Schleswig-Holsteinischer Landtag
Umdruck 20/2980

D64
Zentrum für
Digitalen Fortschritt

Stellungnahme

Berlin, der 22. März 2024

Zum Bericht der Landesregierung „Bericht über die Cybersicherheit unserer Infrastruktur“ an den Schleswig-Holsteinischen Landtag, Drucksache 20/1584

Zum vorstehend genannten Bericht nimmt D64 – Zentrum für Digitalen Fortschritt e.V. wie folgt Stellung:

Zu 2. Übergreifende Aspekte

Der Bericht kann im Sinne einer Bestandsaufnahme der Lage der Cybersicherheit in Schleswig-Holstein dahingehend verstanden werden, dass – Zitat aus Unterkapitel 2.4 – „es einer strukturierten und ganzheitlichen Herangehensweise – eines systematischen Informationssicherheitsmanagements“ bedarf. Die explizite Anerkennung dieser übergreifenden Aufgabenwahrnehmung als einer „Grundvoraussetzung der Digitalisierung und des Verwaltungshandelns insgesamt“ (letzter Satz im Kapitel 2) seitens der Landesregierung ist ausdrücklich zu begrüßen.

Die Betrachtung der Bedrohungslage ist eine Zusammenfassung aus dem Lagebericht 2022 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sie enthält leider keine Beispiele aus Schleswig-Holstein – hier wäre es sinnvoll gewesen, etwa auf Informationen vom CERT Nord[1] oder regionalen IT-Dienstleistern zurückzugreifen, um die tatsächliche Lage im Bundesland plastischer darzustellen.

Zu 3. Spezifische Aspekte

Für die anschließende Betrachtung konkreter Bedrohungen in Schleswig-Holstein wurden Fallzahlen der Polizeilichen Kriminalstatistik (PKS) herangezogen, allerdings nur pauschal summiert, nicht nach einzelnen Straftatbeständen differenziert. Konkrete Einzelfälle sind gar nicht benannt, nur eine Beeinträchtigung „über viele Stunden“ des Landesportals aufgrund einer pro-russischen DDoS-Attacke im April 2023 wird erwähnt. Zu anderen als

1 Die statistischen Erkenntnisse beim CERT Nord werden später im Unterkapitel 3.8.1.5 ausführlich gewürdigt, aber auch dort wird auf konkrete Fallbeschreibungen vollständig verzichtet.

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251

Propagandazwecken ausgeführten Cybercrime-Aktivitäten, die bei Einrichtungen in Schleswig-Holstein vielleicht bekannt sind, führt der Bericht nichts weiter aus.

Die personelle Ausstattung zur Erfüllung der Anforderungen, die an die Cybersicherheitsarchitektur im Land gestellt werden müssen, ist offensichtlich nicht zufriedenstellend. Der Bericht enthält an allen Stellen, die sich zur Besetzung von Funktionen äußern, immer wieder den Hinweis, dass dies „angestrebt" werde, „weitgehend eingerichtet" sei oder ähnliche einschränkende Formulierungen. Mit jeder diesen Relativierungen verstärkt sich der Eindruck, dass die Zielstruktur nur unzureichend mit personellen und organisatorischen Ressourcen hinterlegt ist. Leider ist allerdings nicht erkennbar, wie sehr Anspruch und Wirklichkeit auseinanderliegen. An keiner Stelle des Berichts wird benannt, wie viele Personen rekrutiert werden müssten, um die für eine funktionierende Cybersicherheitsarchitektur erforderlichen Planstellen zu besetzen. Diese Art der Darstellung, mit der im Bericht auf eine Bezifferung des Bedarfs verzichtet wird, ist unzureichend: Eine Einschätzung, welches Niveau der Cybersicherheit in Schleswig-Holstein tatsächlich gewährleistet wird, ist angesichts mangelnder Quantifizierung der Stellen und ihrer Besetzung nicht möglich.

