SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 20/1584**
20. Wahlperiode 07.11.2023

Bericht

der Landesregierung – Der Minister und Chef der Staatskanzlei

Bericht über die Cybersicherheit unserer Infrastruktur
Antrag der Fraktion des SSW, Drs.-Nr. 20/797

Inhalt

1. Einleitung 5
2. Übergreifende Aspekte 5
2.1. Informations- und Cybersicherheit 5
2.2. Abgrenzung zu Cyberkriminalität und Spionageabwehr 6
2.3. Informationssicherheit und Vertrauen in staatliches Handeln 7
2.4. Informationssicherheitsmanagement als "Ermöglicher" 7
2.5. Aktuelle Bedrohungslage 8
3. Spezifische Aspekte 15
3.1. Bedrohungen durch Cyber-Kriminelle, Cyber-Angriffe und Fälle von Cyber-Erpressung in Schleswig-Holstein 15
3.2. Personelle Situation in der Landesverwaltung in Bezug auf die Cybersicherheit 17
3.2.1. Allgemeine personelle Situation 17
3.2.2. Aus- und Fortbildung, Zertifizierungen 18
3.2.3. Fachkräftemangel 19
3.2.4. Zusammenarbeit mit dem CERT Nord 19
3.2.5. Informationssicherheitsaufgaben im IT-Management und in anderen Bereichen 19
3.3. Cybersicherheit in der Energieversorgung 20
3.4. Cybersicherheit bei den in Rückbau befindlichen Atomkraftwerken 21
3.5. Cybersicherheit in der Wasserver- und -entsorgung 24
3.6. Cybersicherheit im Katastrophenschutz 25
3.7. Cybersicherheit in der kommunalen Verwaltung 27
3.7.1. Projekt "Sicherheit für Kommunen in Schleswig-Holstein", SiKoSH 27
3.7.2. Information und Sensibilisierung 28
3.7.3. Fachtagungen und Vernetzung 29
3.8. Cybersicherheit in der Landesverwaltung 30
3.8.1. Organisation der Informations- und Cybersicherheit in der Landesverwaltung 33
3.8.1.1. CISO und Informationssicherheitsbeauftragte 36
3.8.1.2. AG Informationssicherheitsmanagement (AG ISM) 36
3.8.1.3. Verantwortung der Behördenleitung 37
3.8.1.4. Mitarbeiterinnen und Mitarbeiter 38
3.8.1.5. CERT Nord 38
3.8.2. Landes-IT-Dienstleister Dataport 40
3.8.3. Mehrländer-ISM-Verbund der Trägerländer 40
3.8.4. Weitere Akteure 41
3.8.5. Landtagswahl 2022: Beispiel für Zusammenspiel der Akteure 41
3.9. Cybersicherheit bei der Polizei 41
3.10. Cybersicherheit bei der Justiz und in den Justizvollzugsanstalten 42
3.11. Cybersicherheit im Gesundheitswesen 43
3.11.1. Krankenhäuser 43
3.11.2. Krankenhäuser mit Unterbringungen nach Spezialgesetzen 45
3.11.3. Kassenärztliche Vereinigung Schleswig-Holstein (KVSH) 46

3.11.4. Krebsregister ... 46
3.11.5. Rettungsdienst ... 47
3.11.6. Heilberufekammern, Aufsicht Gesundheitsberufe und Schulische Bildung, Ausbildungsfonds der Pflegeberufe ... 47
3.12. Cybersicherheit in den Bildungseinrichtungen ... 48
3.12.1. Schulen ... 48
3.12.2. Hochschulen ... 49
3.12.3. Bildungszentrum der Steuerverwaltung des Landes ... 51
3.13. Cybersicherheit im Verkehrswesen – ÖPNV, SPNV/Fernzugverkehr ... 51
3.14. Cybersicherheit im Verkehrswesen – Individualverkehr ... 52
3.15. Cybersicherheit im Verkehrswesen – Häfen/Schiffsverkehr ... 53
3.16. Cybersicherheit im Verkehrswesen – Luftverkehr ... 54
3.17. Cybersicherheit in der Telekommunikation ... 54
3.18. Cybersicherheit in der Lebensmittelversorgung ... 55
3.19. Bisherige Aktivitäten des "Servicepoint Cybersecurity" ... 56
3.20. Aktivitäten der Landesregierung im Bereich der Bedrohung durch Desinformation ... 58
3.21. Darstellung der gesamtstaatlichen Cybersicherheitsarchitektur in den Bereichen Prävention, Detektion und Reaktion, insbesondere mit Blick auf die kritische Infrastruktur ... 60
3.21.1. Überblick ... 60
3.21.2. Länder- und Bund-Länder-Gremien ... 61
3.21.2.1. AG Informationssicherheit ... 61
3.21.2.2. LAG Cybersicherheit ... 62
3.21.3. Verwaltungs-CERT-Verbund ... 62
3.21.4. Nationales Cyber-Abwehrzentrum (NCAZ, Cyber-AZ) ... 63
3.21.5. Informationsaustausch KRITIS ... 63
3.21.6. Umsetzung der NIS-2-Richtlinie ... 64
3.21.7. Umsetzung der CER-Richtlinie ... 65
3.21.8. BSI-Zentralstellenkonzept ... 66
4. Ausblick ... 66
4.1. Antizipierte Bedrohungen 2030 (ENISA) ... 66
4.1.1. Kompromittierung der Lieferkette durch Software-Abhängigkeit ... 67
4.1.2. Fortschrittliche Desinformationskampagnen ... 67
4.1.3. Zunahme digitaler Überwachung, Verlust der Privatsphäre ... 67
4.1.4. Menschliche Fehlhandlungen und ausgenutzte Altsysteme in Cyber-physischen Ökosystemen ... 68
4.1.5. Verstärkung gezielter Angriffe (z. B. Ransomware) durch Daten smarter Geräte ... 68
4.1.6. Fehlende Analyse und Kontrolle weltraumgestützter Infrastruktur und Objekte ... 69
4.1.7. Zunahme fortschrittlicher hybrider Bedrohungen ... 69
4.1.8. Fachkräftemangel ... 69
4.1.9. Grenzübergreifende Dienstanbieter der Informations- und Kommunikationstechnik als ein einzelner Ausfallpunkt ... 70
4.1.10. Missbrauch künstlicher Intelligenz ... 70
4.1.11. Weitere antizipierte Bedrohungen ... 70

4.2. Digitale Resilienz in der Digitalen Vorzeigeregion Schleswig-Holstein – Stärkung der Informations- und Cybersicherheit 71
4.2.1. Ausbau des Informations- und Cybersicherheitsmanagements der Landesregierung 71
4.2.2. Fachkräftegewinnung und -bindung 73
4.2.3. Kooperationsvereinbarung mit dem BSI 73
4.2.4. Entwurf eines Gesetzes für Digitale Resilienz in Schleswig-Holstein (Informationssicherheitsgesetz) 73
4.2.5. Weiterentwicklung der SicherheitsPartnerschaft SH 73
4.2.6. Förderung der Informations- und Cybersicherheitsforschung 74
4.2.7. Intensivierung der Zusammenarbeit mit Bund und Ländern 74
4.2.8. Förderung des Informationssicherheitsmanagements an Hochschulen 74
4.2.9. Förderung des Informationssicherheitsmanagements an Schulen 74

1. Einleitung

Der Schleswig-Holsteinische Landtag hat die Landesregierung aufgefordert, einen Bericht zur Cybersicherheit unserer Infrastruktur vorzulegen.[1] Diesem Auftrag kommt die Landesregierung nach und legt den geforderten Bericht hiermit vor.

In diesem Bericht ist einerseits auf etliche Teilfragen einzugehen, die sehr unterschiedliche spezifische Bereiche betreffen. Teils liegt die Verantwortung für die betreffenden Fachthemen in einem einzelnen Ressort, teils sind auch mehrere Ressorts beteiligt.

Andererseits bezieht sich die Anfrage auf Querschnittsthemen wie Informations- und Cybersicherheit sowie Digitale Resilienz. Viele Aspekte dieser Themen bearbeitet die Landesverwaltung ressort- und sektorenübergreifend. Somit bestehen erhebliche Schnittmengen der Antworten bei den übergreifenden Aspekten.

Deshalb ist dieser Bericht in mehrere Teile gegliedert und folgendermaßen strukturiert:

- Zunächst stellt die Landesregierung übergreifende Aspekte dar und nimmt dabei auch Begriffsklärungen und Abgrenzungen vor.
- Auf den übergreifenden Teil folgen Ausführungen zu den spezifischen Teilfragen.
- Schließlich gibt die Landesregierung einen Ausblick und stellt laufende und geplante Maßnahmen, Vorhaben und Initiativen vor.

2. Übergreifende Aspekte

2.1. Informations- und Cybersicherheit

Informationssicherheit zielt auf einen angemessenen Schutz der:

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität (Unversehrtheit, Verlässlichkeit)

von Informationen samt deren Verarbeitungsprozessen. Dabei verfolgt die Informationssicherheit einen ganzheitlichen Ansatz – die Schutzziele bestehen unabhängig davon, ob die betreffenden Informationen Personenbezug haben (Datenschutz), als Verschlusssache eingestuft sind (materieller Geheimschutz), es

[1] Drucksache 20/797.

sich um Geschäfts- oder Staatsgeheimnisse oder aus sonstigem Grund zu schützende Informationen handelt.

Zudem geht die Perspektive der Informationssicherheit über reine IT-Sicherheit bzw. Cybersicherheit hinaus und betrachtet auch den Schutz von Informationen beispielsweise auf Papier oder in Köpfen.

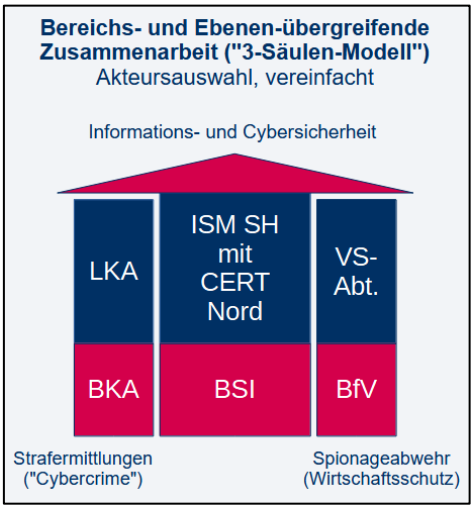
Informationssicherheit verfolgt einen Allgefahrenansatz und betrachtet nicht nur vorsätzliche Taten, sondern auch beispielsweise technische Defekte, Fahrlässigkeit, organisatorische Mängel, Naturereignisse und anderes mehr.

In diesem Sinne ist Cybersicherheit als eine Untermenge der Informationssicherheit zu verstehen. Der Begriff Cybersicherheit wird im Alltag unterschiedlich verwendet.

2.2. Abgrenzung zu Cyberkriminalität und Spionageabwehr

In Schleswig-Holstein wird – wie auf Bundesebene – das sogenannte "3-Säulen-Modell" zur Bereichs- und Ebenen-übergreifenden Zusammenarbeit verwendet:

- Die Säule der Informations- und Cybersicherheit umfasst das federführende Informations- und Cybersicherheitsmanagement der Landesregierung mit der Schnittstelle zum Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Bundesebene.
- Die polizeiliche Säule fokussiert auf die Strafermittlungsaufgaben bei Cyberkriminalität mit den Kernaufgaben Täterermittlung und Beweissicherung. Hier liegt die Schnittstelle zum Bundeskriminalamt auf Bundesebene.
- Die Verfassungsschutzsäule umfasst Tätigkeiten der Spionageabwehr und des Wirtschaftsschutzes im Zuständigkeitsbereich der Verfassungsschutzabteilung und bildet die Schnittstelle zum Bundesamt für Verfassungsschutz.



In allen drei Säulen werden auch Tätigkeiten der Prävention und der Gefahrenabwehr vorgenommen.

2.3. Informationssicherheit und Vertrauen in staatliches Handeln

Demokratie und Rechtsstaatlichkeit benötigen und schaffen Vertrauen in staatliche Institutionen. Dieses Vertrauen wiederum erfordert Transparenz staatlichen Handelns und basiert auf der Gebundenheit an geltendes Recht.

Zudem benötigt der Staat Souveränität in seinen Entscheidungen, auch in der digitalen Welt. Voraussetzungen für digitale Souveränität sind Rahmenbedingungen wie Wahlmöglichkeit, Kontrollierbarkeit und Steuerungsfähigkeit der Grundlagen dieser Entscheidungen.

In den Prozessen staatlichen Handelns spielen digitale Infrastrukturen und Verfahren der Informationsverarbeitung eine immer größere Rolle.

Hohe Informationssicherheit ist ein zentraler Baustein für digitale Souveränität und ein wesentlicher Bestandteil der Vertrauensbasis in ordnungsgemäßes staatliches Handeln. Sie ist eine notwendige Voraussetzung, damit der digitale Wandel gelingt.

2.4. Informationssicherheitsmanagement als "Ermöglicher"

Die Herstellung und Aufrechterhaltung eines angemessenen Schutzniveaus hat ausgesprochenen Prozesscharakter. Das Informationssicherheitsmanagement steuert, organisiert, bewertet und kontrolliert verschiedene, insbesondere übergreifende und strategische Aspekte der Informationssicherheit. An der Umsetzung sind viele Akteure beteiligt – Informationssicherheit ist ein Querschnittsthema.

Informationsverarbeitung findet heute in weiten Teilen digital statt. Aus Sicht der Informationssicherheit stehen wir dabei enormen Herausforderungen gegenüber:

- Die Komplexität der IT-Umgebungen und -Netze steigt immer weiter an.
- Die Gefährdungen in vernetzten IT-Infrastrukturen sind hochgradig asymmetrisch: Wenn die Landesverwaltung zehn Mal angegriffen wird, muss sie bei der Verteidigung zehn Mal Erfolg haben – dem Angreifer reicht ein Mal. Zudem sind fortgeschrittene Angreifer heutzutage mit enormen finanziellen, personellen, zeitlichen und technischen Ressourcen ausgestattet – das stellt die Verteidiger vor neue Herausforderungen.
- Die Abhängigkeit von der digitalen Informationsverarbeitung ist stark gewachsen und besteht heute fast flächendeckend.

Angesichts dieser Herausforderungen reichen isolierte Ad-hoc-Maßnahmen längst nicht mehr aus. Stattdessen bedarf es einer strukturierten und ganzheitlichen Herangehensweise – eines systematischen Informationssicherheitsmanagements.

Das Informationssicherheitsmanagement formuliert übergreifende Strategien und Anforderungen, setzt einen Ordnungsrahmen, ist prozessverantwortlich für Kernprozesse wie Sicherheitsvorfallmanagement oder Risikomanagement, stellt relevante Informationen bereit, initiiert und steuert übergreifende Aktivitäten, bewertet und kontrolliert die Maßnahmenumsetzung und anderes mehr. Damit unterstützt das Informationssicherheitsmanagement insbesondere die Hausleitungen bei der Wahrnehmung ihrer Verantwortung für ordnungsgemäßes Verwaltungshandeln. Zudem berät das Informationssicherheitsmanagement auch das IT-Management sowie die Mitarbeiterinnen und Mitarbeiter bei der Wahrnehmung von deren jeweiligen Aufgaben zur Informationssicherheit.

Angemessenes Informationssicherheitsmanagement ist in diesem Sinne vor allem ein "Ermöglicher" der ordnungsgemäßen Informationsverarbeitung samt ordnungsgemäßem Einsatz technischer Werkzeuge.

2.5. Aktuelle Bedrohungslage

Der BSI-Lagebericht, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, ist ein jährlich erscheinendes Dokument von herausragender Bedeutung für die IT-Sicherheitslandschaft in Deutschland. In einer Zeit, in der die digitale Welt eine immer zentralere Rolle in unserem Alltag sowie in der öffentlichen Verwaltung und Wirtschaft spielt, gewinnt die Sicherheit unserer digitalen Infrastruktur zunehmend an Gewicht. Dieser Lagebericht bietet einen tiefgreifenden Einblick in die aktuelle Bedrohungslage, die Herausforderungen und Entwicklungen im Bereich der Informationssicherheit. Er dient als wichtige Informationsquelle, um die drängenden Fragen der Cybersicherheit in Deutschland zu verstehen und darauf zu reagieren.

Der BSI-Lagebericht dient aber nicht nur als Quelle umfassender Information über die Bedrohungen und Herausforderungen, denen unsere digitale Welt gegenübersteht. Sondern er fungiert auch als Leitfaden für Behörden, Unternehmen und die breite Öffentlichkeit. Von der Analyse der neuesten Angriffsmuster bis hin zu Empfehlungen zur Verbesserung von Sicherheitspraktiken bietet der BSI-Lagebericht eine Ressource, um das Bewusstsein zu schärfen, bewährte Praktiken zu fördern und die IT-Infrastrukturen in Deutschland zu schützen. Der aktuelle Lagebericht bezieht sich auf den Berichtszeitraum: 01.06.2021 bis 31.05.2022.

Die folgende Zusammenfassung wird die Schlüsselergebnisse aus dem BSI-Lagebericht 2022 kompakt präsentieren, um einen klaren Überblick über die wichtigsten Erkenntnisse zu bieten.

Im vorliegenden Berichtszeitraum hat sich die bereits zuvor angespannte Lage im Cyberraum weiter verschärft. Die Bedrohungslage durch Cyberkriminalität erreichte ein nie dagewesenes Niveau, wobei sogenannte Ransomware nach wie vor die vorherrschende Bedrohung für Organisationen darstellt. Zusätzlich traten vermehrt Cyberbedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine auf, darunter sogenannter Hacktivismus durch gezielte Überlastungsangriffe (*Distributed Denial-of-Service,* DDoS) und Kollateralschäden durch Cyber-Sabotage-Angriffe. Sowohl Cyberkriminalität als auch kriegsbezogene Cyberaktivitäten führten zu Störungen in IT-Lieferketten, was die Erhöhung der Resilienz gegenüber Cyberangriffen und technischen Störungen als entscheidende Aufgabe für staatliche, wirtschaftliche und gesellschaftliche Akteure hervorhebt.

