Schleswig-Holsteinischer Landtag
Umdruck 20/3011

UVNord Postfach 9 10 24758 Rendsburg

CDU-Fraktion
im Schleswig-Holsteinischen Landtag
Herrn Claus Christian Claussen, MdL
Düsternbrooker Weg 70
24105 Kiel

per E-Mail: wirtschaftsausschuss@landtag.ltsh.de

Vereinigung der Unternehmensverbände
in Hamburg und Schleswig-Holstein e.V.

BDI-Landesvertretung Schleswig-Holstein

Hauptgeschäftsführer
Michael Thomas Fröhlich

Telefon 04331 1420-43
Telefax 04331 1420-50
E-Mail froehlich@uvnord.de

Rendsburg, 26.03.2024
Fr./Te.

Gesamtstellungnahme UVNord

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

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

wir nehmen Bezug auf Ihr Schreiben vom 28.02.2024 und danken für die Gelegenheit, zu dem vorgenannten Bericht Stellung nehmen zu dürfen.

Aufgrund der Bedeutung haben wir alle 114 angeschlossenen Mitgliedsverbände von UVNord angehört, die derzeit mehr als 100.000 Mitgliedsunternehmen mit über 1,8 Millionen sozialversicherungspflichtig Beschäftigten in Schleswig-Holstein und Hamburg betreuen. Zudem sind die ehrenamtlichen Gremien von UVNord angehört worden.

Aus Sicht der norddeutschen Wirtschaft ist die Stärkung der Cybersicherheit grundlegend positiv zu bewerten, grade vor dem Hintergrund der aktuellen Bedrohungslage und der Entwicklung hin zu mehr Digitalisierung in allen Branchen. Dadurch spielt die Cybersicherheit eine zunehmend kritische Rolle in der gesamten Wirtschaft. Es geht nicht nur die Implementierung technischer Schutzmaßnahmen, sondern auch die Schaffung eines Bewusstseins für Cybersicherheit. Dies vorangestellt möchten wir die Gelegenheit nutzen, folgende Punkte anzumerken:

Mehr Beachtung geschenkt werden sollte nach unserem Dafürhalten denjenigen Bereichen der sozialen Infrastruktur in Schleswig-Holstein, welche durch die Einrichtungen der freien Wohlfahrtspflege erbracht werden. Beispielhaft möchten wir auf den Bereich der Betreuung, Beschäftigung und Begleitung im Rahmen der Eingliederungshilfe nach dem SGB IX hinweisen, der im Bericht der Landesregierung komplett ausgeblendet wurde. Auch hier besteht einerseits ein erhebliches Gefährdungsrisiko, insbesondere bezogen auf die tatsächliche Begleitung dieser Menschen, als auch hinsichtlich der hier erfassten umfangreichen Sozialdaten, die mit den Leistungsträgern der EGH, also den Kommunen direkt oder über Portale ausgetauscht werden. Dieser Austausch von Daten von Einrichtungen der Eingliederungshilfe beispielsweise mit der KOSOZ AöR und den Kommunalverwaltungen erfordert den Betrieb cybersicherer Systeme und muss durch die Öffentliche Hand finanziell und personell angemessen ausgestattet sein. Zudem müssen die Einrichtungen in konkreten Bedrohungssituationen angemessen fachlich unterstützt werden.
Ebenso sollten weitere Bereiche der durch die Einrichtungen der freien Wohlfahrtspflege bereitgestellten sozialen Infrastruktur zukünftig laufend in der Betrachtungsweise der Landesregierung zum Thema Cybersicherheit berücksichtigt werden. So sind beispielsweise auch Einrichtungen der Jugendhilfe potenzielle Ziele von Hackerangriffen und die vielen im Land gemeinnützigen, ehrenamtlichen Einrichtungen und Initiativen benötigen für ihr Engagement fachliche und finanzielle Unterstützung bei der Schaffung und Nutzung sicherer Systeme für die digitale Kommunikation und Zusammenarbeit.

Auch die Feststellung unter dem Punkt 3.11.2., dass die „IT-Ausstattung in den Krankenhäusern des Maßregelverzugs notleidend“ sei, zeigt Handlungsbedarf. Zum Schutz der hier arbeitenden Menschen müssen digitale Sicherheitssysteme und Patientenakten unbedingt auf neustem Stand sein.

Das enge Zusammenspiel der AöR Dataport und CERT-Nord, also dem Datenverarbeiter des Landes und dem Kontrollgremium, ist äußerst kritisch einzustufen. Besonders kritisch ist in diesem Zusammenspiel der in 3.2.4 als besonders herausfordernd bezeichnete personelle Mangel zu sehen.
Vor diesem Hintergrund ist auch zu hinterfragen, ob selbst gehostete Open-Source-Software oder aus vielen Open-Source-Komponenten zusammengebaute Software, wirklich die bessere Lösung ist, als kommerzielle Softwareprodukte. Es muss in Betracht gezogen werden, dass feindselige Programmierer oder andere Akteure in einzelne Open-Source-Komponenten

Schadsoftware eingebaut haben. Das komplexe Zusammenspiel verschiedener Komponenten ist heute kaum noch zu überprüfen, wie die angeführten Angriffe zeigen. Großen Softwareanbietern stehen hier ganz andere Prüfprozesse zur Verfügung. Das weit verbreitete und im öffentlichen Dienst gepflegte Paradigma, dass in eigener Regie gehostete Open-Source-Software „gut“, dagegen aber von Unternehmen programmierte Software und Cloud-Strukturen, insbesondere, wenn sie beim verbündeten USA beheimatet sind, „böse“ sind, ist aufzuheben.
Insbesondere im Hinblick auf den Personalmangel sollte außerdem bedacht werden, die vorhandenen Mitarbeiter nicht auf Grund ausufernder Bürokratie mehr zu belasten.

Abschließend sei die Bemerkung gestattet, dass die im Ausblick zusammengefassten „Emerging Security Threads“ nicht Probleme der fernen Zukunft sind, sondern im Wesentlichen bereits heute stattfinden. Dringend geboten ist eine Prüfung der IT-Sicherheitsstruktur rund um die Logistikprozesse der Häfen, insbesondere vor dem Hintergrund der zunehmenden Drogenimporte, über die in den letzten Wochen berichtet wurde. Auch wenn nicht alle Cyberbedrohungen sofort die kritische Infrastruktur zerstören, so zermürben oder untergraben sie bereits jetzt demokratische Prozesse und Strukturen: Mangelnde staatliche Leistungsfähigkeit aufgrund von Personalmangel in deren Folge digitale Prozesse nicht angeschoben werden oder nicht funktionieren, untergraben das Vertrauen in das Staatswesen. Hybride Angriffe, Desinformationskampagnen und erleichterte Angriffe auf IT-Systeme mit Unterstützung von KI sind bereits heute Realität.

Für einen weiteren konstruktiven Dialog stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Michael Thomas Fröhlich