BSKI
Bundesverband für den Schutz
Kritischer Infrastrukturen e. V.

Schleswig-Holsteinischer Landtag
Umdruck 20/3902

Herrn

Claus Christian Claussen,

Vorsitzender des Wirtschafts- und Digitalisierungsausschusses

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

Wir nehmen hierzu wie folgt Stellung:

Die Cybersicherheitsstrategie in Schleswig-Holstein zielt darauf ab, die Widerstandsfähigkeit kritischer Infrastrukturen (KRITIS) und öffentlicher Verwaltungen zu erhöhen, um den Bedrohungen im digitalen Raum zu begegnen. Während die Ambitionen dieser Strategie aus Sicht der Kommunen und der Wirtschaft unterstützenswert sind, gibt es entscheidende Herausforderungen und Lücken, die behoben werden müssen, um eine wirkungsvolle Umsetzung zu gewährleisten.

1. Forderung nach einer ganzheitlichen Sicherheitsstrategie

Das KRITIS-Dachgesetz über die Resilienz kritischer Einrichtungen, das die RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 umsetzen soll, dient als einheitlicher Rahmen zur Verbesserung des Schutzes kritischer Infrastrukturen. Es geht über die NIS-2-Richtlinie hinaus, indem es nicht nur digitale, sondern auch physische und organisatorische Schutzmaßnahmen adressiert. Kommunen, die kritische Einrichtungen wie Wasser- und Energieversorgung betreiben, sind direkt betroffen und müssen komplexe Sicherheitsanforderungen erfüllen, die sowohl IT- als auch physische Sicherheitsaspekte umfassen.

Angesichts der zunehmend volatilen geopolitischen Lage sind die Umsetzung des KRITIS-Dachgesetzes und die Einhaltung der NIS2-Richtlinie unerlässlich, um die Widerstandsfähigkeit kritischer Infrastrukturen zu erhöhen. Eine ganzheitliche Sicherheitsstrategie, die sowohl digitale als auch physische Schutzmaßnahmen umfasst, ermöglicht es, potenzielle Bedrohungen effektiver zu begegnen und die Versorgungssicherheit zu gewährleisten. Dies schützt nicht nur die nationale Sicherheit, sondern fördert auch die Stabilität und das Vertrauen der Bevölkerung in die Infrastruktur.

Die heutige Bedrohungslage ist durch technologische Innovationen geprägt, die neue Angriffsvektoren eröffnen, wie etwa Angriffe auf die Lieferkette und gezielte Sabotage. Das KRITIS-Dachgesetz verlangt den Schutz der gesamten Lieferkette und den Aufbau robuster Sicherheitskonzepte, die sowohl Prävention als auch die Reaktion auf Vorfälle abdecken. Zusammen mit der NIS2-Richtlinie, die auf die Stärkung der digitalen Resilienz abzielt, entsteht ein integrativer Schutzschirm, der umfassend auf diese komplexen Bedrohungen vorbereitet ist.

Insoweit ist es begrüßenswert, dass die Landesregierung sich für eine angemessene Beteiligung der Länder auf Bundesebene einsetzen will. Da es sich um ein Bundesgesetz handeln wird, ist Schleswig-Holstein dafür verantwortlich, die Umsetzung der Regelungen zu gewährleisten und kann aber durch ergänzende Maßnahmen zur Verbesserung der Resilienz in ihrem Gebiet beitragen, solange diese mit den nationalen Vorgaben im Einklang stehen.

Die Landesregierung sollte daran arbeiten, eine Strategie zu entwickeln, die sowohl die Anforderungen des KRITIS-Dachgesetzes als auch der NIS2-Richtlinie berücksichtigt. Diese kombinierte Strategie stellt sicher, dass sowohl physische als auch digitale Sicherheitsanforderungen umfassend erfüllt werden. Eine integrative Herangehensweise fördert eine höhere Resilienz gegenüber vielfältigen Bedrohungen, sowohl im physischen als auch im digitalen Bereich.

2. Ressourcenmangel und personelle Herausforderungen

Ein zentraler Kritikpunkt betrifft die unzureichende personelle Ausstattung. Kommunen und Unternehmen sind gleichermaßen betroffen, da der Mangel an qualifiziertem Personal die Umsetzung der komplexen Sicherheitsanforderungen erschwert. Im Bericht wird mehrfach darauf hingewiesen, dass Funktionen wie die des CISO nur „weitgehend eingerichtet“ oder „angestrebt“ werden. Dies deutet darauf hin, dass die vorhandenen Ressourcen nicht ausreichen, um die erforderlichen Planstellen zu besetzen.

Die Umsetzung der umfangreichen Anforderungen scheitert häufig an der Verfügbarkeit qualifizierten Personals.

Dieser Mangel führt dazu, dass Kommunen und Unternehmen Schwierigkeiten haben, die notwendige Expertise aufzubauen, um die geforderten Schutzmaßnahmen effektiv umzusetzen. Der Fachkräftemangel im Bereich der IT-Sicherheit ist ein weitverbreitetes Problem, das nicht nur die Wirtschaft, sondern auch öffentliche Verwaltungen betrifft.

Die Empfehlung des LKA[1], mindestens zwei Personen für koordinierende Rollen in der Informationssicherheit zu benennen, ist für viele Kommunen und KMUs schwer umsetzbar, da Fachkräfte bereits in anderen Projekten gebunden sind.

Unternehmen, insbesondere KMUs, stehen vor der Herausforderung, mit größeren Konzernen um qualifiziertes Personal zu konkurrieren, was die Einführung umfassender IT-Sicherheitsmaßnahmen weiter verzögert. Kommunen berichten von ähnlichen Problemen, da sie oft nicht die Gehälter und Anreize bieten können, um Fachkräfte in den öffentlichen Sektor zu ziehen.