Erpressungsmethoden im Cyberraum, insbesondere die Erpressung von erkennbar profitablen Unternehmen und Organisationen durch Verschlüsselung und Diebstahl von Daten – das sogenannte "*Big Game Hunting*" – setzten sich fort. Lösegeld- und Schweigegeldzahlungen sowie die Anzahl der Opfer, deren Daten veröffentlicht wurden, stiegen weiter.

Die Anzahl bekannter Schwachstellen stieg um zehn Prozent im Vergleich zum Vorjahr, wobei mehr als die Hälfte davon hohe oder kritische Bewertungen nach dem gängigen System der Kritikalitätseinstufung (*Common Vulnerability Scoring System*, CVSS) erhielt. Die Schwachstelle in der Software-Komponente "Log4j" wurde als besonders kritisch betrachtet, da sie in vielen frei verfügbaren Anwendungen vorhanden und zudem schwer zu identifizieren war. Dies schuf eine große Verwundbarkeit für Cyberangriffe.

Ebenso wurden im aktuellen Berichtszeitraum vermehrt Angriffe auf sogenannte Perimetersysteme wie Firewalls und Router beobachtet, da diese direkt aus dem Internet erreichbar sind. Zudem wurde eine Zunahme von DDoS-Angriffen verzeichnet, insbesondere während des Online-Shopping-Events "*Cyber Week"* und in der Vorweihnachtszeit.

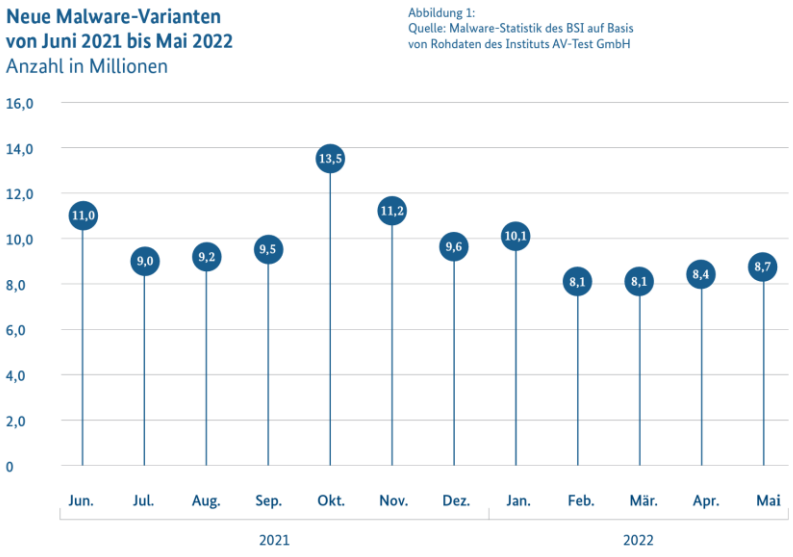
Insgesamt zeigt der Bericht, dass die Bedrohungslage im Cyberraum zunehmend komplex und gefährlich ist, was eine verstärkte Zusammenarbeit und Resilienz auf verschiedenen Ebenen erfordert.

Schadprogramme und neue Varianten

Schadprogramme sind Computerprogramme, die schädliche Aktionen ausführen oder andere Programme dazu befähigen können. Sie gelangen oft über E-Mail-Anhänge oder Webseiten-Links auf Computer. Wenn Nutzer auf einen bösartigen Anhang oder Link klicken, kann sich das Schadprogramm installieren. Gefälschte Webseiten-Links und der Missbrauch legitimer Programme sind auch typische Angriffswege. Schadprogramme nutzen Schwachstellen in Software, Hardware oder Netzwerken, um IT-Systeme zu infizieren. Zudem wird der menschliche Faktor, insbesondere durch psychologisch geschickte direkte Ansprache, das sogenannte *Social Engineering*, immer wichtiger bei Cyberangriffen.

Im Gegensatz zu bekannten Schadprogramm-Varianten können neu entstandene Varianten kurz nach ihrem Auftreten möglicherweise nicht sofort erkannt werden, was sie besonders gefährlich macht. Eine neue Variante eines Schadprogramms entsteht durch Änderungen im Programmcode, wobei jede Variante einzigartig ist in Bezug auf ihre Prüfsumme (Hashwert).

Während des betrachteten Zeitraums stieg die Anzahl neuer Schadprogramm-Varianten um 116,6 Millionen an, wobei täglich durchschnittlich etwa 319.000 neue Varianten hinzukamen. Dies bedeutet einen Rückgang um 19 Prozent im Vergleich zum vorherigen Berichtszeitraum, der durch außergewöhnlich hohe Werte gekennzeichnet war. Obwohl es erhebliche Schwankungen gab, hat sich der Trend wieder normalisiert. Im Sommer 2021 wurden etwa 300.000 neue Varianten pro Tag registriert, während es im Herbst desselben Jahres bis zu 436.000 neue Schadprogramm-Varianten pro Tag gab.

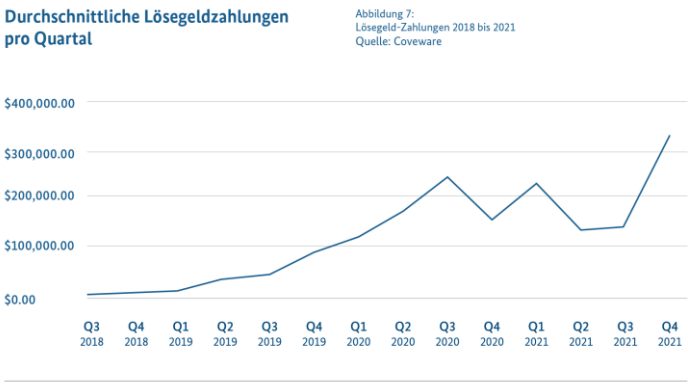


Quelle: Bundesamt für Sicherheit in der Informationstechnik

Ransomware

Ransomware-Angriffe stellen eine erhebliche Bedrohung für staatliche Institutionen, Unternehmen und die Gesellschaft dar. Diese Art von Schadsoftware verhindert den Zugriff auf lokale oder vernetzte Daten und Systeme, verschlüsselt häufig wichtige Nutzerdaten und Dateninfrastrukturen wie Datenbanken. Die Angreifer fordern dann Lösegeld und drohen damit, den einzigen Entschlüsselungsschlüssel zu zerstören. Zusätzlich erpressen sie Opfer, indem sie sensible Daten vor der Verschlüsselung stehlen und mit Veröffentlichung drohen ("*Double Extortion*").

Ransomware-Angriffe umfassen oft die Kombination von Lösegelderpressung und Schweigegelderpressung und erfordern üblicherweise digitale Währungen als Zahlungsmittel, was die Strafverfolgung erschwert. Obwohl hauptsächlich von Cyberkriminellen verübt, könnten auch fortgeschrittene Angreifer mit anderen Motiven – sogenannte APT-Angreifer, oft staatliche oder staatsnahe Akteure – sie zur Verschleierung oder Ablenkung von anderen Angriffen nutzen. In einigen Fällen agiert die Ransomware als sogenannter "Wiper", bei dem die Daten gelöscht und nicht wiederhergestellt werden können.



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Cyberkriminelle Angreifer werden in Gruppen aufgrund ihrer Schadsoftware und Methoden zusammengefasst, und es gibt eine Arbeitsteilung im Bereich der Cyberkriminalität. Diese Arbeitsteilung wird als "*Cybercrime-as-a-Service*" (CCaaS) bezeichnet. Dies ermöglicht es Angreifern, Schritte eines Angriffs als Dienstleistung oder Schadsoftware von anderen Kriminellen zu beziehen. Das BSI betrachtet dies als einen treibenden Faktor für die Zunahme dieser Bedrohung.

Katastrophenfall nach Ransomware-Angriff auf Kreisverwaltung

Im Juli 2021 wurde in Sachsen-Anhalt die Landkreisverwaltung Anhalt-Bitterfeld Opfer eines Ransomware-Angriffs, der alle IT-Systeme beeinträchtigte und die Erbringung von Diensten für Bürgerinnen und Bürger unmöglich machte. Der Ausfall der Verwaltungsprozesse hatte erhebliche Auswirkungen auf die Bevölkerung,

insbesondere auf solche, die von ausbleibenden Zahlungen betroffen waren. Der Landkreis erklärte am 09. Juli 2021 den Katastrophenfall, der erst im Februar 2022 aufgehoben wurde, obwohl zu diesem Zeitpunkt noch nicht alle Schäden behoben waren.

Die Ransomware "Grief" wurde als Ursache identifiziert. Die Landkreisverwaltung zahlte kein Lösegeld und die Angreifer veröffentlichten gestohlene Daten auf einer Leak-Seite. Die Ransomware "Grief" wurde als Nachfolger von "DoppelPaymer" identifiziert. Angreifer wechseln häufig ihre Namen, um die Zuordnung zu erschweren.

Die Ermittlungen wurden vom Landeskriminalamt Sachsen-Anhalt und der Staatsanwaltschaft aufgenommen, und das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Land Sachsen-Anhalt, das CERT Nord und andere Akteure unterstützten den Landkreis bei der Bewältigung der Krise und der Analyse der eingesetzten Schadsoftware. Dies geschah in enger Zusammenarbeit mit der Bundeswehr, die ebenfalls zur Unterstützung angefordert wurde.

Schwachstellen in Software-Produkten

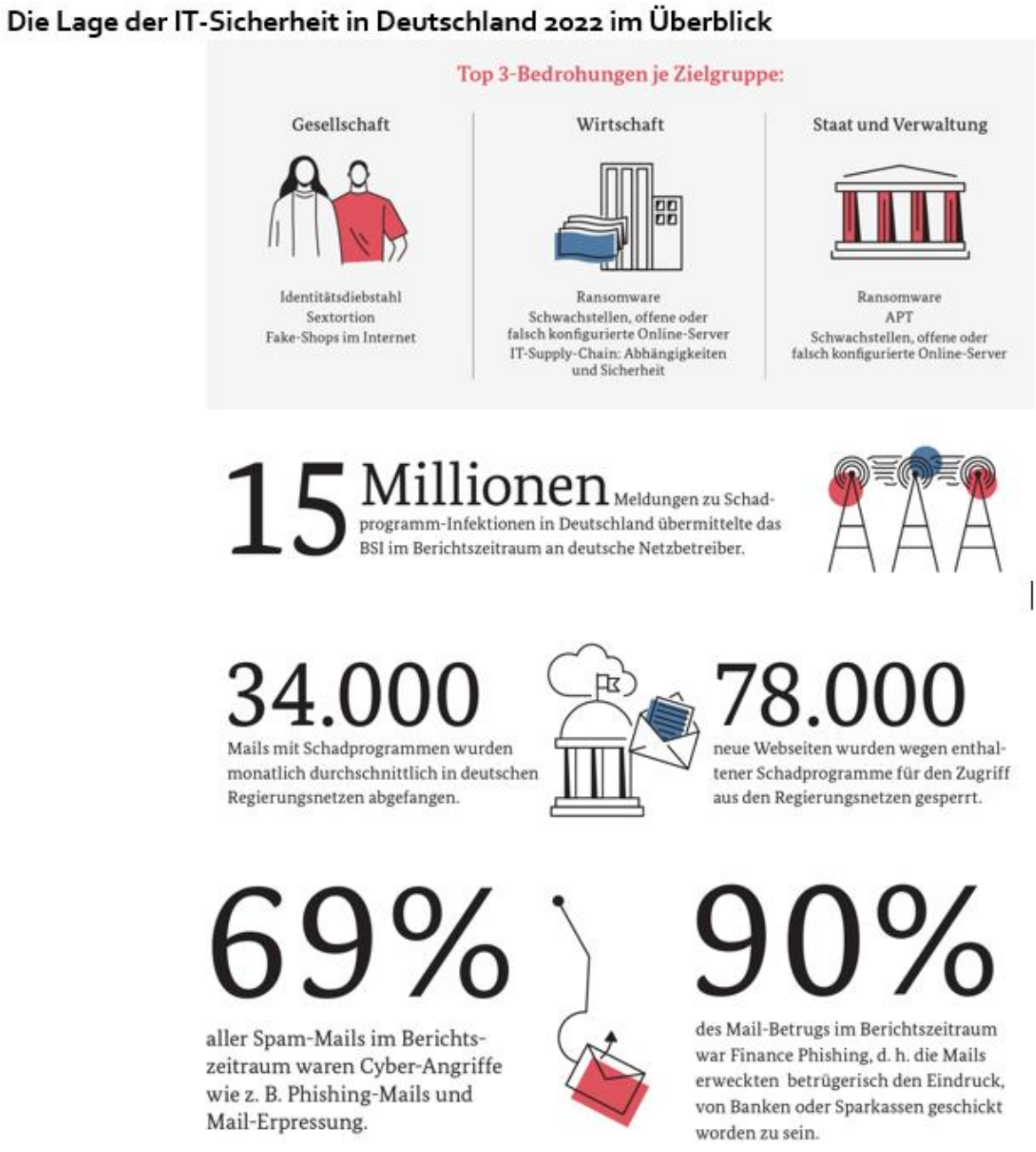
Im aktuellen Berichtszeitraum wurden dem BSI häufig Schwachstellen in der Software von Corona-Testzentren gemeldet, vermutlich aufgrund der Sensibilität der dort gespeicherten Daten. Die Sicherheitslage war überdurchschnittlich bedrohlich, da kritische Schwachstellen in weit verbreiteten Produkten wie Microsoft Exchange und Log4j auftraten. Die Anzahl der bekanntgewordenen Schwachstellen ist insgesamt gestiegen, mit 20.174 Schwachstellen in Software-Produkten im Jahr 2021, was etwa 10 Prozent mehr als im Vorjahr ist. Die Kritikalität der Schwachstellen war gemischt, wobei etwa 13 Prozent als kritisch bewertet wurden. Diese Informationen fließen in den Warn- und Informationsdienst (WID) des BSI ein, der die 150 gängigsten Software-Produkte auf dem deutschen Markt überwacht und über Schwachstellen informiert.

Distributed Denial of Service

Denial-of-Service-Angriffe (DoS-Angriffe) sind gezielte Überlastungsangriffe auf Internetdienste oder andere Systeme, während *Distributed Denial-of-Service* (DDoS) Angriffe mittels mehrerer, meist sehr vieler Systeme gleichzeitig durchgeführt werden. DDoS-Angriffe sind seit über 20 Jahren eine bedeutende Bedrohung für die Cybersicherheit. Eine Studie des Bitkom e. V. bestätigt die Schädlichkeit solcher Angriffe, da 27 Prozent der befragten Unternehmen angaben, innerhalb der letzten zwölf Monate Schäden durch DDoS-Angriffe erlitten zu haben. Das BSI hat im Berichtszeitraum DDoS-Angriffe in einem deutschen Internetprovider-Netz beobachtet, bei denen die durchschnittliche Bandbreite etwa 684 Mbps betrug.

Einige Angriffe erreichten jedoch Bandbreiten von über 200.000 Mbps, mit einem Höchstwert von über 290.000 Mbps bei einem Angriff am 2. Dezember 2021. Die durchschnittliche Bandbreite dieses Angriffs betrug 50.000 Mbps. Im Allgemeinen zeigen die beobachteten DDoS-Angriffe im Berichtszeitraum einen rückläufigen Trend in Bezug auf die durchschnittliche Bandbreite. Dies ist darauf zurückzuführen, dass Angreifer vermehrt auf Netzwerk- und Transportebenen abzielen, anstatt hohe Bandbreiten zu nutzen, und dabei präziser vorgehen, um Überlastungen im Zielnetzwerk effizient auszulösen.

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Insgesamt verdeutlicht der BSI-Lagebericht die Dringlichkeit der Stärkung der Informationssicherheit in Deutschland und liefert wertvolle Informationen, wie sich Organisationen und die Gesellschaft insgesamt besser gegen Cyberbedrohungen schützen können. Die Zusammenarbeit, Sensibilisierung und Investitionen in Informationssicherheit werden in den kommenden Jahren von entscheidender Bedeutung sein. Damit verbunden ist der Aufbau von Personal für Informationssicherheit als steuernder und unterstützender Faktor enorm wichtig.

Die öffentliche Verwaltung verwaltet eine Fülle von sensiblen Informationen, die von persönlichen Daten der Bürgerinnen und Bürger bis hin zu staatlichen Geheimnissen reichen. Die Etablierung spezialisierten Personals für Informationssicherheit ist von zentraler Bedeutung:

- Schutz sensibler Informationen: Die öffentliche Verwaltung verwaltet und speichert eine Fülle von sensiblen Daten, darunter persönliche Informationen, medizinische Aufzeichnungen, Steuerdaten und vieles mehr. Der Verlust oder die Kompromittierung dieser Informationen kann schwerwiegende Auswirkungen auf die Privatsphäre und die Sicherheit der Bürgerinnen und Bürger haben. Die Bereitstellung von Fachpersonal für Informationssicherheit ist entscheidend, um diese Informationen vor unbefugtem Zugriff und Datenverlust zu schützen.

- Schutz vor Cyberangriffen: Die öffentliche Verwaltung ist ein attraktives Ziel für Cyberangriffe, sei es von kriminellen Hackern, staatlichen Akteuren oder Hacktivisten. Ein spezialisiertes Informationssicherheitsteam kann frühzeitig potenzielle Bedrohungen erkennen, Abwehrmaßnahmen ergreifen und die Auswirkungen von Angriffen minimieren.

- Gewährleistung von Rechenschaftspflicht: Die Bürgerinnen und Bürger haben das Recht zu wissen, dass ihre Daten und Informationen in der öffentlichen Verwaltung sicher aufbewahrt werden. Ein starkes Informationssicherheitsteam gewährleistet Transparenz und Erfüllung der Rechenschaftspflicht in Bezug auf Sicherheitspraktiken und Datenverwaltung.

- Einhaltung gesetzlicher Vorschriften: Die öffentliche Verwaltung unterliegt einer Vielzahl von gesetzlichen Vorschriften und Datenschutzbestimmungen. Die Nichteinhaltung dieser Vorschriften kann zu rechtlichen Konsequenzen führen. Ein dediziertes Informationssicherheitsteam kann die Leitung wesentlich dabei unterstützen, alle Vorschriften einzuhalten.