Auch die Beschreibung von angestrebten Aus- und Weiterbildungen, Zertifizierungen und weiteren Maßnahmen zur Personalentwicklung, zur externen Unterstützung, bei der Zusammenarbeit mit dem CERT Nord etc. wird im Bericht der Landesregierung ohne jede Quantifizierung, Fristen oder Ziele vorgelegt.

Die folgenden Unterkapitel zur Cybersicherheit in den Bereichen Energieversorgung, kerntechnischen Einrichtungen, Wasserversorgung und -entsorgung machen das Dilemma deutlich, in dem sich Landesbehörden nicht nur in Schleswig-Holstein befinden: Sie verfügen über keine spezifische Zuständigkeit für die Aufrechterhaltung der Cybersicherheit in diesen Sektoren kritischer Infrastrukturen und haben deshalb weder Expertise noch übernehmen sie Aufgaben bei der Überwachung solcher Einrichtungen. Aufsicht über die Einhaltung von regulatorischen Anforderungen – und ihre Durchsetzung – obliegen hier ausschließlich Bundesbehörden. Diese Verantwortungsdiffusion steht im direkten Widerspruch zu den expliziten Zuständigkeiten, die außerhalb des eng abgegrenzten Bereichs der Informationssicherheit durchaus bei der obersten

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251

Landesbehörde liegen: Hier liegen die Verantwortlichkeiten zum Beispiel für Meldepflichten nach § 49 Energiewirtschaftsgesetz, Genehmigungsverfahren für kerntechnische Anlagen und sämtliche Wasserwirtschaftsbelange beim MEKUN, das auf die Cybersicherheitsbelange derselben Sektoren keinerlei Einfluss nimmt.

Dem ausführlichen Unterkapitel 3.6 ist zu entnehmen, wohin eine solche Verantwortungsdiffusion führen kann. Im Katastrophenschutz arbeiten Bund, Länder, Berufs- und freiwillige Feuerwehren, Polizeikräfte, ehrenamtliche Hilfsorganisationen zusammen – an den Schnittstellen ihrer digitalen Kommunikation herrscht eine beunruhigende Vielfalt an Protokollen, Techniken und Verfahren, die in ebenso mannigfaltiger Weise versagen können. Dass eine „unzulässige Weiterverarbeitung der Informationen (…) nicht auszuschließen" sei (letzter Satz im Unterkapitel 3.6), ist eine elegante Formulierung für das potenzielle Versagen des Katastrophenschutzes, das auf Brüche in der Sicherheitsarchitektur zurückzuführen wäre.

Die Darstellung der genuin vom Land betriebenen Cybersicherheitsarchitektur in Landes- und Kommunalverwaltungen ist streng an den Empfehlungen des UP BUND und des BSI IT-Grundschutzes respektive der nativen ISO/IEC 27001 entlang beschrieben. Die in den Kapiteln 3.7 und 3.8 aufgeführten Grundlagen, Verfahren, Hilfsmittel und Techniken referieren im Wesentlichen Normbestandteile, deren Einhaltung ausdrücklich zu begrüßen ist.

Nicht übersehen werden darf allerdings, dass bereits im 2. Kapitel darauf hingewiesen wurde, beispielsweise die in Unterkapitel 3.8.1.1 erwähnten CISO-Funktionen gar nicht vollständig umgesetzt zu haben. Die im gesamten Abschnitt über die Cybersicherheit in kommunalen und Landesverwaltungen dargelegten Informationen beschreiben also die Zielstruktur, nicht die aktuelle Situation. Um den tatsächlichen Zustand beurteilen zu können, bedarf es weiterer Konkretisierungen, die der vorliegende Bericht nicht enthält.