3. Umfangreiche Pflichten und erhöhte Anforderungen durch die NIS-2-Richtlinie

Die NIS-2-Richtlinie und das KRITIS-Dachgesetz stellen hohe Anforderungen an alle betroffenen Sektoren, die sowohl öffentliche als auch private Einrichtungen umfassen. Die Erweiterung auf 18 Sektoren, wie im Dokument des Landeskriminalamts (LKA) beschrieben[2], erhöht die Anzahl der betroffenen Akteure erheblich und umfasst nun auch öffentliche Verwaltungen, die als „wesentlich“ eingestuft werden. Normen fordern umfassende Maßnahmen wie Risikoanalysen, Sicherheitskonzepte, Krisenmanagement sowie die Sicherstellung der Lieferkettensicherheit. Für die Wirtschaft und Kommunen bedeutet dies eine erhebliche Steigerung des Umsetzungsaufwands, der personelle, finanzielle und organisatorische Ressourcen bindet.

4. Finanzielle Belastung und fehlende Unterstützung

Die Umsetzung der Vorgaben, einschließlich der Registrierung beim BSI und dem BBK sowie der Erfüllung von Berichts- und Risikomanagementpflichten, stellt eine erhebliche finanzielle Belastung dar. Der Bericht der Landesregierung enthält keine detaillierten finanziellen Analysen, die die tatsächlichen Kosten und die erforderlichen Mittel zur Umsetzung der Cybersicherheitsmaßnahmen beziffern. Die Wirtschaft und Kommunen fordern deshalb gezielte Förderprogramme und finanzielle Unterstützung durch Land und Bund, um die Umsetzung der Maßnahmen zu erleichtern und langfristige Investitionen in Cybersicherheit zu ermöglichen.

[1] Vgl. Landeskriminalamt Schleswig-Holstein, NIS-2, Network and Information Security, Oktober 2024.
[2] A.a.O..

5. Hoher administrativer Aufwand

Die Anforderungen an die Dokumentation und die Einrichtung eines umfassenden Informationssicherheitsmanagementsystems (ISMS) bedeuten für viele Kommunen und kleinere Unternehmen eine erhebliche bürokratische Hürde. Die Umsetzung der Maßnahmen erfordert detaillierte Prozesse, die den laufenden Betrieb beeinträchtigen können, ohne zusätzliche Mittel bereitzustellen.

6. Unklarheiten bei Zuständigkeiten

Ein zentrales Problem sind die Zuständigkeitsverteilungskonflikte, die sich aus den Überschneidungen zwischen landesweiten und bundesweiten Zuständigkeiten ergeben. Es existieren (noch) keine klaren Vorgaben, wer für die Überwachung und Durchsetzung der Sicherheitsmaßnahmen in verschiedenen kritischen Sektoren verantwortlich ist. Diese Unsicherheit führt zu einer ineffektiven Umsetzung und Koordination der Maßnahmen, was die Cybersicherheit schwächt.

7. Schulungen und Sensibilisierung

Es werden regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter, um das Bewusstsein für Cybersicherheitsrisiken zu stärken empfohlen. Diese Maßnahmen sind zwar positiv zu bewerten, erfordern jedoch zusätzliche Ressourcen, die sowohl Kommunen als auch Unternehmen belasten. Besonders KMUs haben häufig nicht die Kapazitäten, umfassende Schulungsprogramme zu implementieren.

8. Technologische Modernisierung und Infrastrukturausbau

Viele Kommunen verfügen nicht über die notwendige technische Infrastruktur, um die neuen Anforderungen zu erfüllen. Veraltete IT-Systeme und fehlende Investitionen in moderne Technologien erschweren es, den Schutz kritischer Infrastrukturen sicherzustellen. Die Resilienz und Reaktionsfähigkeit müssen in einem fortlaufenden Prozess verbessert werden, was auch die Integration von modernen Sicherheitslösungen erfordert nach dem Stand der Technik.

9. Zusammenführung der Empfehlungen

Um den Herausforderungen zu begegnen, sind aus Sicht der Kommunen und der Wirtschaft folgende Maßnahmen notwendig:

- Gezielte finanzielle Unterstützung durch Förderprogramme, um die Umsetzung der Anforderungen zu finanzieren.
- Klare Zuweisung von Verantwortlichkeiten und bessere Koordination zwischen Landes- und Bundesbehörden.
- Praxisnahe Schulungs- und Unterstützungsangebote, um die Fachkenntnisse in Cybersicherheit bei kommunalem und betrieblichem Personal zu stärken.
- Verwaltungsvereinfachung, um den bürokratischen Aufwand für die Umsetzung der Cybersicherheitsmaßnahmen zu reduzieren.
- Investitionen in technische Infrastruktur und den Ausbau moderner Sicherheitstechnologien.

Fazit

Die Cybersicherheitsstrategie in Schleswig-Holstein ist ein notwendiger Schritt, um den steigenden Anforderungen und Bedrohungen im digitalen Raum zu begegnen. Jedoch zeigt der Bericht der Landesregierung deutliche Schwächen in der praktischen Umsetzung und Unterstützung. Eine engere Zusammenarbeit zwischen der Regierung, den Kommunen und der Wirtschaft sowie gezielte finanzielle und personelle Unterstützung sind essenziell, um die Ziele effektiv zu erreichen und die Cybersicherheit und Resilienz ganzheitlich und nachhaltig zu stärken.

Köln, 02.11.2024

Holger Berens