- Bewahrung des öffentlichen Vertrauens: Ein effektives Informationssicherheitsteam trägt dazu bei, das Vertrauen der Bürgerinnen und Bürger in die öffentliche Verwaltung aufrechtzuerhalten. Wenn

Bürgerinnen und Bürger wissen, dass ihre Daten sicher sind, sind sie eher bereit, mit Behörden zusammenzuarbeiten und Informationen bereitzustellen.

- Proaktive Risikominimierung: Informationssicherheit ist keine einmalige Aufgabe, sondern erfordert eine kontinuierliche Überwachung und Anpassung an neue Bedrohungen. Ein Informationssicherheitsteam kann proaktiv Schwachstellen identifizieren und Maßnahmen ergreifen, um diese zu beheben, bevor sie ausgenutzt werden.
- Schutz der nationalen Sicherheit: In einigen Fällen kann die öffentliche Verwaltung auch für die Sicherung von Staatsgeheimnissen und Informationen über kritische Infrastrukturen verantwortlich sein. Ein spezialisiertes Informationssicherheitsteam trägt wesentlich zu diesem Schutz bei.

Angesichts dieser Gefährdungslage ist angemessene Informationssicherheit mehr denn je eine Grundvoraussetzung der Digitalisierung und des Verwaltungshandelns insgesamt.

3. Spezifische Aspekte

3.1. Bedrohungen durch Cyber-Kriminelle, Cyber-Angriffe und Fälle von Cyber-Erpressung in Schleswig-Holstein

Vorangestellt sei, dass die Fallzahlen ausweislich der Polizeilichen Kriminalstatistik (PKS) sowohl bundesweit als auch in Schleswig-Holstein seit Jahren zunehmen. Seit dem Jahr 2019 ist ein Anstieg i. H. v. 39,58% festzustellen.

	2019	**2020**	**2021**	**2022**
Cybercrimetaten Schleswig-Holstein*	2.125 Taten	2.476 Taten	3.035 Taten	2.966 Taten

*gemäß PKS-Summenschlüssel 897000

Cybercrimeangriffe nehmen seit Jahren kontinuierlich zu. Die rasant voranschreitende Digitalisierung aller Gesellschaftsbereiche geht einher mit neuen Kriminalitätsfeldern und Herausforderungen für die Polizei, die u. a. in einer sukzessiven Zunahme der Delikte des Cybercrime mit immer höherem Schadens- und Bedrohungspotential zu sehen sind. Phänomene der Cyberkriminalität unterliegen dabei einem stetigen und insbesondere schnellen Wandel und sind darüber hinaus in ihrer Komplexität stark variabel. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt auch 2022 in ihrem Jahresbericht zu der Einschätzung: „Die Gefährdungslage im Cyber-Raum ist so hoch wie nie“ (BSI-Jahresbericht 2022, S. 11).

Dies liegt zum einen an immer wieder auftretenden Sicherheitslücken, beispielsweise von verbreitet eingesetzter Software, die täterseitig ausgenutzt werden und sodann eine Vielzahl an Behörden, Unternehmen und anderen Einrichtungen treffen können. Sogenannte Lieferkettenangriffe (*Supply-Chain*-Angriffe) stellen Cyberangriffe auf Hersteller von IT-Produkten oder andere Einrichtungen in Lieferketten dar, bei denen durch Manipulation der jeweiligen Produkte eine weite Verbreitung von Schadsoftware erfolgt. Zum anderen sind unmittelbare und/oder mittelbare Auswirkungen des russischen Angriffskrieges auf die Ukraine nicht ausgeschlossen. Kriegerische Akte finden auch im Cyber-Raum statt bzw. strahlen in diesen aus. In diesem Zusammenhang sind u. a. die durch die Gruppierung „NoName057“ vorgenommenen und mutmaßlich politisch motivierten Überlastungsangriffe auf die Webseiten vieler Landes- und Bundesbehörden im April 2023 zu benennen, bei denen auch in Schleswig-Holstein das Landesportal über viele Stunden nicht erreichbar gewesen ist.

Bezogen auf Unternehmen, Behörden und sonstige Institutionen, einschließlich der kritischen Infrastruktur, stellen Erpressungen mittels eingesetzter Ransomware auch weiterhin die Hauptbedrohung dar. Hierbei werden ganze Server bzw. die darauf gespeicherten Daten entwendet und verschlüsselt. Das potentielle Schadensausmaß ist enorm und mündet nicht selten in die Insolvenz des betroffenen Unternehmens. Der Branchenverband Bitkom schätzt den bundesweiten Schaden allein durch entsprechende Erpressungstaten für das Jahr 2022 auf 10,7 Milliarden Euro. Eine im Jahr 2022 durchgeführte Umfrage ergab eine entsprechende Betroffenheit von 73% unter den befragten Unternehmen (Studie „Ransomware: The true cost to Business Study 2022“). Oftmals wird das Lösegeld an die Tätergruppierungen gezahlt, da dieses meist geringer ausfällt, als der wirtschaftlich zu erwartende Schaden. Das Dunkelfeld dürfte nach übereinstimmenden Schätzungen beträchtlich sein.

Von den circa 2,6 Millionen kleinen und mittelständischen Unternehmen in Deutschland sind nach Einschätzung des BSI, aber auch nach Erkenntnissen der Landespolizei Schleswig-Holstein, eine beträchtliche Anzahl nur unzureichend gegen Cyberangriffe geschützt. Oftmals sind keine Maßnahmen der Angriffserkennung oder auch IT-Notfallpläne implementiert.

Die Bedrohungslage wird daher auch für Schleswig-Holstein von polizeilicher Seite aus als sehr hoch eingeschätzt. Gefährdet sind neben jeglichen Unternehmen auch Behörden, u. a. Kommunalverwaltungen, sowie Krankenhäuser und die kritische Infrastruktur. Zu entsprechenden Vorfällen ist es bundesweit bereits mehrfach gekommen. Angriffe auf hiesige Behörden, Verwaltungen und/oder kritische Infrastruktur werden daher als wahrscheinlich bis sehr wahrscheinlich eingeschätzt.

3.2. Personelle Situation in der Landesverwaltung in Bezug auf die Cybersicherheit

3.2.1. Allgemeine personelle Situation

Das Informations- und Cybersicherheitsmanagement (ISM) der Landesregierung gliedert sich in zwei Bereiche:

- übergreifendes Informations- und Cybersicherheitsmanagement unter Leitung des *Chief Information Security Officers* (CISO) der Landesregierung
- Informationssicherheitsmanagement in der Staatskanzlei und in den Ressorts

Diese Bereiche sind personell sehr heterogen aufgestellt.

Gemäß den Anforderungen der aktuellen Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein sind neben der CISO-Funktion auch die Funktionen der Informationssicherheitsbeauftragten (ISB) in der Staatskanzlei und in den Ressorts zu besetzen. Diese Beauftragtenfunktionen samt Stellvertretung sind weitgehend eingerichtet. Zukünftig ist darauf zu achten, dass diese auch vollständig besetzt sind. Bei Besetzung mit Stellenanteilen sind zudem häufig Rollenkonflikte festzustellen, beispielsweise im Fall gleichzeitiger Aufgabenwahrnehmungen im IT-Management oder in der IT-Haushaltsplanung in Personalunion. Auch hinsichtlich der organisatorischen Einordnung der Stellen im Informationssicherheits-management strebt die Landesregierung die Vermeidung von Rollenkonflikten an. Dabei orientiert sich die Landesregierung an den in den BSI-Standards vorgesehenen Zielen.

In den letzten Jahren konnten tragfähige Strukturen in einigen Bereichen aufgebaut und unterschiedliche Rollen im Informationssicherheitsmanagement personell ausgestattet werden. Beispielsweise in der Justiz wurde ein Team unter Leitung des Informationssicherheitsbeauftragten aufgebaut, in dem auch Informationssicherheitskoordinatorinnen und -koordinatoren sowie verfahrensspezifische Informationssicherheitsbetreuerinnen und -betreuer jeweils spezifische Aufgaben der Informationssicherheit wahrnehmen. In einigen anderen Bereichen wurden ähnliche Strukturen aufgebaut, wiederum andere Bereiche sind noch nicht so weit fortgeschritten.

Generell ist festzuhalten, dass gutes Informations- und Cybersicherheitsmanagement wesentlich auf angemessener Personalausstattung und angemessenen organisatorischen Rahmenbedingungen basiert. Angesichts der derzeitigen und für die absehbare Zukunft zu erwartenden Bedrohungslage liegt für das Informations- und Cybersicherheitsmanagement hier eine zu bewältigende Herausforderung. Dies gilt insbesondere für den CISO-Funktionsbereich. Hier nimmt derzeit lediglich eine Person Aufgaben wahr, die in anderen Ländern zum Teil mit mehreren Personen

wahrgenommen werden. Aktuell wird der Bereich Informationssicherheit verstärkt. Um eine der enormen und gewachsenen Bedeutung des Informationssicherheits-managements angemessene Aufgabenerfüllung sicherzustellen, ist eine weitere Verstärkung angezeigt – sowohl im CISO-Funktionsbereich als auch in der Landesverwaltung insgesamt.

Das ist auch deshalb sinnvoll, um die Wirtschaftlichkeit von Maßnahmen der Informationssicherheit insgesamt zu verbessern. Denn die Organisation der Informationssicherheit in der Landesverwaltung sieht vor, übergreifende Angelegenheiten auch übergreifend zu bearbeiten bzw. zu koordinieren. Durch eine weitere Zentralisierung der Aufgaben können Mehrfachaufwände in den Ressorts für Wahrnehmung dieser Aufgaben vermieden werden. Deshalb ist die Landesregierung entschlossen, sich diesen Herausforderungen mit höchster Priorität und schnellstmöglich zu stellen.

3.2.2. Aus- und Fortbildung, Zertifizierungen

Die Landesregierung strebt ein einheitliches Mindestniveau der Aus- und Fortbildung der ISBs und der weiteren Beschäftigten im Informationssicherheitsmanagement an, das sich an standardisierten Curricula orientiert. Von besonderer Bedeutung sind dabei folgende Formate:

- Informationssicherheitsbeauftragte für die öffentliche Verwaltung, 3 Wochen, ehemals von der Bundesakademie der öffentlichen Verwaltung (BAköV) auch für ISBs aus den Ländern angeboten, derzeit werden eigene Rahmenverträge der Länder erarbeitet, Zertifikat möglich
- IT-Grundschutz-Praktiker nach BSI-Curriculum, 3 Tage, Personenzertifizierung möglich
- Einführungs- und Fortgeschrittenenschulungen im ISMS-Tool SH
- Angebote der internen Schulung, insbesondere hinsichtlich der ISM- und Verwaltungsspezifika in Schleswig-Holstein

Neben diesen Standardangeboten werden weitere, individuelle Schulungen und Fortbildungen nach Bedarf angestrebt. Zudem wird der Bereich IT-Notfallmanagement als Teil des *Business Continuity Managements* wachsende Bedeutung auch hinsichtlich Schulungen erfahren.

Bei der Schulungskonzeption findet ressortübergreifende Zusammenarbeit im Rahmen des AG ISM statt.

3.2.3. Fachkräftemangel

Selbst vorhandene Stellen können oft nicht mit geeignetem Personal besetzt werden. Hier hat die Landesregierung erheblichen Bedarf für die nächsten Jahre erkannt, die Situation zu verbessern, derzeit insbesondere in folgenden Bereichen:

- Auf- und Ausbau interner Angebote der Personalentwicklung zur Wahrnehmung von Aufgaben im Bereich Informationssicherheitsmanagement
- Steigerung der Attraktivität der Arbeitsplätze in der Landesverwaltung im Bereich Informationssicherheitsmanagement
- Ausbau der externen Personalunterstützung in Bereichen, in denen dieses möglich ist – allerdings sind gerade im sensitiven Bereich Informationssicherheitsmanagement viele Aufgaben dauerhaft durch eigenes Personal der Landesverwaltung zu erbringen

3.2.4. Zusammenarbeit mit dem CERT Nord

Das CERT Nord benötigt zur Wahrnehmung seiner Aufgaben engmaschigen Kontakt zum Informationssicherheitsmanagement in den Trägerländern, insbesondere zum jeweiligen CISO-Funktionsbereich. Das erfordert entsprechende Erreichbarkeit im Informationssicherheitsmanagement. Gerade die Kommunikation zwischen dem CISO-Funktionsbereich und dem CERT Nord ist häufig von hoher Dringlichkeit. Durch die allgemeine personelle Situation (siehe oben, Abschnitt 3.2.1) ist auch die Zusammenarbeit mit dem CERT Nord in Schleswig-Holstein aktuell von besonders großen Herausforderungen geprägt. Hier ist eine personelle Verstärkung angezeigt.

3.2.5. Informationssicherheitsaufgaben im IT-Management und in anderen Bereichen

Komplementär zum Informationssicherheitsmanagement sind auch im IT-Management Aufgaben der Informationssicherheit wahrzunehmen. Hierbei handelt es sich primär um Umsetzungsaufgaben auf Seite der Landesverwaltung, die nicht an den IT-Dienstleister übertragen werden können. Das sind beispielsweise Aufgaben im Anforderungsmanagement oder zur Erstellung und Pflege der Teilsicherheitskonzepte auf Seite der Landesverwaltung. Zudem handelt es sich um Aufgaben der Dienstleistersteuerung.

Hierfür benötigen die jeweiligen IT-Verantwortlichen[2] der Fachverfahren Unterstützung und Zuarbeit. Hier ist eine personelle Verstärkung angezeigt.

Zudem ist Informationssicherheit ein Querschnittsthema, das alle Mitarbeiterinnen und Mitarbeiter betrifft. Auch als reine Nutzerin oder reiner Nutzer von

[2] Rolle "IT-Verantwortung" im Sinne des Standardrollenmodells ITSH.

Informationstechnik ist Vertrautheit mit dem sicheren Umgang auf Basis entsprechender Schulung erforderlich.

3.3. Cybersicherheit in der Energieversorgung

Cybersicherheit in der Energieversorgung ist bundesweites Thema, das wesentlich vom BSI und von der Bundesnetzagentur (BNetzA) behördlich begleitet wird. Energieanlagen sind so zu errichten und zu betreiben, dass die technische Sicherheit gewährleistet ist.

Das BSI ist die zentrale Cybersicherheitsbehörde auf Bundesebene. Es entwickelt Standards und Leitlinien für die Informationssicherheit in kritischen Infrastrukturen (KRITIS), zu denen auch die Energieversorgung gehört.[3] Das BSI unterstützt Betreiber von KRITIS bei der Umsetzung von Sicherheitsmaßnahmen und überwacht die Einhaltung der gesetzlichen Anforderungen. Danach sind KRITIS-Betreiber verpflichtet, angemessene Maßnahmen zur Gewährleistung der Cybersicherheit zu treffen. Hierzu gehören unter anderem Risikoanalysen, Notfallpläne und regelmäßige Sicherheitsaudits.

Bei Sicherheitsvorfällen oder Störungen, die die IT-Systeme oder die Versorgung beeinträchtigen könnten, besteht eine Meldepflicht des Anlagenbetreibers an das BSI. Diese Meldepflicht gilt auch für erhebliche Cyberangriffe oder entsprechende Verdachtsfälle. Die Meldepflicht gemäß § 8b Absatz 4 BSI-Gesetz (BSIG) betrifft Betreiber Kritischer Infrastrukturen, die anhand der in der BSI-Kritisverordnung (BSI-KritisV) festgesetzten Schwellenwerte als Kritische Infrastrukturen im Sinne des BSIG identifiziert wurden. Mit Inkrafttreten des "Gesetzes zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinien-Umsetzungsgesetz) am 30.06.2017 erweitert sich diese Meldepflicht von Betreibern von Energieversorgungsnetzen, deren Anlagen nach der BSI-KritisV als Kritische Infrastrukturen bestimmt wurden, auf alle Energieversorgungsnetzbetreiber.

Eine weitere Meldepflicht ergibt sich aus dem § 52 des "Gesetzes über die Elektrizitäts- und Gasversorgung" (Energiewirtschaftsgesetz, EnWG), wonach Betreiber von Energieversorgungsnetzen einen jährlichen Bericht an die BNetzA

[3] Weitere Hinweise des BSI zu branchenspezifischen Sicherheitsstandards für den Energiesektor: <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/Energie/Branchenspezifische-Sicherheitsstandards/branchenspezifische-sicherheitsstandards_node.html>.

übermitteln müssen.[4] Sofortige Meldepflichten für Störungen mit überregionalen Auswirkungen richten sich nach § 13 Absatz 8 EnWG.

Zusätzlich ist auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) mit der Beschreibung möglicher Ausfälle im Energiesektor und der Erarbeitung von Schutzkonzepten betraut.

Auf Landesebene haben die Betreiber von Energieanlagen gemäß § 49 EnWG auf Verlangen der nach Landesrecht zuständigen Behörde Auskünfte über technische und wirtschaftliche Verhältnisse zu geben. Eine spezifische landesbehördliche Zuständigkeit für Aspekte der Informations- und Cybersicherheit der betreffenden Einrichtungen im Land besteht nicht.

3.4. Cybersicherheit bei den in Rückbau befindlichen Atomkraftwerken

Im Ministerium für Energiewende, Klimaschutz, Umwelt und Natur (MEKUN) ist die Abteilung 3 – Technischer Umweltschutz, Reaktorsicherheit und Strahlenschutz – zuständig für die kerntechnischen Standorte Brunsbüttel, Brokdorf, Krümmel und Hereon sowie für den Strahlenschutz in Einrichtungen und Anlagen außerhalb der Kerntechnik innerhalb des Landes Schleswig-Holstein.

Zur Ausgestaltung dieser Aufgabe gehört die Durchführung der atomrechtlichen und der strahlenschutzrechtlichen Genehmigungs- und Aufsichtsverfahren für die im Nachbetrieb bzw. im Rückbau befindlichen Kernkraftwerke und für die in Errichtung befindlichen Läger für nicht Wärme entwickelnde Abfälle an den oben genannten Standorten. Darüber hinaus ist die Abteilung 3 zuständig für die Aufsicht über die an den Standorten befindlichen Zwischenläger für Wärme entwickelnde Abfälle (in Castoren).

Die strahlenschutzrechtlichen Genehmigungs- und Aufsichtsaufgaben in allen nicht-kerntechnischen Institutionen in Medizin, Wirtschaft, Forschung und Lehre des Landes Schleswig-Holstein werden innerhalb des Referates V34 bearbeitet.