In den weiteren Unterkapiteln zu den im Antrag des SSW auf Drucksache 20/797 einzeln abgefragten Bereichen sind jeweils höchst unterschiedliche Betrachtungsweisen zusammengeflossen. Die Hochschulen nennen als einzige Institution konkrete Cybersicherheitsvorfälle sogar über den eigenen Zuständigkeitsbereich hinaus, während

im Schifffahrtsverkehr im weiten Feld zwischen den außerhalb der Landeszuständigkeit liegenden Bundeswasserstraßen einerseits und den unteren Hafenbehörden andererseits keine unmittelbare Verantwortung für die Cybersicherheit übernommen wird. Auch in jedem anderen Bereich des MWVATT ist jede Einrichtung „eigenverantwortlich" für sich selbst zuständig. Innerhalb des Zuständigkeitsbereichs dieses Ministeriums bietet der „Servicepoint Cybersecurity" Anlass zu einer Neukonzeptionierung, ohne dass dem Bericht zu entnehmen wäre, welcher Einsatzzweck erfolgversprechend sein könnte.

Der Abschnitt über Desinformation ist überwiegend auf Staatsschutz- und Strafverfolgungsmaßnahmen fokussiert, die zur Verteidigung gegen gezielte Falschinformation, Propaganda und Angriffe auf Demokratie und Rechtsstaat ergriffen werden. Dass ein erheblicher Anteil der Techniken zur medialen Sabotage gesellschaftlicher Diskurse ein Problem der Informationssicherheit darstellt, kommt in dieser Darstellung zu kurz. Während der Bericht Desinformation immerhin als „Querschnittsthema" bezeichnet, bleibt er bei klassischen Ermittlungs- und Repressionsmethoden. Dabei erfordern Mechanismen wie Astroturfing[2], viele Arten des Social Engineering[3], aber auch kommerzielle Werbekampagnen zur Wahlbeeinflussung auf Plattformen oder ähnliche Manipulationen der öffentlichen Meinung deutlich mehr als nur polizeiliche und Verfassungsschutzaktivitäten. Zur Bekämpfung von Desinformation wird sowohl mehr und bessere informationstechnische Unterstützung bei Abwehrmaßnahmen als auch Sensibilisierungs- und Aufklärungsarbeit in allen klassischen Medien, Messenger- und Social-Media-Diensten benötigt. Dass hier von den Betreibern aller medialen Verbreitungskanäle viel zu wenig Kooperation bei der Abwehr von Hetze und Lügen geleistet wird, bleibt im Bericht unerwähnt. Auch der Digital Services Act der Europäischen Union, eine der konsequentesten Regulierungen des Desinformationsraums, wird hier nicht weiter beachtet, obwohl zum Beispiel die darin vorgesehene Auditierung der Very Large Online Platforms (VLOP) ein besonders scharfes Schwert im Kampf gegen Desinformation darstellt.

Mehr Substanz enthält die gesamtstaatliche Darstellung der Cybersicherheitsarchitektur, die im Wesentlichen die verschiedenen von Bund und Ländern betriebenen Gremien

2 Massenhafte Schein-Accounts zur Verbreitung von Falschinformation

3 Etwa der CEO-Fraud mit KI-Unterstützung zur Stimmennachahmung

auflistet, deren Aufgaben im Bereich Prävention, Detektion und Reaktion liegen. Keine der erwähnten Einrichtungen übernimmt allerdings operative Verantwortung für Belange der Informationssicherheit, weder auf übergeordneter Ebene noch in Schleswig-Holstein. Die erwähnte Kooperationsvereinbarung mit dem BSI gibt es seitens der Behörde bereits mit sechs Bundesländern, darunter Sachsen-Anhalt als eines der vier Länder, die im CERT Nord zusammenarbeiten – ein kurzfristiger Abschluss des Kooperationsabkommens nach der bereits erfolgten Absichtserklärung durch Schleswig-Holstein wäre erfreulich.

Zu 4. Ausblick

Die Entwicklung der Bedrohungslage baut auf den Projektionen der ENISA auf. Wie realistisch die Einschätzungen der europäischen Cybersicherheitsbehörde sind und inwieweit sie sich auf schleswig-holsteinische Verhältnisse portieren lassen, ist unbekannt.

