehmen liegt, da diese Auswirkung Schleswig-Holstein betreffen – sowie die Logistik und Versorgungssicherheit von und aus SH in andere Regionen.

Es gilt Risiken und Szenarien zu bewerten, zu vermeiden, um im Schadensfall bestmöglich und schnell reagieren zu können. Hier ist in ‚Worst-Case' Szenarien zu denken und zu agieren. Es gilt der Kooperations- und Koordinationsgedanke.

Havarierte Landfahrzeuge sind einfacher zu kontrollieren und zu bergen als havarierte Schiffe. Ebenso sind die Auswirkungen auf die maritime Umgebung / Umwelt schwerwiegender, da sich z. B. Schadstoffe im Wasser wesentlich schneller und weiter verteilen und die Umgebung längerfristig schädigen.

Bei Rückfragen sowie für weiteren Input stehe ich jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

gez.
Peter Moller

Leiter Geschäftsstelle Schleswig-Holstein
Maritimes Cluster Norddeutschland