Im Rahmen von atomrechtlichen bzw. strahlenschutzrechtlichen Genehmigungsverfahren findet eine vollständige Überprüfung der Auslegung und des Betriebes von IT-Komponenten in den Anlagen und Einrichtungen gestuft nach ihrer sicherheitstechnischen Bedeutung statt. Bei Änderungen oder Instandsetzungen von Anlagenteilen bzw. Komponenten ist die Bewertung hinsichtlich IT-Relevanz und Auslegung ein Bestandteil des Verfahrens.

[4] Weitere Hinweise der BNetzA zu IT-Sicherheitskatalogen für den Energiesektor und Zertifizierungen: <https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/start.html>.

Für Anlagen der 12. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (BImSchV) – Störfallanlagen – hat der Betreiber die notwendigen Maßnahmen zu treffen, um den Betriebsbereich gegen Eingriffe Unbefugter zu sichern (§3 der 12. BImSchV). Das schließt Maßnahmen der Cybersicherheit ein. Dies ist im Sicherheitskonzept und im Sicherheitsbericht des Betreibers zu dokumentieren. Für Anlagen der kritischen Infrastruktur sowie zukünftig auch für alle Betriebsbereiche der oberen Klasse sind das BBK und das BSI die zuständigen Behörden für die Cybersicherheit.

Grundsätzlich ist für die Einhaltung der Informationssicherheit der jeweilige Betreiber der Anlage zuständig. Dies gilt ebenso für die Umsetzung und Einhaltung der Meldeverpflichtung von besonderen Vorkommnissen der IT-Sicherheit gegenüber der Aufsichtsbehörde und dem BSI. Die Vorgaben der Meldeverpflichtung sind in betrieblichen Regelungen verankert und konkretisiert. Sie orientieren sich unter anderem an den diesbezüglichen bundesweiten Vorgaben.

Für die Informationssicherheit im atom- und strahlenschutztechnischen Bereich gibt es bundesweite Regelungen im Bereich der Anlagensicherung – Lastannahmen (nach Verschlusssachenanweisung eingestuft im Grad VS-V), Anforderungen, Maßnahmen – die als Bewertungsmaßstab für den Betreiber und die Behörde heranzuziehen sind. Dies sind im Einzelnen:

- Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT); nach Verschlusssachenanweisung eingestuft im Grad VS-NfD
- Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III); nach Verschlusssachenanweisung eingestuft im Grad VS-NfD
- Richtlinie zur Sicherung sonstiger radioaktiver Stoffe in kerntechnischen Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie sonstige radioaktive Stoffe in Kerntechnischen Anlagen - SisoraK); nach Verschlusssachenanweisung eingestuft im Grad VS-NfD
- Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen (SEWD-Richtlinie sonstige radioaktive Stoffe - SisoraSt); nach Verschlusssachenanweisung eingestuft im Grad VS-NfD

und für weitergehende IT-Anforderungen:

- BSI-Normen
- DIN-Normen

Innerhalb dieser bundesweiten Regelungen gilt es gestuft nach ihrer sicherheitstechnischen Bedeutung Sicherheitskonzepte, Sicherheitsanalysen und Sicherheitsnachweise zur Informationssicherheit zu erstellen und der Behörde vorzulegen. Die Behörde überprüft im jeweiligen Verwaltungsverfahren unter Hinzuziehung von IT-Expertinnen und -Experten die eingereichten Dokumente. Die Geheimhaltung der Regelungen ist Teil des Sicherungskonzeptes.

Im aufsichtlichen Verfahren überprüft die Behörde in regelmäßigen Abständen die Einhaltung der Vorgaben der Informationssicherheit durch den Betreiber. Hierzu werden unter Teilnahme der Behörde und unter Hinzuziehung von externer IT-Expertise die IT-relevanten Bereiche geprüft (Fachanweisungen, IT-Auffälligkeiten, Schutzmaßnahmen, installierte Technik usw.)

Grundsätzlich folgt der Aufbau der Informationssicherheit in den kerntechnischen Einrichtungen einem "*Defence-in-Depth*"-Konzept. Der Zugriff auf die Systeme folgt diesem Konzept und berücksichtigt die Bedrohungen über "*Air Gaps*" (Stick, WLAN) gleichermaßen durch technische und administrative/organisatorische Maßnahmen. Ebenfalls gibt es Regelungen für das Einbringen von Software und die Härtung von Komponenten (z. B. Servicegeräte).

In regelmäßigen Fachgesprächen auf Länder- und Bundesebene unter Einbindung des BSI findet ein gezielter Austausch zu den Aspekten der Informationssicherheit statt. Das entsprechende Regelwerk wird kontinuierlich auf dessen Aktualität überprüft und angepasst.

In besonderen Lagen informiert das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) bzw. das BSI die zuständigen Stellen der Länder auf direktem Wege über eingetretene bzw. zu erwartende IT-Vorfälle.

Durch den Ausstieg aus der Kerntechnik zählen die Kernkraftwerke nicht mehr zu den Einrichtungen der Daseinsvorsorge. Zudem gehören die Kernkraftwerke nach Einstellung des Leistungsbetriebes nicht mehr zur KRITIS.

Als eine Vorsorgemaßnahme für die Unterstützung der Stäbe im Katastrophenfall sind beteiligte Stellen und Personen im Ministerium benannt. Der Aufgabenbereich dieser Stellen und Personen beinhaltet unter anderem besondere Kenntnisse im Strahlenschutz, in der Katastrophen- und Notfallorganisation sowie in der

Stabsarbeit. Dieser Aufgabenbereich umfasst darüber hinaus auch Belange der Informationssicherheit in kerntechnischen Anlagen und Vertrautheit mit dem gesamten IT-Regelwerk im atom- und strahlenschutztechnischen Bereich.

3.5. Cybersicherheit in der Wasserver- und -entsorgung

Die Cybersicherheit in der Wasserver- und -entsorgung liegt in der Verantwortung insbesondere jener, die betreffende kritische Infrastrukturen betreiben. Die Herstellung und Aufrechterhaltung eines angemessenen Niveaus der Cybersicherheit setzt unter anderem voraus:

- ein entsprechendes Problembewusstsein und die Bereitschaft zur Auseinandersetzung mit diesen Themen
- die Bereitstellung notwendiger Ressourcen sowie
- eine konsequente Umsetzung erforderlicher Maßnahmen

Angesichts der Vielzahl der Akteure im Bereich der öffentlichen Hand bedarf es einer übergeordneten fachlichen Unterstützung. Denn sonst könnten die speziellen IT-Sicherheitsanforderungen in organisatorischer und technischer Hinsicht insbesondere kleinere Kommunen und Betreiber überfordern. Hier ist zentral und ressortübergreifend auch das Land gefordert.

Die Abteilung V 4 des MEKUN ist als oberste Landesbehörde fachlich zuständig für die Wasserwirtschaft, den Boden- und den Küstenschutz. Dazu zählen die der Daseinsvorsorge zuzurechnenden Infrastrukturen für die Wassergewinnung, die Abwasserbeseitigung, die Entwässerung des Binnenlandes sowie den Hochwasser- und Küstenschutz.

In der originären Zuständigkeit des Landes befinden sich die Anlagen des Küstenschutzes der ersten Deichlinie (u. a. Deiche, Schöpf- und Sperrwerke), die landeseigenen Häfen (Federführung im Ministerium für Wirtschaft, Verkehr, Arbeit, Technologie und Tourismus – MWVATT –, Vollzug im MEKUN und im Landesbetrieb für Küstenschutz, Nationalpark und Küstenschutz – LKN.SH) und die Unterhaltung der Gewässer 1. Ordnung.

Für den Betrieb und die Instandhaltung der Abwasseranlagen (Kanalnetze, Pumpwerke, Abwasserbehandlungsanlagen für Schmutz- und Niederschlagswasser) sind die abwasserbeseitigungspflichtigen Körperschaften (Städte, Gemeinden, Zweckverbände, Wasser- und Bodenverbände) zuständig, über die die unteren Wasserbehörden der Kreise und kreisfreien Städte die Fachaufsicht ausüben.

Die Unterhaltung der Gewässer 2. Ordnung einschließlich des Betriebes der dazu gehörigen Anlagen wie der Deiche und Schöpfwerke liegt in der Zuständigkeit der

Wasser- und Bodenverbände. Die Verbands- und Fachaufsicht üben die Kreise und kreisfreien Städte aus.

Der Geschäftsbereich beinhaltet keine spezifische landesbehördliche Zuständigkeit für Aspekte der Informations- und Cybersicherheit der betreffenden Einrichtungen im Land. Vielmehr gehört es zu originären Aufgaben eines jeden Anlagenbetreibers, den ordnungsmäßen Betrieb sicherzustellen. Dazu zählt auch der Schutz technischer Anlagen vor Cyberangriffen und anderen Risiken der Informationssicherheit.

Die Abteilung 4 des MEKUN übt die Fachaufsicht gegenüber dem LKN.SH und den unteren Wasserbehörden aus. Eine besondere aufsichtsbehördliche Funktion hinsichtlich der Informations- und Cybersicherheit besteht nicht. Entsprechend gibt es keine fachliche Expertise in der Fachabteilung, um sich mit diesen Fragestellungen vertieft auseinanderzusetzen und ggf. sogar initiativ zu werden.

Formalisierte landesbehördliche Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen nach speziellen Rechtsvorschriften gibt es nicht. Die Anlagenbetreiber melden Störfälle welcher Art auch immer ihren Aufsichtsbehörden. Weitere spezifische landesrechtliche Anforderungen für Maßnahmen der Informations- und Cybersicherheit bestehen nicht.

Die Anlagen der Wasserver- und -entsorgung, die Anlagen zur Entwässerung des Binnenlandes und zum Schutz vor Hochwasser sowie die Anlagen des Küstenschutzes sind essentielle Bestandteile der Daseinsvorsorge. Akteure sind das Land, die wasserversorgungs- und abwasserbeseitigungspflichtigen Körperschaften und die Wasser- und Bodenverbände für die von ihnen jeweils wahrzunehmenden Aufgaben.

Im Ministerium ist eine Kontaktperson für KRITIS für den Bereich der Abwasserbeseitigung benannt.

3.6. Cybersicherheit im Katastrophenschutz

Die Systeme der Informations- und Kommunikationstechnik für den Katastrophenschutz in Schleswig-Holstein sind aufgrund der unterschiedlichsten Gefahrenlagen und mitwirkenden Akteure ressort- und verwaltungsebenen-übergreifend zu betrachten.

Für die Bewältigung von Katastrophenlagen gibt es Führungsstäbe, die sich für Ihre Organisationseinheiten überwiegend der vorhandenen Bürokommunikation bedienen. Hierfür greifen die Informationssicherheitsstrukturen, die in den Verwaltungen bzw. bei deren IT-Betreibern etabliert sind. Für den Führungsstab Katastrophenschutz auf Landesebene befinden wir uns dabei in einer geschlossenen

Benutzergruppe des Landesnetzes, so dass hier die gleichen Abwehrmaßnahmen gegen Cyberattacken gelten, wie für die übrige Landesverwaltung.

Für das Informationsmanagement in dem Führungsstab Katastrophenschutz des Landes und für den Informationsaustausch mit den polizeilichen Stäben wird die eine spezifische Fachanwendung verwendet. Für diese wurde gemäß geltenden BSI-Standards eine den besonderen Verfügbarkeits- und sonstigen Anforderungen entsprechende Schutzbedarfsfeststellung durchgeführt. Darauf aufbauend erfüllt die Fachanwendung die entsprechenden Anforderungen im Sinne der IT-Grundschutz-Methodik des BSI.

Viele Informationen zur Erzeugung eines Lagebildes kommen aus Internetportalen und Fachanwendungen der zuständigen Fachbehörden, die überwiegend in den Rechenzentren des IT-Dienstleisters des Landes (Dataport AöR) gehostet werden.

Darüber hinaus gibt es weitere Kommunikationsverbindungen welche über Sondernetze abgestützt sind. So besitzen alle Führungsstäbe einen Meldekopf im BOS-Digitalfunk, welcher drahtlose Kommunikation mit missionskritischem Inhalt ermöglicht. Die Cybersicherheit wird hier in Verantwortung der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) gewährleistet.

Jegliche Kommunikation mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) bezüglich der Warnung und Unterrichtung der Bevölkerung geschieht in dem modularen Warnsystem MoWaS des Bundes, welches sich auf ein geschlossenes Kommunikationssystem stützt. Die Sicherheitsvorgaben legt das BBK fest und sie werden technisch durch die operativen Partner umgesetzt.

Die Kommunikation im 24/7/365 Betrieb zur Übermittlung von Lagemeldungen erfolgt über ein System für formelle Kommunikation. Dieses System besitzt eine sogenannte obere Netzebene, welche durch das Bundeskriminalamt (BKA) betrieben wird und die Bund-/Länderkommunikation abdeckt. Die Kommunikation zwischen polizeilichen Dienststellen des Landes und der Ebene der unteren Katastrophenschutzbehörden in der sogenannten unteren Netzebene wird von der Landespolizei verantwortet. Hier gelten die einschlägigen Sicherheitsstandards, deren Umsetzung die Landespolizei mit Dataport vereinbart hat.

Für die Alarmierung der Einsatzkräfte der täglichen Gefahrenabwehr wird die sogenannte digitale Alarmierung verwendet. Sie kommt vielerorts auch für die Alarmierung von Katastrophenschutzeinheiten zum Einsatz. Der Betrieb dieser Infrastruktur wird auf Grundlage des Brandschutzgesetzes und des Rettungsdienstgesetzes von den Kreisen und kreisfreien Städten verantwortet. Die Alarmierungsnetze übertragen unidirektional die für die Alarmierung von

Einsatzkräften notwendigen Informationen an Funkmeldeempfänger und ggf. auch an Sirenen. Auch wenn die Informationsübertragung nahezu flächendeckend verschlüsselt erfolgt, ist eine unzulässige Weiterverarbeitung der Informationen durch grundsätzlich zum Empfang berechtigte Stellen nicht auszuschließen.

3.7. Cybersicherheit in der kommunalen Verwaltung

Im föderalen Kompetenzgefüge regeln die Kommunen ihre Angelegenheiten in eigener Verantwortung.[5] Im Sinne dieser verfassungsrechtlichen Zuständigkeiten sind die Kommunen auch für die Informations- und Cybersicherheit ihrer Verwaltungen eigenverantwortlich tätig.

Die Verbesserung der Informations- und Cybersicherheit auf kommunaler Ebene hat – im Rahmen der verfassungsrechtlichen Zuständigkeiten – strategische Bedeutung auch für die Landesverwaltung. Deshalb unterstützt die Landesregierung die Kommunen bei der Herstellung und Aufrechterhaltung eines angemessenen Informations- und Cybersicherheitsniveaus in den kommunalen Verwaltungen.

In bestimmten Fällen befinden sich Land und Kommunen in einem gemeinsamen Sicherheitsverbund, beispielsweise bei Ebenen-übergreifenden Fachverfahren, bei einem kommunalen Anschluss ans Landesnetz oder bei der Mitnutzung von Basis- und Onlinediensten nach dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG). Auch nimmt im Zuge der Umsetzung des OZG die Anzahl der Ebenen übergreifenden elektronischen Verfahren stark zu, an denen sowohl Land als auch Kommunen beteiligt sind.

Deshalb betrachtet die Landesregierung die eigene Informations- und Cybersicherheit sowie die kommunale Informations- und Cybersicherheit nicht losgelöst voneinander. Die Landesregierung unterstützt die Kommunen beispielsweise mit den nachstehend beschriebenen Maßnahmen.

3.7.1. Projekt "Sicherheit für Kommunen in Schleswig-Holstein", SiKoSH

Die Landesregierung finanziert und steuert übergreifend das Projekt "Sicherheit für Kommunen in Schleswig-Holstein" (SiKoSH). Im Rahmen dieses Projektes, das vom übergreifenden Informations- und Cybersicherheitsmanagement der Landesregierung in Zusammenarbeit mit dem IT-Verbund Schleswig-Holstein AöR (ITV.SH) durchgeführt wird, erhalten Kommunen Unterstützung insbesondere beim Einstieg in ein systematisches Informationssicherheitsmanagement und bei dessen Aufrechterhaltung und Weiterentwicklung.

[5] Vgl. insbesondere Art. 28 GG.

Damit wird es Kommunen erleichtert, ihren Verpflichtungen zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen samt deren Verarbeitung nachzukommen – auch in gemeinsamen Informations- und Sicherheitsverbünden mit dem Land.

Im öffentlichen Sektor kommt vor allem ein Informationssicherheitsmanagement gemäß den einschlägigen Standards des BSI zur Anwendung. Ein solches zu initiieren und neu aufzubauen kann gerade für kleinere Kommunalverwaltungen mit hohen Einstiegshürden versehen sein.

Das Projekt SiKoSH setzt genau hier an und senkt die Einstiegshürden. Den Kommunen werden systematische Einstiegshilfen und Unterstützung beispielsweise in folgender Form angeboten:

- Beratung und Information
- Checklisten zur Feststellung des aktuell vorhandenen Status
- Methodik für den Informationssicherheitsprozess
- Kriterien für die Priorisierung von Maßnahmen
- Musterdokumente für die Sicherheitskonzeption und deren laufende Fortschreibung
- Umsetzungsbegleithilfen wie Selbsttests zum Soll-Ist-Vergleich

Die SiKoSH-Hilfsmittel sind vollständig kompatibel zu den BSI-Standards. Dadurch können die Kommunen sukzessive weitere Maßnahmen zur vollständigen Umsetzung der BSI-Standards auf dem mit SiKoSH erreichten Stand aufsetzen.

Um die SiKoSH-Kompatibilität mit den BSI-Standards dauerhaft zu erhalten, steht die Landesverwaltung in kontinuierlichem Austausch mit dem BSI.

Zudem findet aus dem SiKoSH-Projekt heraus eine Mitarbeit an der Weiterentwicklung des sogenannten Grundschutzprofils Kommunale Basisabsicherung statt. Ein Grundschutzprofil ist eine Zusammenstellung typischer Sicherheitsanforderungen samt geeigneten Schutzmaßnahmen gemäß BSI-Standards für einen abgegrenzten Anwendungsbereich – in diesem Fall für den Anwendungsbereich typischer Kerntätigkeiten einer Kommunalverwaltung mit Maßnahmen für eine Basisabsicherung. Grundschutzprofile stellen eine praxisorientierte Umsetzungsunterstützung für die anwendenden Einrichtungen dar.