Was die Planungen der Landesverwaltung für die künftige Stärkung der Cybersicherheitsarchitektur Schleswig-Holsteins angeht, enthält Unterkapitel 4.2 eine Fülle von Vorhaben, die in der „Digitalen Vorzeigeregion" umgesetzt werden sollen. Ein erheblicher Teil sind bereits begonnene Maßnahmen, die eine „Verstetigung" (das Projekt SiKoSH für die Sicherheit der Kommunen) oder „Ausbau" (CERT Nord und Security Operation Center) erfahren sollen. Auch der strategische Ausbau des Informationssicherheitsmanagements spielt eine zentrale Rolle im Konzept der Landesregierung. Alle Bemühungen im Kapitel 4.2.1 sind unbedingt begrüßenswert, bedürfen aber einer klaren Zielsetzung und Frist zu ihrer Erreichung. Nur die Einführung des zentralen ISMS-Tools ist bis Ende des Jahres 2025 terminiert, bei allen anderen Vorhaben fehlt der Umsetzungshorizont.[4]

Mit Spannung wird der Entwurf zum Gesetz für digitale Resilienz in Schleswig-Holstein (Informationssicherheitsgesetz) erwartet. Hier besteht die Gelegenheit, landesrechtliche Vorgaben zu konkretisieren und verbindlich für alle nachgeordneten Bereiche, aber auch für in Schleswig-Holstein ansässige privatwirtschaftliche oder gemeinnützige Institutionen zu veranlassen.

4 Außerhalb 4.2.1 ist immerhin beim angestrebten Kooperationsabkommen mit dem BSI das Jahr 2024 genannt.

Fazit

Auf der Grundlage des vorliegenden Berichts wird es dem Schleswig-Holsteinischen Landtag kaum möglich sein, die Tragfähigkeit der Cybersicherheitsarchitektur des Landes zu beurteilen. Um im Rahmen des Haushaltsrechts des Parlaments die angemessene finanzielle Ausstattung der einzelnen Ressorts der Landesregierung sowie anderer, aus Landesmitteln zu bestreitender Bereiche gewährleisten zu können, müssten jedenfalls die aktuelle Bedarfslage und künftige Erfordernisse klar benannt und beziffert werden. Auch die in Schleswig-Holstein vorliegende Bedrohung und gegebenenfalls gezielt dagegen zu ergreifende Maßnahmen müssten zunächst konkretisiert werden, bevor der voraussichtliche Handlungsbedarf verlässlich zu ermitteln ist.

Erfüllungsaufwände zur Umsetzung künftiger gesetzlicher Vorgaben, wie sie im Bericht der Landesregierung bereits anerkannt werden, sind derzeit noch nicht seriös einzuschätzen. Bis zur Verabschiedung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) fehlen selbst belastbare Zahlen auf Bundesebene, von den Erfüllungsaufwänden der Länder ganz zu schweigen. Geht es nach den Empfehlungen des IT-Planungsrats (Beschluss 2023/39 vom 3.11.2023), sollen Gebietskörperschaften von den Verpflichtungen der Richtlinie (EU) 2022/2555 (NIS2) ausgenommen werden. Die Richtlinie enthält die Maßgabe, dass die nationale Gesetzgebung zur Umsetzung der NIS2 eines Mitgliedstaats selbst festlegt, welche regionalen Organe und Einrichtungen einzubeziehen sind. Ein vollständiger, freiwilliger Verzicht auf diese Festlegungskompetenz, womöglich aus Rücksicht auf die mangelnden Fähigkeiten und Ressourcen zur Umsetzung in den regionalen Einrichtungen, ist unwahrscheinlich und trüge jedenfalls nicht zur Stärkung der Cybersicherheit bei. Bei einer künftigen Schätzung des Erfüllungsaufwands muss deshalb berücksichtigt werden, dass es hier abweichend von der Auffassung der Landesregierung betroffene Einrichtungen geben kann, die nach Maßgabe des Bundes unter Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie fallen. Die daraus entstehenden, aus der bisherigen Einschätzung der Lage noch unberücksichtigten Aufwände dürfen bei der zukünftigen Planung der Cybersicherheitsarchitektur Schleswig-Holsteins nicht aus den Augen verloren werden.

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251