3.7.2. Information und Sensibilisierung

Das Informationssicherheitsmanagement der Landesregierung erhält aus unterschiedlichen Quellen aktuelle Informationen und Warnhinweise beispielsweise

zu akuten Gefährdungen. Einige dieser Informationen sind auch für die kommunale Ebene relevant. Deshalb steuert die Landesverwaltung bestimmte Informationen im Rahmen verfügbarer Kapazitäten auch an Informationssicherheitsbeauftragte aus Kommunen in Schleswig-Holstein.

Derzeit findet diese Informationsdistribution primär in Zusammenarbeit mit dem ITV.SH statt und nutzt dortige Verteilmechanismen. Die Landesregierung beabsichtigt eine Ausweitung der Warn- und Informationsdienste für Kommunen und befindet sich bereits in entsprechenden Verhandlungen mit den anderen Trägern des CERT Nord (siehe unten, Abschnitt 3.8, Cybersicherheit in der Landesverwaltung, und Abschnitt 4, Ausblick).

Zudem befindet sich die Landesregierung in Vorbereitung eines Webinar-Formates mit dem Titel "Roadshow Kommunen" gemeinsam mit dem BSI und unter Einbeziehung der kommunalen Spitzenverbände und des ITV.SH. Dabei handelt es sich um eine gemeinsame virtuelle Informations- und Sensibilisierungsveranstaltung, die sich an die Kommunen richtet und erstmalig 2024 angeboten werden soll. Inhaltlich sind insbesondere Beiträge zu aktuellen Themen der Informationssicherheit sowie zu Unterstützungsangeboten im Rahmen des übergreifenden Informationssicherheitsmanagements der Landesregierung vorgesehen.

3.7.3. Fachtagungen und Vernetzung

Das Informationssicherheitsmanagement der Landesregierung beteiligt sich regelmäßig mit Vorträgen, Workshops und Vernetzungsaktivitäten an einschlägigen Fachtagungen. Dazu gehören insbesondere die beiden folgenden Veranstaltungen für den öffentlichen Sektor, die sich spezifisch auch an Mitarbeitende im Informationssicherheitsmanagement von Kommunen richten:

- Kommunaler IT-Sicherheitskongress der kommunalen Spitzenverbände unter Federführung des Deutschen Landkreistages
- Jahrestagung für Informationssicherheitsbeauftragte aus Ländern und Kommunen des IT-Planungsrates

An diesen jeweils jährlich durchgeführten Veranstaltungen nehmen regelmäßig auch Vertreterinnen und Vertreter von Kommunen aus Schleswig-Holstein teil. Um die Teilnahmehürde möglichst niedrig zu halten, wurden die Kosten für die Durchführung beider Veranstaltungen in den letzten Jahren regelmäßig zentral aus den Mitteln der AG Informationssicherheit des IT-Planungsrates getragen.

Auf diesen Fachkongressen ist auch das SiKoSH-Projekt (siehe oben) bereits vorgestellt worden und stieß bundesweit auf erhebliches Interesse und positive Resonanz.

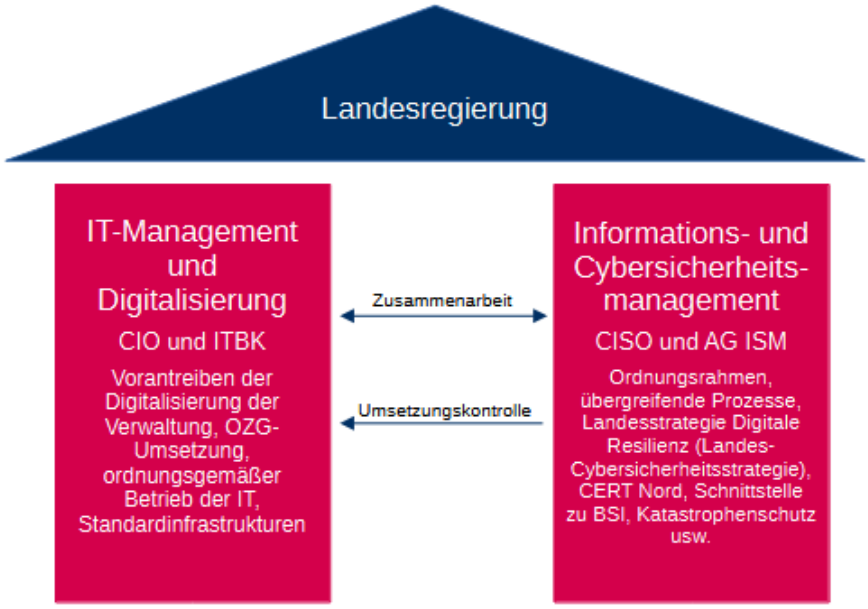
3.8. Cybersicherheit in der Landesverwaltung

Modernes Verwaltungshandeln ist in hohem Maße abhängig von zuverlässig und ordnungsgemäß funktionierender Informationsverarbeitung. Das Ziel der Informationssicherheit ist es, Informationen jeglicher Art und Herkunft zu schützen, insbesondere die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen und ihrer Verarbeitung zu gewährleisten. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Die Digitalisierung der Verwaltungsarbeit in den Landesbehörden in Schleswig-Holstein nimmt stetig zu. Gleichzeitig ist ein stetiger Anstieg von Bedrohungen der informationsverarbeitenden Systeme festzustellen. Durch die zunehmenden Bedrohungen steigen die Anforderungen an die Gewährleistung der Informationssicherheit, wobei die Gefährdungen der Informationssicherheit sowohl technische als auch nicht-technische, insbesondere organisatorische, Aspekte umfassen. Es besteht die Herausforderung, die Informationssicherheit in allen Bereichen der Landesverwaltung aufrecht zu erhalten und im Lichte der sich ständig ändernden Gefährdungslage kontinuierlich zu verbessern und dabei den Grundsatz der Wirtschaftlichkeit zu beachten.

Die Landesregierung stellt sich dieser Herausforderung und bekennt sich zu ihrer Verantwortung für die Gewährleistung von Informationssicherheit in der Landesverwaltung.

Das übergreifende Informations- und Cybersicherheitsmanagement der Landesregierung ist eine eigenständige und komplementäre Struktur neben dem IT-Management der Landesverwaltung. Beide Bereiche stehen aber in enger Beziehung zueinander.



Die Strategien, Regelungen und Anforderungen des übergreifenden Informationssicherheitsmanagements stellen einen Ordnungsrahmen dar, der über die Landesverwaltung hinausgeht.

Für den Bereich der öffentlichen Verwaltung haben sich Bund und Länder auf eine bestimmte Art des Informationssicherheitsmanagements verständigt. Schleswig-Holstein ist auf die Umsetzung der betreffenden BSI-Standards verpflichtet (sog. IT-Grundschutz-Methodik auf Basis von ISO 27001 ff.). Im Rahmen dieser Standards sind technische und organisatorische Maßnahmen auf drei Handlungsebenen umzusetzen:

- Prävention: Verletzungen der Schutzziele sollen möglichst vermieden werden.
- Detektion: Wenn Schutzziele verletzt werden, soll dieses möglichst frühzeitig erkannt werden.
- Reaktion: Wenn eine Verletzung von Schutzzielen erkannt wurde, soll sachgerecht reagiert werden.

Gemäß BSI-Standards wird hierbei ein ganzheitlicher Ansatz verfolgt:

Methodisch ist die Anwendung einer spezifischen Systematik hervorzuheben, wodurch bestimmte Kernaufgaben der Informationssicherheit sich unter Einbeziehung aller Beteiligten mit ihren jeweiligen Aufgaben vergleichsweise effizient wahrnehmen lassen.

Übergreifende Aspekte betreffen insbesondere die Organisation, den Betrieb und die Weiterentwicklung des Informationssicherheitsmanagements selbst. Zu den Kernprozessen des Informationssicherheitsmanagements gehören beispielsweise:

- Sicherheitsvorfallmanagement
- Risikomanagement
- IT-Notfallmanagement als Teil des ganzheitlichen Notfallmanagements bzw. *Business Continuity Managements* (s. u.)
- Audits und Revisionen
- Ausnahmemanagement
- Berichtswesen
- Formulierung bestimmter übergreifender Anforderungen
- Informationssteuerung, Sensibilisierung, Schulung

Bei der Erstellung verfahrens- und infrastrukturspezifischer Sicherheitskonzepte führt eine klare und systematische Abgrenzung von betrachteten Teilverbünden zu einer Art Modularisierung, die Mehrfachaufwände vermeidet und Transparenz hinsichtlich der jeweiligen Aufgaben auf Seite der Landesverwaltung und auf Seite des Dienstleisters erzeugt.

Ausgangspunkt der Erstellung einer Sicherheitskonzeption ist der jeweilige Geschäftsprozess. In diesem Geschäftsprozess werden bestimmte Informationen verarbeitet, diese Verarbeitung findet auf bestimmten IT-Systemen statt, diese befinden sich in bestimmten Räumen und kommunizieren über bestimmte Netzverbindungen, die Verarbeitung findet unter bestimmten organisatorischen Rahmenbedingungen statt und involviert bestimmte Personen und Rollen sowie bestimmte Dienstleister. Für diesen Gesamtverbund wird – ausgehend vom Geschäftsprozess – der jeweilige Schutzbedarf festgestellt. Dieser kann normal, hoch oder sehr hoch sein; die Kriterien für diese Kategorisierung sind ressortübergreifend abgestimmt.

Betrachtete Bedrohungen umfassen insbesondere:

- vorsätzliche Taten
- technische Defekte
- organisatorische Mängel
- höhere Gewalt, beispielsweise Hochwasser oder Pandemien
- menschliches Fehlverhalten, Fahrlässigkeit

Dabei finden folgende Schadensszenarien Berücksichtigung, und zwar jeweils hinsichtlich des Schutzes der Vertraulichkeit, Verfügbarkeit und Integrität:

- Verstoß gegen Gesetze, Verträge und andere Vorschriften
- Beeinträchtigung der Aufgabenerfüllung
- Negative Außenwirkung
- Finanzielle Auswirkungen
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung des informationellen Selbstbestimmungsrechts

Zudem wurden in der Landesverwaltung Schleswig-Holstein gemeinsam mit dem Datenschutzmanagement Synergien identifiziert und entsprechende Kriterien ressortübergreifend abgestimmt. Beispielsweise kann eine derart vorgenommene Schutzbedarfsfeststellung direkt als Grundlage der datenschutzrechtlichen Schwellwertanalyse herangezogen werden.

Die jeweils zu ergreifenden Sicherheitsmaßnahmen richten sich nach dem jeweils festgestellten Schutzbedarf.

In der Vorgehensweise gemäß BSI-Standards folgen weitere Schritte, beispielsweise Regelüberprüfungen (Soll-Ist-Vergleiche) oder Maßnahmen des systematischen Risikomanagements einschließlich der Offenlegung etwaiger Restrisiken gegenüber dem jeweiligen Risikoträger oder der jeweiligen Risikoträgerin.

Das übergreifende Informationssicherheitsmanagement umfasst auch das übergreifende IT-Notfallmanagement. Auch in diesem Bereich sind Informationssicherheitsmanagement und IT-Management jeweils eigene, komplementäre Strukturen nebeneinander. Das übergreifende IT-Notfallmanagement als Teil des ganzheitlichen Notfallmanagements der Landesregierung stellt einen Ordnungsrahmen dar, innerhalb dessen das IT-Management geeignete Maßnahmen und Prozesse umsetzt.

Das IT-Management und dessen Digitalstrategie sind hinsichtlich der umzusetzenden Maßnahmen und Prozesse zur Informationssicherheit eingebettet in diesen übergreifenden und strategischen Ordnungsrahmen.

3.8.1. Organisation der Informations- und Cybersicherheit in der Landesverwaltung

Mit der Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein legt die Landesregierung den übergreifenden Rahmen der Informationssicherheit verbindlich fest. Grundlage ist ein umfassendes Informationssicherheitsmanagement auf Basis des IT-Grundschutzes und der entsprechenden BSI-Standards sowie der entsprechenden ISO-Normenreihe zur Informationssicherheit.

Diese Leitlinie gilt in der unmittelbaren Landesverwaltung Schleswig-Holstein. Der Landesrechnungshof und die Präsidentin des Landtages Schleswig-Holstein können die Regelungen in ihrem Zuständigkeitsbereich für anwendbar erklären. Diese Anwendbarkeitserklärung haben beide Behörden abgegeben.

Diese Leitlinie findet im Bereich der Justiz keine Anwendung, sofern die Regelungen des IT-Gesetzes für die Justiz des Landes Schleswig-Holstein (ITJG) und die auf dieser Grundlage getroffenen Bestimmungen und Regelungen dem entgegenstehen.

Anderen Trägern der öffentlichen Verwaltung steht die Anwendung dieser Leitlinie offen.

Die vom IT-Planungsrat auf Grundlage des IT-Staatsvertrags verabschiedete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung verpflichtet die Länder zur Erstellung einer Informationssicherheitsleitlinie und zum Aufbau eines Informationssicherheitsmanagementsystems auf Basis des BSI-IT-Grundschutzes[6]. Durch die gemeinsame Leitlinie für Informationssicherheit von Bund und Ländern soll sichergestellt werden, dass dem jeweiligen Schutzziel angemessene und dem Stand der Technik sowie dem Grundsatz der Wirtschaftlichkeit entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Sicherheitsvorfällen weitestgehend zu verhindern und mögliche Schäden zu minimieren. Es wird ein Sicherheitsniveau angestrebt, das festgelegten Mindestanforderungen genügt und keine hohen Risiken akzeptiert.

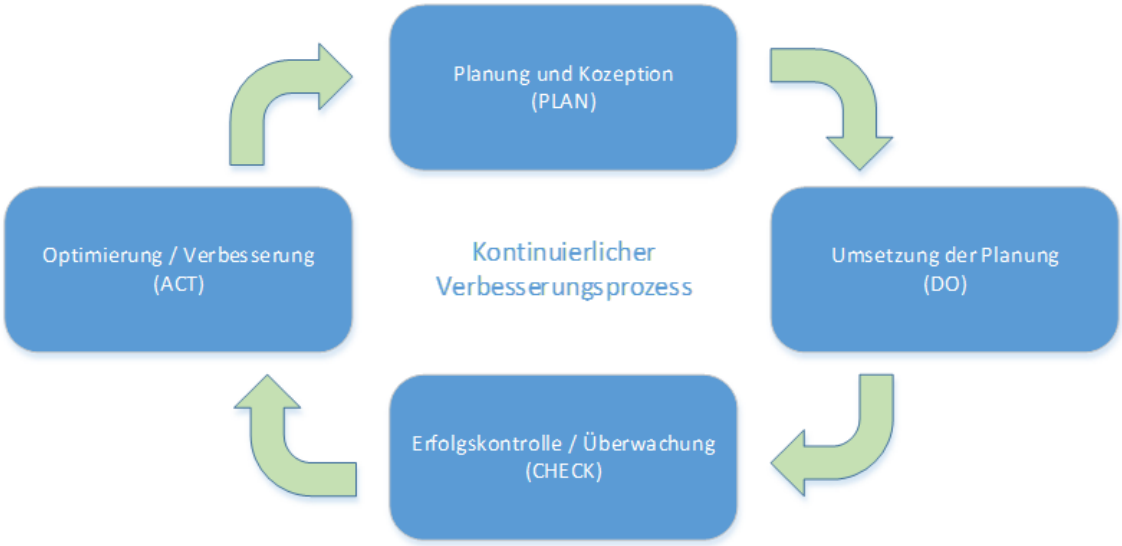
Zur Sicherung und Weiterentwicklung des Informationssicherheitsniveaus wird ein Informationssicherheitsmanagementsystem (ISMS) mit entsprechender Dokumentation sowie relevanten Prozessen eingeführt. Das ISMS wird im Rahmen der nachfolgend beschriebenen Organisation der Informationssicherheit unter Leitung des CISOs mit Unterstützung der dezentralen Informationssicherheitsbeauftragten umgesetzt. Alle im Geltungsbereich dieser Leitlinie beteiligten Behörden haben dafür Sorge zu tragen, dass die abgestimmten ressortübergreifenden Vorgaben und Standards eingehalten werden. Diese können durch eigene Vorgaben und Standards erweitert werden, wobei die vorgegebenen Mindeststandards nicht unterschritten werden dürfen.

Die Festlegungen der Mindestsicherheitsstandards leiten sich ab insbesondere aus den Bestimmungen des BSI-IT-Grundschutzes in der jeweils aktuellen Fassung, aus der entsprechenden ISO 2700x-Normenreihe und deren Umsetzungsempfehlungen sowie aus den datenschutzrechtlichen Anforderungen. Die entsprechenden

[6] Alternativ können die Mitglieder des IT-Planungsrates ein gleichwertiges anderes Informationssicherheitsmanagementsystem verwenden.

Anforderungen der Rechnungshöfe sowie vorgegebene Mindeststandards im Rahmen der Bund-/Länder-Zusammenarbeit sind zu berücksichtigen.

Das Vorgehen im ISMS folgt einem ganzheitlichen PDCA-Modell (*Plan-Do-Check-Act*, Planung-Durchführung-Überprüfung-Aktualisierung):



Zur Erreichung der Ziele der Informationssicherheit sind Schutzbedarfe bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie deren Verarbeitung zu ermitteln. Anhand der ermittelten Schutzbedarfe müssen risikoorientiert Maßnahmen geplant und umgesetzt werden. Bei IT-Vorhaben und IT-Verfahren sind Schutzbedarfsfeststellung und Maßnahmenplanung Aufgaben der jeweiligen IT-Verantwortlichen gemäß Standardrollenmodell ITSH. Dabei werden sie von dem jeweils zuständigen Informationssicherheitsmanagement unterstützt.

Auf der Basis dieser Maßnahmen ist das erforderliche Sicherheitsniveau aufrecht zu erhalten. Bei IT-Vorhaben und -Verfahren trifft diese Verpflichtung sowohl die IT-Verantwortlichen als auch diejenigen, die das IT-Verfahren nutzen.

Weiterhin bestehen als zentrale Ziele für die Informationssicherheit:

- die Wirkung von Sicherheitsmaßnahmen zu stärken,
- eine lückenlose Umsetzung der Informationssicherheitskonzepte,
- die Umsetzung der speziellen datenschutzrechtlichen Anforderungen,
- die Unterstützung des Notfallmanagements im Zusammenhang mit der Verfügbarkeit von Systemen durch proaktive und reaktive Sicherheitsmaßnahmen.

Für die Aufrechterhaltung der Informationssicherheit und die Erreichung der Ziele gilt der Grundsatz der Wirtschaftlichkeit. Alle Maßnahmen der Informationssicherheit müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen stehen.

3.8.1.1. CISO und Informationssicherheitsbeauftragte

Der CISO hat einen strategischen Fokus. Er leitet das übergreifende Informations- und Cybersicherheitsmanagement der Landesregierung und plant, steuert und koordiniert dieses. Zudem kontrolliert er die Umsetzung der Maßnahmen. Er berichtet direkt an die Hausleitung.

Die Staatskanzlei und die Ministerien bestimmen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB). Es gibt eine Stellvertretung. Entsprechendes gilt für jene obersten Landesbehörden, die diese Leitlinie fakultativ für anwendbar erklären. Bei Bedarf können für weitere Organisationsbereiche zuständige Mitarbeiterinnen und Mitarbeiter für die Informationssicherheit benannt werden, beispielsweise bei Ämtern, die nach § 5 Abs. 2 Landesverwaltungsgesetz (LVwG) einer obersten Landesbehörde zugeordnet sind, bei den Landesoberbehörden oder innerhalb eines organisatorisch selbstständigen Teils einer obersten Landesbehörde.

Die oder der ISB steuert das Informationssicherheitsmanagement in ihrem oder seinem Zuständigkeitsbereich und wirkt auf die Aufrechterhaltung und kontinuierliche Verbesserung hin. Dazu arbeitet er oder sie eng mit den IT-Verantwortlichen in seinem oder ihrem Bereich zusammen und berät diese bei ihrer Aufgabenwahrnehmung.

Bei der organisatorischen Zuweisung der Aufgaben sollen Rollen- und Interessenkonflikte vermieden werden. Den Beauftragten sind ausreichende Zeitanteile zur Wahrnehmung ihrer Aufgaben einzuräumen und die Möglichkeit zu angemessener Aus- und Fortbildung zu gewähren.

3.8.1.2. AG Informationssicherheitsmanagement (AG ISM)

Die Schnittstelle zwischen dem zentralen und den dezentralen Bereichen bildet das ressortübergreifende Arbeitsgremium Informationssicherheitsmanagement (AG ISM). Das AG ISM setzt sich mindestens aus dem CISO (Vorsitz) und den benannten ISB der obersten Landesbehörden im Geltungsbereich der Leitlinie zusammen. Das Gremium hat sich eine Geschäftsordnung gegeben, in der auch Näheres zur Aufnahme weiterer Mitglieder und deren Stimmberechtigung geregelt ist.

Das AG ISM koordiniert landesweit die Maßnahmen der Informationssicherheit und sorgt für eine geeignete Informationssicherheitsorganisation sowie ein angemessenes Berichtswesen. Es kann Mindeststandards beschließen, die im

betreffenden Geltungsbereich bindend sind; Näheres regelt eine Richtlinie auf Basis der Informationssicherheitsleitlinie.

Der CISO und die ISBs tauschen sich im AG ISM regelmäßig über den Status der Informationssicherheit in ihren Zuständigkeitsbereichen aus.

In beratender Funktion sind auch Datenschutzbeauftragte sowie die Prüfbehörden Landesrechnungshof und das Unabhängige Landeszentrum für Datenschutz (ULD) im AG ISM vertreten. Zudem sind das CERT Nord und das Informationssicherheitsmanagement von Dataport eingebunden.

3.8.1.3. Verantwortung der Behördenleitung

Bei der Behördenleitung liegt die Gesamtverantwortung für die Ordnungsmäßigkeit der IT-Verfahren und die Informationssicherheit im jeweiligen Zuständigkeitsbereich. Bei Zentralen IT-Verfahren liegt die Verfahrensverantwortung bei der jeweiligen zentralen Stelle; hier ist eine dezentrale Behördenleitung im Sinne einer geteilten Verantwortung verantwortlich für die jeweilige dezentrale Umsetzung der zentralen Vorgaben und entsprechende Maßnahmen. Die Behördenleitung trägt dafür Sorge, dass die Mitarbeiterinnen und Mitarbeiter die entsprechenden Vorgaben und Anforderungen berücksichtigen. Im Sinne der Vorbildfunktion kommt dem eigenen Sicherheitsverhalten der Behördenleitung besondere Bedeutung zu.

Die Behördenleitung veranlasst in ihrem Zuständigkeitsbereich komplementär zur Umsetzung der Regelungen des Organisationserlasses ITSH, dass:

- bei obersten Landesbehörden im Geltungsbereich der Leitlinie eine oder ein ISB samt Stellvertretung für diese oberste Landesbehörde benannt werden,
- bei Bedarf weitere Mitarbeitende für die Informationssicherheit samt deren jeweiliger Zuständigkeit benannt werden,
- die erforderlichen Ressourcen für eine angemessene Informationssicherheit zur Verfügung gestellt werden,
- die übergreifenden Regelungen zur Informationssicherheit sowie gegebenenfalls die ergänzenden Regelungen im Ressort umgesetzt werden,
- die Wirksamkeit und Umsetzung der Informationssicherheitsregelungen sowie -maßnahmen regelmäßig überprüft werden
- bedarfsgerechte Risikoanalysen zu den Aufgaben der Informationsverarbeitung des jeweiligen Zuständigkeitsbereichs durchgeführt werden,

- die Verantwortlichkeiten im Umgang mit Informationen definiert und gegenüber den Mitarbeiterinnen und Mitarbeitern kommuniziert werden.

Die Behördenleitung lässt sich regelmäßig über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich berichten. Sie entscheidet im Rahmen der zentralen Vorgaben über die Umsetzung angemessener Sicherheitsmaßnahmen und übernimmt für verbleibende Restrisiken die Verantwortung.

3.8.1.4. Mitarbeiterinnen und Mitarbeiter

Informationssicherheit muss durchgehend über alle organisatorischen Ebenen gewährleistet sein. Mitarbeiterinnen und Mitarbeiter sind im Rahmen ihrer allgemeinen Dienstpflichten dafür verantwortlich, Vorgaben zur Informationssicherheit in ihrem Arbeitsbereich zu beachten und einzuhalten. Hierzu müssen die Informationssicherheitsleitlinie und die – gegebenenfalls mitbestimmungspflichtigen – mitgeltenden Richtlinien, Arbeitsanweisungen und sonstige Vorgaben allen Mitarbeiterinnen und Mitarbeitern in jeweils geeigneter Weise bekannt gemacht werden.

Sicherheitsrelevante Ereignisse sind umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können; Näheres ist in einer Richtlinie zum Sicherheitsvorfallmanagement zu regeln.

Den Mitarbeiterinnen und Mitarbeitern sind ausreichende Mittel und Möglichkeiten zur qualifizierten Aus- und Fortbildung in Themen der Informationssicherheit zu gewähren. Dies gilt auch für die spezifische Aus- und Fortbildung der IT-Verantwortlichen im Rahmen ihrer Zuständigkeit bei IT-Vorhaben und -Verfahren.

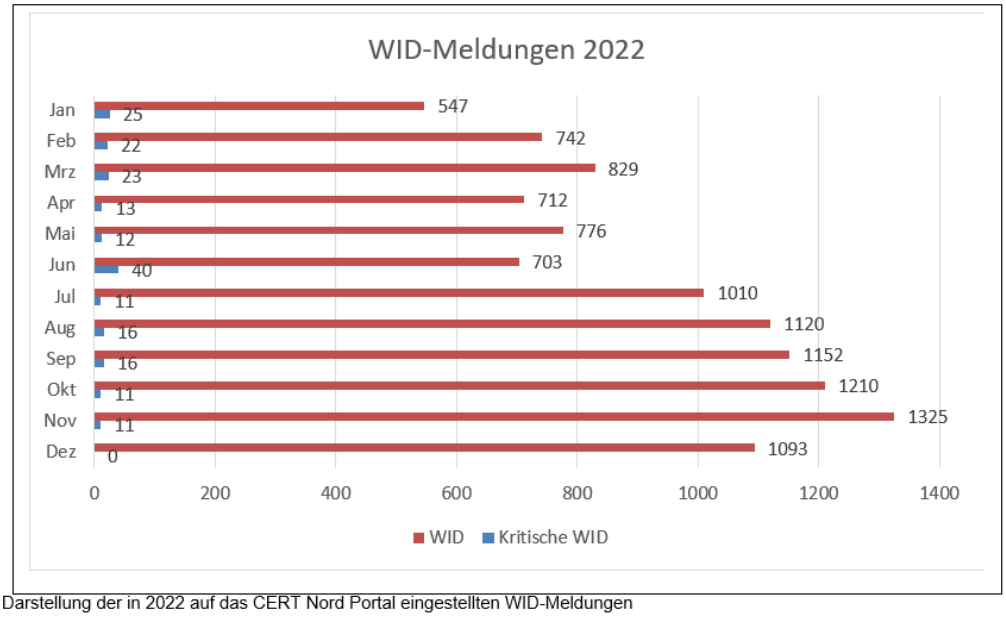
3.8.1.5. CERT Nord

Schleswig-Holstein betreibt gemeinsam mit den Ländern Hamburg, Bremen und Sachsen-Anhalt ein *Computer Emergency Response Team,* das CERT Nord. Dieses gemeinsame Landes-CERT unterstützt das Informationssicherheitsmanagement bei Maßnahmen zur Informationssicherheit, insbesondere dem Sicherheitsvorfallmanagement. Relevante Sicherheitsvorfälle müssen dem CERT Nord gemeldet werden; Näheres hat eine Richtlinie zum Sicherheitsvorfallmanagement zu regeln. Das CERT Nord ist organisatorisch und personaladministrativ bei dem Landesdienstleister Dataport AöR angesiedelt. Das CERT Nord ist aber keine Einrichtung von Dataport, sondern ist den CISOs der Trägerländer unterstellt und berichtet anlassbezogen und regelmäßig über Themen der Informationssicherheit an das zentrale Informationssicherheitsmanagement der Landesverwaltung.

Zu den Kernaufgaben des CERT Nord gehört auch die Bereitstellung eines Warn- und Informationsdienstes (WID) für das Informationssicherheitsmanagement der Landesverwaltungen seiner Träger. Informationen aus unterschiedlichen Quellen

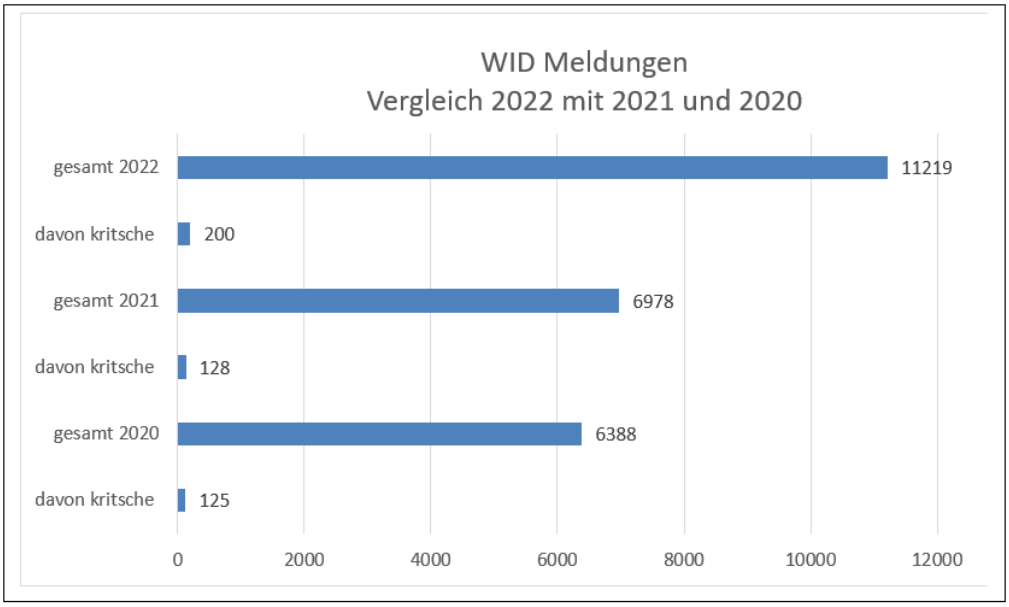
analysiert und bewertet das CERT Nord, bereitet sie auf und verteilt sie an relevante Empfängerkreise.

Im Jahr 2022 hat das CERT Nord über 11.000 derartige Meldungen verarbeitet, davon 200 mit hoher Kritikalität:



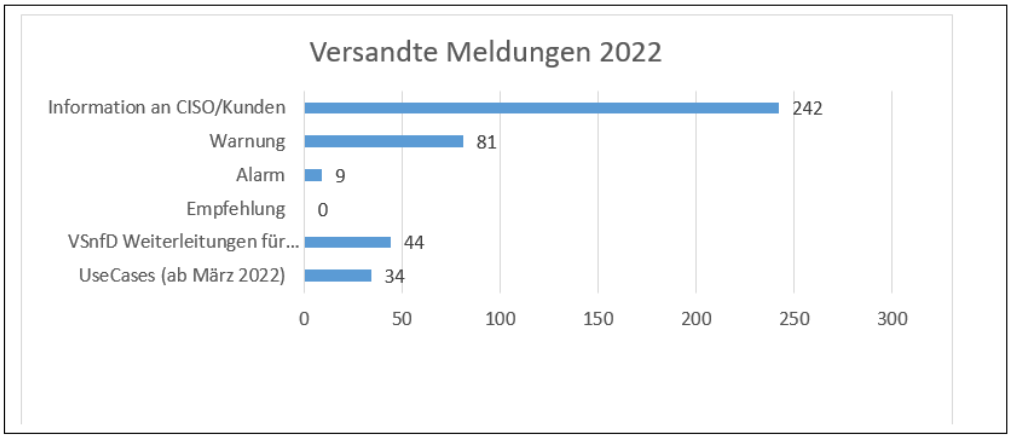
Darstellung der in 2022 auf das CERT Nord Portal eingestellten WID-Meldungen

Im laufenden Jahr 2023 wurde der Vorjahreswert bereits Mitte Oktober übertroffen mit circa 11.400 Meldungen. Im Vergleich mit den Vorjahren ist eine deutliche Steigerung sowohl der Anzahl der Meldungen insgesamt als auch der Meldungen mit hoher Kritikalität zu verzeichnen:



Anstieg der WID Meldungen von im Zeitraum von 2020 bis 2022

Bestimmte relevante Meldungen versendet das CERT Nord direkt an die jeweiligen Zielgruppen:



Darstellung der im Jahr 2022 versandten Meldungen an CISO bzw. alle ISB

3.8.2. Landes-IT-Dienstleister Dataport

Der Landes-IT-Dienstleister Dataport AöR ist der zentrale IT-Dienstleister für weite Teile der Landesverwaltung. Insbesondere der Rechenzentrumsbetrieb für Infrastrukturen und Fachverfahren ist weitgehend dort angesiedelt.

Dataport betreibt ein eigenes Informationssicherheitsmanagement im Rahmen seiner Rolle als Auftragnehmer. Zudem betreibt Dataport ein *Security Operations Center* (SOC) für die insbesondere technische Überwachung der bei Dataport betriebenen Verfahren und Infrastrukturen; das SOC ergreift kontinuierliche und anlassbezogene Maßnahmen in den Handlungsebenen Prävention, Detektion und Reaktion.

Teile seiner Infrastruktur und Verfahren lässt Dataport regelmäßig auditieren und nach BSI-Standards zertifizieren. Dabei handelt es sich insbesondere um folgende Bereiche:

- Gebäudeinfrastruktur für den Rechenzentrumsbetrieb
- Managementverfahren und -prozesse bestimmter Bereiche
- Netzsegmente bestimmter Art

Diese Zertifizierungsverfahren sind ein kontinuierlicher Prozess, der auch jährliche Überprüfungen durch unabhängige Auditierung beinhaltet.

3.8.3. Mehrländer-ISM-Verbund der Trägerländer

Durch die gemeinsame Trägerschaft sowohl des IT-Dienstleisters Dataport als auch des CERT Nord befinden sich die betreffenden Länder auch hinsichtlich des Informationssicherheitsmanagements in einem Verbund. Entsprechend finden regelmäßig und anlassbezogen Abstimmungen zwischen den jeweiligen Bereichen des Informationssicherheitsmanagements der Trägerländer, von Dataport, dem SOC und dem CERT Nord statt.

3.8.4. Weitere Akteure

Zur Unterstützung der kommunalen Ebene arbeitet die Landesverwaltung unter anderem mit dem IT-Verbund Schleswig-Holstein AöR (ITV.SH) zusammen. Beispielsweise unterstützt der ITV.SH das Informationssicherheitsmanagement der Landesregierung bei der Verteilung bestimmter Warn- und Informationsmeldungen an Informationssicherheitsbeauftragte in Kommunen in Schleswig-Holstein.

Mit der Gebäudemanagement Schleswig-Holstein AöR (GMSH) findet eine Zusammenarbeit hinsichtlich der Sicherheitsmaßnahmen an und in Gebäuden statt, die von der Landesverwaltung genutzt werden.

3.8.5. Landtagswahl 2022: Beispiel für Zusammenspiel der Akteure

Die Vorbereitung, Durchführung und Auszählung der Landtagswahl 2022 wurde seitens des übergreifenden Informationssicherheitsmanagements der Landesregierung eng begleitet. Angesichts der zentralen Bedeutung einer Landtagswahl für die Demokratie wurden besondere Sicherheitsmaßnahmen ergriffen und Notfallvorsorge hinsichtlich möglicher Störungen getroffen.

Viele der Aufgaben des Informationssicherheitsmanagements bei derartigen Anlässen werden im Hintergrund wahrgenommen. Dabei zeigt sich deutlich die Wichtigkeit des Zusammenspiels der vielen Akteure in etablierten Strukturen.

3.9. Cybersicherheit bei der Polizei

Das Informationssicherheitsmanagement der Landespolizei Schleswig-Holstein wird aktuell im zuständigen Dezernat des Landespolizeiamts (LPA) wahrgenommen. Dort ist ebenfalls die IT-Sicherheitsbeauftragte der Landespolizei Schleswig-Holstein angebunden. Das Informationssicherheitsmanagement betrachtet, bewertet und steuert die Sicherheitsmaßnahmen, welche sowohl intern als auch in der polizeilichen IT-Infrastruktur bei Dataport untergebracht sind. Das Informationssicherheitsmanagement der Landespolizei ist in das übergreifende Informations- und Cybersicherheitsmanagement der Landesregierung integriert, siehe auch oben, Abschnitt 3.8.

Die zuständige Stelle im LPA ist stimmberechtigtes Mitglied in den landes- und bundesweiten Gremien und Arbeitsgruppen wie beispielsweise der Kommission IuK-Sicherheit (KomSi) oder dem AG ISM. Zudem nimmt das Informationssicherheitsmanagement beschlusskonform an den zweijährlich durchgeführten IT-Sicherheits-Revisionen (IS-Revisionen) der IT-Infrastruktur der Landespolizei Schleswig-Holstein teil.

Der größte Teil der polizeilichen IT-Infrastruktur in Schleswig-Holstein ist zentral, in einem abgeschlossenen, speziell für die Landespolizei eingerichteten Bereich in

einem Rechenzentrum von Dataport untergebracht. Die Sicherheitsstandards und Maßnahmen werden dort nach den jeweils aktuellen BSI-Standards betrachtet und umgesetzt.

Der in Konzeption befindliche Studiengang „IT-Management Polizei“ bietet für die Besetzung offener Stellen in diesem Themengebiet voraussichtlich hohes Potential.

3.10. Cybersicherheit bei der Justiz und in den Justizvollzugsanstalten

Für die Justizverwaltung bestehen die üblichen Zuständigkeiten, die sich aus der Fachaufsicht ergeben. Ein systematisches Informationssicherheitsmanagement wurde aufgebaut und wird betrieben. Der Informationssicherheitsbeauftragte Justiz (ISB Justiz) im Justizministerium leitet das Informationssicherheitsmanagement der Justiz (InSiMa Justiz). Im InSiMa Justiz werden verschiedene Aspekte der Informationssicherheit unter Beteiligung der Informationssicherheitskoordinatoren der Gerichte, der Staatsanwaltschaften und des Justizvollzugs wahrgenommen und gesteuert. Die Informationssicherheitskoordinatoren werden fachlich durch den ISB Justiz gesteuert.

Die Justizverwaltungen sind verpflichtet, Sicherheitsvorfälle an das Justizministerium zu melden, damit das Justizministerium seinerseits den eigenen Meldepflichten nachkommen kann.

Das IT-Gesetz für die Justiz des Landes Schleswig-Holstein (IT-Justizgesetz, ITJG) regelt die organisatorischen Rahmenbedingungen der zentralen Ausstattung der Gerichte und Staatsanwaltschaften des Landes Schleswig-Holstein mit der erforderlichen Informations- und Kommunikationstechnik (IT) und deren Betreuung durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde und das für Justiz zuständige Ministerium des Landes, unterstützt durch Dataport AöR und andere externe IT-Dienstleister. Die landesspezifische Umsetzung der Anforderungen aus § 2 Abs. 2 ITJG erfolgt größtenteils über die Umsetzung von Maßnahmen zur Informationssicherheit.

Spezifische landesbehördliche Initiativen und Projekte zur Förderung der Informations- und Cybersicherheit erfolgen nach eigenem Ermessen und im Personalumfang des InSiMa Justiz. Vereinzelt wurden IT-Notfallübungen für Szenarien der Informations- und Cybersicherheit vom ISB Justiz in der Rolle als IT-Notfallbeauftragter der Justiz initialisiert, durchgeführt und ausgewertet. Dabei wurden verschiedene Verbesserungen identifiziert und umgesetzt.

Die Gerichte, Staatsanwaltschaften und der Strafvollzug sind essentiell für den Erhalt der Rechtsstaatlichkeit. Dies umfasst personell insbesondere Personen im

richterlichen, staatsanwaltlichen und rechtspflegerischen Bereich (Legalitätsprinzip und sachliche Unabhängigkeit).

Zur Gewährleistung der Rechtsstaatlichkeit bestehen für die Justiz rechtlich verankerte Unabhängigkeiten in der Entscheidungsfindung sowie der Gewährleistung eines öffentlichen Glaubens in der Justiz-Fachlichkeit (beispielsweise Grundbuch, Handelsregister). Diese Vorgaben sind bei der Gestaltung der Informationssicherheit wesentlich zu berücksichtigen.

3.11. Cybersicherheit im Gesundheitswesen

Im Gesundheitswesen bestehen vielfältige fachliche Zuständigkeiten, Aufgaben und Schwerpunkte auf Bundes- und Landesebene. Hinsichtlich der Fragestellung für diesen Bericht sind insbesondere folgende Bereiche zu nennen.

3.11.1. Krankenhäuser

Die Abgrenzung auf Basis der geltenden Rechts- und Gesetzeslage richtet sich nach diversen Normen auf Bundes- und Landesebene, darunter die folgenden:

- Sozialgesetzbuch Fünftes Buch (SGB V) – Gesetzliche Krankenversicherung
- Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz, KHG)
- Krankenhausgesetz für das Land Schleswig-Holstein (Landeskrankenhausgesetz, LKHG)

Diese regeln die Zuständigkeiten der Länder im Bereich des Krankenhauswesens. Das betrifft vor allem die Krankenhausrechtsaufsicht im Rahmen der Vorschriften des LKHG, die Krankenhausplanung, die Qualitätssicherung sowie die Krankenhaus-Investitionsfinanzierung.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Entsprechende Aufsichtspflichten liegen beim BSI. Sollte aufgrund von Mängeln oder Vorkommnissen bei Einrichtungen in Schleswig-Holstein jedoch eine Zusammenarbeit erforderlich werden, wird dieser Aufgabe nachgekommen. Dazu kam es jedoch bislang nicht.

Die Krankenhausplanungsbehörde hat die Rechtsaufsicht über die Vorschriften nach dem Landeskrankenhausgesetz (LKHG). Darunter fällt unter anderem die Krankenhausalarm- und Einsatzplanung. Krankenhäuser sind verpflichtet, sich auf interne und externe Schadenslagen vorzubereiten. Die Zusammenarbeit mit dem für den Katastrophenschutz zuständigen Ministerium wird ebenfalls normiert. Gemeint sind hier jedoch Fälle, in denen es zu Großschadensereignissen und dadurch ausgelöst einer Vielzahl von Verletzten kommt, die es zu versorgen gilt.

Bei Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen gibt es verschiedene Meldewege für die Krankenhäuser. An die Krankenhausplanungsbehörde als rechtsaufsichtsführende Stelle ist über die Aktivierung der Krankenhausalarmpläne zu melden. Bei Ereignissen, die Strahlung oder Medizintechnik betreffen, ist an das Landesamt für soziale Dienste (LAsD) und deren rechtsaufsichtsführende Stelle zu melden. Wenn der Rettungsdienst eingebunden ist, muss dieser an seine rechtsaufsichtsführende Stelle melden. Da die Akteure im Gesundheitsministerium jedoch gut vernetzt sind, befinden sich die einzelnen Stellen in einem kontinuierlichen Austausch.

Die Deutsche Krankenhausgesellschaft stellt den branchenspezifischen Sicherheitsstandard (B3S) im Sinne des § 8a BSIG bereit.

Spezifische landesbehördliche Initiativen, Projekte oder Vorhaben zur Förderung der Informations- und Cybersicherheit bei den Krankenhäusern im Land bestehen derzeit nicht. Auf Grundlage von § 19 des Gesetzes für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz, KHZG) und § 14a Abs. 2 Satz 1 KHG wurde der Krankenhauszukunftsfonds zur Förderung der Digitalisierung der Krankenhäuser eingerichtet. Mit dem Fördertatbestand 10 werden in einem Sonderprogramm des Bundes, kofinanziert durch die Länder, auch dezidiert Maßnahmen der Informationssicherheit zur Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit gefördert.

In auf diesem Wege geförderten Vorhaben sind mindestens 15 Prozent der gewährten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden (§ 14a Abs. 4 KHZG). Besondere Bedeutung haben dabei organisatorische und personelle Maßnahmen.

Seit 01.01.2022 sind alle Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

Die Plankrankenhäuser im Land haben allesamt ihre Rolle in der akut-stationären Krankenversorgung. Es gibt unterschiedliche Versorgungsstufen in der Krankenhausversorgung. Besonders relevant für diese Fragestellung sind die Stufen in der Notfallversorgung (von der Basisversorgung bis hin zur umfassenden Notfallversorgung) und die Versorgung von unfallchirurgischen Patienten und Patientinnen im Rahmen des Traumanetzwerks (regionale bis Maximalversorgung).

Kontaktpersonen für KRITIS und Katastrophenschutz sind im Ministerium benannt.

3.11.2. Krankenhäuser mit Unterbringungen nach Spezialgesetzen

Krankenhäuser, in denen Unterbringungen nach dem Maßregelvollzugsgesetz (MVolllzG) oder nach dem Gesetz zur Hilfe und Unterbringung von Menschen mit Hilfebedarf infolge psychischer Störungen (PsychHG) stattfinden, unterliegen spezifischen rechtlichen Anforderungen. Diese werden nachfolgend genannt. Im Übrigen wird auf die Ausführungen im vorangehenden Abschnitt verwiesen.

Die Abgrenzung auf Basis der geltenden Rechts- und Gesetzeslage richtet sich nach diversen Normen auf Bundes- und Landesebene, darunter neben insbesondere MVollzG und PsychHG auch das Strafgesetzbuch (StGB) und die Strafprozessordnung (StPO). Dort sind Zuständigkeiten der Länder im Bereich des Unterbringungsrechts geregelt.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Sollte aufgrund von Mängeln oder Vorkommnissen eine Zusammenarbeit erforderlich werden, wird dieser Aufgabe im Rahmen der Landeszuständigkeit nachgekommen. Dazu kam es jedoch bislang nicht.

Der Beauftragte für den Maßregelvollzug gemeinsam mit weiteren Stellen im Ministerium (Abteilung Gesundheitsversorgung, Referat Psychiatrie und Maßregelvollzug) übt die Fachaufsicht über die beliehenen Einrichtungen des Maßregelvollzugs aus. Andere Stellen im Referat Psychiatrie und Maßregelvollzug üben die Fachaufsicht nach PsychHG über die sozialpsychiatrischen Dienste der Kreise und kreisfreien Städte aus.

Diverse Meldepflichten bestehen, sowohl nach MVollzG als auch nach PsychHG, und sind im Rahmen des Weisungsrechts konkretisiert. Diese beziehen sich aber bisher, da es sich um Krankenversorgung handelt, primär auf Entweichungen und besondere Vorkommnisse mit Schadenswirkung gesundheitlicher Art und weniger auf Informations- und Cybersicherheit.

Die Deutsche Krankenhausgesellschaft stellt den branchenspezifischen Sicherheitsstandard (B3S) im Sinne des § 8a BSIG bereit.

Notstromaggregate sind an beiden Forensik-Standorten in Schleswig-Holstein beschafft worden, zudem an einigen Standorten, wo PsychHG-Unterbringung erfolgt. Exakte Daten hierzu liegen nicht vor. Generell lässt sich festhalten: Die IT-Ausstattung in den Krankenhäusern des Maßregelvollzugs ist notleidend. Das Land ist bestrebt, beispielsweise die elektronische Patientenakte einzuführen – den bislang sehr mäßigem Umsetzungsgrad zu erhöhen, stellt sich als Herausforderung dar. Die digitale Sicherheitsarchitektur (beispielsweise Zaundetektion und Personennotrufsysteme) soll auf aktuellen technischen Stand gebracht werden.

Seit 01.01.2022 sind alle Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

3.11.3. Kassenärztliche Vereinigung Schleswig-Holstein (KVSH)

Aufgaben der KVSH liegen insbesondere in der Sicherstellung der vertragsärztlichen Versorgung im Land, der Abrechnung sämtlicher ambulanter Leistungen (Gesetzliche Krankenversicherung, GKV), der Zulassung von Ärztinnen und Ärzten zur Versorgung, der Qualitätssicherung, der Organisation ärztlicher Bereitschaftsdienste sowie im Betreiben der zentralen Rufnummer 116117.

Die KVSH nimmt ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Landesbehördlich besteht ausschließlich Rechtsaufsicht gemäß § 78 Abs. 1 SGB V.

Eine Meldepflicht von Datenschutzvorfällen an das Ministerium besteht gemäß § 83a SGB X und der DSGVO.

Die Verabschiedung von Leitlinien, Richtlinien und Dienstanweisungen zum Datenschutz und zur Informationssicherheit erfolgt durch den Vorstand der KVSH. Dieser orientiert sich hierfür an den BSI-Standards und der darauf basierenden IT-Grundschutzmethodik und hat dieses in einer Leitlinie geregelt. Beispielsweise finden regelmäßige Schulungen und Sensibilisierungen der Mitarbeiterinnen und Mitarbeiter im Rahmen eines Schulungskonzeptes statt, insbesondere auch neuer Mitarbeiterinnen und Mitarbeiter, zum Umgang mit E-Mail, Internet, Spam. Zudem besteht ein hausinternes Konzept zum Umgang mit Informationssicherheitsvorfällen.

3.11.4. Krebsregister

Das Krebsregister dient der Erhebung, Speicherung, Verarbeitung, Analyse, Interpretation und Veröffentlichung von Daten über Krebsneuerkrankungen in Schleswig-Holstein.

Träger des Krebsregisters SH ist das Land Schleswig-Holstein. Das Institut für Krebsepidemiologie e. V. mit Sitz in Lübeck nimmt die hoheitlichen Aufgaben der Registerstelle zur Erledigung in der Handlungsform des öffentlichen Rechts und zur Erfüllung nach Weisung durch die oberste Landesgesundheitsbehörde wahr. Die oberste Landesgesundheitsbehörde (Ministerium für Justiz und Gesundheit) führt die Fachaufsicht über die Vertrauensstelle und die Fachaufsicht über die Registerstelle.

Es bestehen keine IT-Verknüpfungen zu Bundes- oder kommunalen Einrichtungen.

Die Betreiber des Krebsregisters nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr.

Datenschutzvorfälle werden an das Land (Ministerium für Justiz und Gesundheit) und an das ULD gemeldet. In der Registerstelle des Krebsregisters liegen nur pseudonymisierte Daten vor. Ein vorhandenes Datenschutzkonzept wird stets aktualisiert.

Regelmäßige Schulungen und Sensibilisierungen der Mitarbeiterinnen und Mitarbeiter zu Themen der Informationssicherheit und des Datenschutzes finden jährlich statt unter Beteiligung interner und externer Stellen.

3.11.5. Rettungsdienst

Der Rettungsdienst umfasst die Notfallrettung, den Intensivtransport und den Krankentransport, auch im Rahmen der Bewältigung von rettungsdienstlichen Großschadensereignissen.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Das für das Rettungswesen zuständige Ministerium übt die Aufsicht darüber aus, dass die Rettungsdienstträger und der Kreis Ostholstein als Luftrettungsträger die Aufgaben nach diesem Gesetz rechtmäßig erfüllen (Rechtsaufsichtsbehörde). Die Rechtsaufsichtsbehörde kann abweichend von § 129 der Gemeindeordnung, § 68 der Kreisordnung und § 20 des Gesetzes über kommunale Zusammenarbeit in Verbindung mit § 129 der Gemeindeordnung Maßnahmen im Sinne der §§ 123 und 124 der Gemeindeordnung und der §§ 62 und 63 der Kreisordnung im Einvernehmen mit dem für Inneres zuständigen Ministerium treffen. Die Anordnung von Zwangsmaßnahmen nach §§ 125 und 127 der Gemeindeordnung und den §§ 64 und 66 der Kreisordnung bleibt dem für Inneres zuständigen Ministerium vorbehalten.

Das Referat Rettungswesen des Ministeriums ist bei Bedarf im Rahmen des Krisenmanagements der Landesregierung in den Landesführungsstab im Sinne eines Allgefahrenansatzes mit einbezogen.

3.11.6. Heilberufekammern, Aufsicht Gesundheitsberufe und Schulische Bildung, Ausbildungsfonds der Pflegeberufe

Die Heilberufekammern regeln alle ihre organisatorischen Belange im Rahmen der Selbstverwaltung. Das beinhaltet auch die Informations- und Cybersicherheit. Das Ministerium hat lediglich die Rechtsaufsicht.

Hinsichtlich der Aufsicht über die Gesundheitsberufe einschließlich der betreffenden Schulischen Bildung werden partielle Fach- und Rechtsaufsichten wahrgenommen über bestimmte Organisationeinheiten des LAsD und des Schleswig-Holsteinischen

Instituts für Berufliche Bildung (SHIBB). Belange der Informations- und Cybersicherheit sind nicht Teil dieser Aufsichtsfunktion.

Der Ausbildungsfonds der Pflegeberufe SH GmbH (Aufsichtsfonds) ist eine vom Land beliehene GmbH zur fortlaufenden Abwicklung des Umlageverfahrens zur Finanzierung der Pflegeausbildungen nach dem Pflegeberufegesetz. Der Beleihungsakt gibt dem Ausbildungsfonds hierbei die Auflage, dass der Ausbildungsfonds die zu Erfüllung seiner Aufgaben erforderlichen Verwaltungsstrukturen sicherzustellen hat. Über diese Belange sind die zuständige Stelle im Gesundheitsministerium (Referat Berufe des Gesundheitswesens) und der Ausbildungsfonds regelmäßig im Austausch. Bezüglich Informations- und Cybersicherheit hat der Ausbildungsfonds umfassende Schutzmaßnahmen ergriffen. Diese werden teilweise von extern Dienstleistern geprüft und regelmäßig beispielsweise Penetrationstests unterzogen.

Rechtlich normierte Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen gegenüber dem Ministerium bestehen nicht. Gleichwohl kann davon ausgegangen werden, dass die aufsichtsführenden Stellen bei schwerwiegenden Vorfällen – insbesondere Cyber-Attacken mit Schadensfolge – von den beaufsichtigten Institutionen informiert werden würden.

3.12. Cybersicherheit in den Bildungseinrichtungen

3.12.1. Schulen

Das Land Schleswig-Holstein hat die Zuständigkeit für allgemeine und berufliche Bildung im Land. Für die sachliche Ausstattung der Schulen sind die Schulträger – überwiegend Kommunen –, aber in Teilen auch das Land zuständig.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Das Schleswig-Holsteinische Schulgesetz (Schulgesetz, SchulG) ist eine zentrale landesrechtliche Norm für den Bereich der Schulen. Gemäß § 125 SchulG hat das Bildungsministerium die Fach- und Dienstaufsicht über die Schulen und die Rechtsaufsicht über die Schulträger. Eine spezifische aufsichtsbehördliche Funktion hinsichtlich der Informations- und Cybersicherheit, beispielsweise die Überprüfung der Umsetzung von Sicherheitsanforderungen, ist nicht durch Gesetz geregelter Bestandteil der Schulaufsicht.

Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen bestehen einerseits datenschutzrechtlich. Hier sind insbesondere Meldepflichten an die Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO sowie

Meldungen gemäß § 4 Zentrale-Stelle-Verordnung Schule[7] zu nennen. Andererseits bestehen ergänzende Regelungen in den allgemeinen Nutzungshinweisen für die Endgeräte, die das Land den Lehrkräften zur Verfügung stellt – das betrifft beispielsweise Meldungen von Schadsoftwareverdachtsfällen oder Verlust des Endgeräts.

Die Landesverwaltung stellt den Schulen Hilfsmittel zur Verfügung, um die Verantwortlichen beim ordnungsgemäßen Einsatz der Informationstechnik zu unterstützen. Zu diesen Hilfsmitteln gehört beispielsweise ein Muster für ein Basis-IT-Sicherheitskonzept. In den Unterlagen und Fortbildungen zu den landesweiten Diensten wird u. a. für das Thema Datenschutz und Datensicherheit sensibilisiert sowie mit dem IQSH Helpdesk eine landesweit zentrale Anlaufstelle bereitgestellt.

Hinsichtlich der Notfallvorsorge lässt sich festhalten: Grundsätzlich ist die Aufrechterhaltung eines Schulbetriebs ohne digitale Dienste, Strom oder fließendes Wasser denkbar. Derzeit kann jedoch nicht zuverlässig abgeschätzt werden, in welchem Umfang der Schulbetrieb in entsprechenden Notfall- und Krisensituationen auch aufgrund der Arbeits- und Aufgabenverdichtung ohne die elektronische Datenverarbeitung und zentralen Verfahren wie beispielsweise School-SH (einheitliche Schulverwaltungssoftware) reibungslos funktionieren würde.

3.12.2. Hochschulen

Die Hochschulen nehmen ihre Aufgaben der Informations- und Cybersicherheit im Sinne der Hochschulautonomie eigenverantwortlich wahr. Das gilt auch für generelle landesbehördliche Anforderungen zur Informations- und Cybersicherheit an die Hochschulen. Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen an die Landesbehörde bestehen nicht auf gesetzlicher Ebene, entsprechende Meldungen betroffener Hochschulen sind allerdings übliche Praxis.

Im Jahr 2023 wurden den Hochschulen aus dem ZSL-Entwicklungsbudget Sondermittel in Höhe von 3.406.557 € für die Verbesserung der IT-Sicherheit zur Verfügung gestellt. Dafür haben die Hochschulen in Zusammenarbeit mit dem Fachverbund "ITSH-edu" der Hochschulen ein gemeinsames Konzept für Maßnahmen der IT-Sicherheit eingereicht. Dieses Konzept sieht insgesamt sieben Einzelprojekte vor, die allesamt das Ziel haben, vor dem Hintergrund der aktuellen Cyber-Angriffe auf Hochschulinfrastruktur die IT-Sicherheit an den Hochschulen

[7] Landesverordnung über die zentralen Stellen nach dem Landesdatenschutzgesetz für die vom für Bildung zuständigen Ministerium und vom Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein betriebenen automatisierten Verfahren (Zentrale-Stelle-Verordnung Schule - ZStVOSchule) vom 30. Juni 2022, verfügbar unter <https://www.gesetze-rechtsprechung.sh.juris.de/perma?j=ZtrStSchulV_SH>.

nachhaltig zu verbessern. Die Zunahme der digitalen Verwaltung und Lehre wird das Angriffspotential an den Hochschulen (verbunden mit hohen Instandsetzungskosten, einem enormen Verwaltungsaufwand und einem großen Reputations- und Vertrauensverlust) in den nächsten Jahren noch weiter erhöhen. Dies erhöht den Druck der Hochschulen, darauf mit geeigneter technischer Infrastruktur, organisatorischen Maßnahmen und geschultem Personal reagieren zu können. Die vorgestellten Maßnahmen zielen sowohl auf die Prävention von Cyber-Angriffen als auch auf eine verbesserte Handlungsfähigkeit in einem möglichen Krisenszenario. Geplant sind dabei neben Investitionen in die technische IT-Sicherheitsinfrastruktur (DNS-Sicherheit, Multifaktor-Authentifizierung, Netzwerk-Anomalieerkennung, Incident-Management) auch Maßnahmen zur Mitarbeiterschulung und Investitionen zur Verbesserung der IT-Resilienz für den Fall eines erfolgreichen Angriffes (Soforthilfe durch externe Dienstleister).

Das Konzept sieht die Kooperation unter den Hochschulen im Bereich der IT-Sicherheit vor. Alle Maßnahmen werden an allen Hochschulen durchgeführt, jedoch müssen einige Vorhaben aufgrund der Heterogenität der IT-Infrastruktur an den Standorten hochschulspezifisch geplant und umgesetzt werden. Dort, wo es möglich und sinnvoll ist, wurde ein gemeinsames Vorgehen über eine gemeinsame Beschaffung und Zusammenarbeit geplant.

Eine Verstetigung dieser Zahlungen an die Hochschulen ist angezeigt, jedoch vor dem Hintergrund der aktuellen Haushaltslage noch nicht gesichert.

Notfallübungen sind aufgrund der Personalausstattung in den Rechenzentren (Fachkräftemangel betrifft auch Hochschulen; diese stehen auf dem IT-Arbeitsmarkt in einem sehr ungünstigen Wettbewerbsverhältnis zu anderen Arbeitgebern) bisher nur in einem sehr geringen und unzureichenden Umfang möglich. Die Landesverwaltung ist daran nicht beteiligt.

IT-Kontaktpersonen der staatlichen und privaten Hochschulen sind der Landesbehörde bekannt. Auch umgekehrt liegen den Hochschulen Informationen vor, wer im Falle eines Angriffs oder eines anderen sicherheitsrelevanten Vorfalls zu kontaktieren ist.

Aus der jüngeren Vergangenheit lassen sich an dieser Stelle folgende sicherheitsrelevante Vorfälle in Hochschulen nennen:

- Am 25.12.2022 kam es an der FH Westküste zu einem Hackerangriff. Betroffen waren hier vor allem Server mit Datenbanken. Dort wurden alle Dateien (inklusive Backup) verschlüsselt. Zu einem Diebstahl personenbezogener (und auch anderer Daten) kam es nicht.

- Am 29.12.2022 ist an einem einzelnen Institut der Universität zu Lübeck ein Fall von Datenverschlüsselung aufgetreten. In diesem Institut sind der Mail-Server, Teile des Fileservers sowie das Backup verschlüsselt worden.
- Im April 2023 wurde das Leibniz-Informationszentrums Wirtschaft in Kiel (ZBW) von der prorussischen Hackergruppe „Royal“ angegriffen. Wenngleich die ZBW keine Einrichtung des Landes bzw. der Hochschulen des Landes ist, wird dieser Vorfall angesichts der engen Zusammenarbeit im Wissenschafts-Cluster Kiel hier mit aufgeführt. Bei dieser Ransomware-Attacke wurde sich ein Zugriff auf die IT-Infrastruktur verschafft und einige Bereiche der ZBW-Webseite verschlüsselt. Eine Festplatte wurde komplett formatiert.

In allen genannten Fällen haben die Einrichtungen unverzüglich das ULD, das LKA und das MBWFK über die Vorfälle informiert.

3.12.3. Bildungszentrum der Steuerverwaltung des Landes Schleswig-Holstein

Im Geschäftsbereich des Finanzministeriums wurde das Bildungszentrum der Steuerverwaltung des Landes Schleswig-Holstein (BiZ) eingerichtet. Auf Bundesebene gibt es die Bundesfinanzakademie. Aufgrund des föderalen Systems hat jedes Bundesland eigene Bildungseinrichtungen für die Ausbildung der Nachwuchskräfte der Steuerverwaltung. Das BiZ stellt dieses Aus- und Fortbildungszentrum für Schleswig-Holstein dar.

Das Informationssicherheitsmanagement für das Finanzressort nimmt Aufgaben auch für das BiZ wahr. Beispielsweise werden Sicherheitsvorfälle oder andere sicherheitsrelevante Ereignisse an den Ressort-ISB im Finanzministerium SH – Amt für Informationstechnik (AIT) gemeldet. Der Ressort-ISB ist die Kontaktstelle zum CISO und meldet alle sicherheitsrelevante Vorfälle und Ereignisse. Sensibilisierungsmaßnahmen wie etwa Hinweise auf Vorsicht bei Mailanhängen gibt das Informationssicherheitsmanagement im AIT auch an die Belegschaft im BiZ weiter. Die Steueranwärterinnen und Steueranwärter werden für Maßnahmen der Informationssicherheit wie einen sorgsamen Umgang mit dem Internet sensibilisiert.

Bei Notfallübungen durch die Steuerverwaltung ist das BiZ integraler Bestandteil. Das AIT koordiniert und steuert diese.

Im Finanzministerium wurde ein Katastrophenschutzbeauftragter benannt.

3.13. Cybersicherheit im Verkehrswesen – ÖPNV, SPNV/Fernzugverkehr

Das Land Schleswig-Holstein ist Aufgabenträger für den Schienenpersonennahverkehr (SPNV). Die Kreise und kreisfreien Städte sind die

Aufgabenträger für den übrigen öffentlichen Personennahverkehr (ÖPNV). Für Fernverkehr liegt die Zuständigkeit nicht beim Land oder den Kommunen.

Die NAH.SH GmbH organisiert im Auftrag des Landes die Angelegenheiten des SPNV. Das Land ist Gesellschafter der NAH.SH GmbH und hat die Wahrnehmung der Aufgaben der SPNV-Aufgabenträgerschaft per Vertrag auf die NAH.SH übertragen. Allgemeine Meldepflichten der NAH.SH GmbH ergeben sich vor allem aus dem Aufgabenübertragungsvertrag mit dem MWVATT. Die Aufsicht über die NAH.SH GmbH inklusive der Aspekte der Informations- und Cybersicherheit erfolgt über den Aufsichtsrat der GmbH.

Das MWVATT übt die Fachaufsicht über die Kreise und kreisfreien Städte im Bereich ÖPNV und Personenbeförderung aus, die allerdings keine Aspekte der Informations- und Cybersicherheit beinhaltet.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr.

Im MWVATT sind Kontaktpersonen für KRITIS und Katastrophenschutz benannt.

3.14. Cybersicherheit im Verkehrswesen – Individualverkehr

Mit der Gründung der Autobahn GmbH des Bundes (AdB) zum 01.01.2021 ging die Zuständigkeit für die kritische Infrastruktur vom Landesbetrieb Straßenbau und Verkehr Schleswig-Holstein (LBV.SH) auf die AdB über. Die Betriebsdienstzentrale des Landes in Neumünster, welche derzeit auch die Schnittstelle zwischen den Zuständigkeiten Bund zu Land darstellt, ist im Jahr 2023 gemäß den Vorgaben der AdB hinsichtlich der IT-Sicherheit optimiert worden. Im Rahmen der laufenden Kooperationsvereinbarung übernimmt der LBV.SH als Dienstleister für die AdB die betriebliche Überwachung der Anlagen der kritischen Infrastruktur des Bundes.

Zu den Aufgaben des Landes mit Bezug zum Individualverkehr gehören das Straßenverkehrsrecht (Verhaltensrecht im Straßenverkehr, Fahrerlaubnisrecht, Gefahrgutrecht, Güterkraftverkehrsrecht, Fahrzeugtechnik und Zulassungsrecht). Weite Teile der Aufgaben des Straßenverkehrsrechts wurden an die Kreise, kreisfreien Städte und Kommunen übertragen. Da es sich um Pflichtaufgaben handelt, übt das Land (in der Regel LBV.SH, teilweise MWVATT) über die Kreise und kreisfreien Städte die Rechts- und Fachaufsicht aus. Einige Aufgaben des Straßenverkehrsrechts werden durch das Land selbst wahrgenommen. Aufgaben des Straßenverkehrsrechts beruhen auf Bundesrecht.

Ferner nehmen das Land, die Kreise und kreisfreien Städte auf dem Gebiet des Individualverkehrs (Vorsorge-)Aufgaben der Zivilverteidigung wahr. Aufgaben der Zivilverteidigung beruhen ebenfalls auf Bundesrecht.

Eine spezifische landesbehördliche Zuständigkeit für Aspekte der Informations- und Cybersicherheit der betreffenden Einrichtungen im Land besteht nicht. Spezialgesetzliche Regelungen hinsichtlich Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen an die Landesbehörde bestehen nicht.

3.15. Cybersicherheit im Verkehrswesen – Häfen/Schiffsverkehr

Das MWVATT ist als oberste Hafenbehörde zuständig für die Ordnungsverwaltung in den schleswig-holsteinischen Häfen. In diesem Zusammenhang müssen unter anderem bundesrechtliche Vorgaben, EU-Vorgaben oder Vorgaben der Internationalen Seeschifffahrts-Organisation (*International Maritime Organization*, IMO) rechtlich umgesetzt werden. Die Landesverordnung für die Häfen in Schleswig-Holstein (Hafenverordnung, HafVO) enthält spezifische Regelungen. Aufgabe der nach § 4 HafVO SH örtlich zuständigen Hafenbehörden ist es, den sicheren Umschlag von Waren und den sicheren Passagierverkehr sowie die Einhaltung von Umweltvorschriften und anderen sicherheitsrelevanten Vorschriften zu überwachen. Untere Hafenbehörden sind das Land selbst (Landesbetrieb für Küstenschutz, Nationalpark und Meeresschutz Schleswig-Holstein, LKN), die Kreise, die Ämter und amtsfreien Gemeinden (§ 4 HafVO SH). Der Bund hat für landseitige Hafenangelegenheiten keine Zuständigkeiten; für seeseitige nur dann, wenn Häfen unmittelbar an Bundeswasserstraßen liegen.

Der Schiffsverkehr wird durch die Ordnungsverwaltung des Bundes (Wasser und Schifffahrtsverwaltung) durch eigene Behörden überwacht. Hier regelt der Bund sowohl die Verkehrsvorschriften als auch die technische Schiffssicherheit und Besatzungsfragen. Die Regelung und Verwaltungskompetenz des Landes erstreckt sich nur auf die Gewässer, die keine schiffbaren Bundeswasserstraßen sind.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Die oberste Hafenbehörde hat die Fach- und Rechtsaufsicht über die unteren Hafenbehörden (Kreise). Bisher hat sich die oberste Hafenbehörde nicht mit der Überwachung der Informations- und Cybersicherheit bei den unteren Hafenbehörden befasst. Da sich die Fachaufsicht auf die Rechts- und Zweckmäßigkeit bezieht, wäre eine derartige Überwachung grundsätzlich denkbar. Allerdings wäre es aus Sicht der Fachlichkeit nicht sinnvoll, wenn eine Fachaufsichtsbehörde sich mit der generellen Informations- und Cybersicherheit der Organisationseinheit Kreis befasste.

Im MWVATT sind Kontaktpersonen für KRITIS und Katastrophenschutz benannt.

3.16. Cybersicherheit im Verkehrswesen – Luftverkehr

Die Luftsicherheitsbehörde hat die Aufgabe, Angriffe auf die Sicherheit des Luftverkehrs abzuwehren. Auf Landesebene wird diese Aufgabe durch den LBV.SH als Luftsicherheitsbehörde des Landes im Auftrag des Bundes ausgeführt (Bundesauftragsverwaltung), allerdings mit Ausnahmen. Das Luftfahrtbundesamt ist etwa unmittelbar für die Überwachung der Sicherheitsmaßnahmen der Luftfahrtunternehmen zuständig (§ 9 Luftsicherheitsgesetz, LuftSiG). Oberste Luftsicherheitsbehörde des Bundes ist das Bundesministerium des Innern und für Heimat (BMI). Die Fachaufsicht über den LBV.SH liegt beim MWVATT.

Die zuständige Luftsicherheitsbehörde überwacht die nach §§ 5 und 8 LuftSiG regulierten Unternehmen. In Inspektionen wird auch unter Mitwirkung des BSI u. a. die Einhaltung der Vorgaben der DVO 2019/1583 – Durchführungsverordnung zur Änderung der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen – und des Nationalen Luftsicherheitsprogramms (NLSP) überprüft.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Etwaige spezifische Vorgaben werden über das BMI geregelt (Auftragsverwaltung). Diese sind als Verschlusssache eingestuft.

Im MWVATT sind Kontaktpersonen für KRITIS und Katastrophenschutz benannt.

3.17. Cybersicherheit in der Telekommunikation

Im MWVATT besteht eine Zuständigkeit im Bereich der Telekommunikation. Diese Zuständigkeit bezieht sich primär auf Regulierungsfragen und wirtschaftspolitische Angelegenheiten.

Die betreffenden Einrichtungen im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Eine Zuständigkeit für diese Aspekte im Bereich der Telekommunikation ist im Telekommunikationsgesetz (TKG) geregelt und liegt gemäß § 168 TKG bei BSI und BNetzA. Das betrifft auch Meldepflichten zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen – entsprechende Meldepflichten an die Landesbehörde bestehen nicht. Weitere spezifische rechtliche Anforderungen für Maßnahmen der Informations- und Cybersicherheit ergeben sich inssbesondere aus TKG Teil 10, Öffentliche Sicherheit und Notfallvorsorge.

Eine aufsichtsbehördliche Funktion gegenüber Einrichtungen im Bereich der Telekommunikation im Land liegt bei der BNetzA. Das MWVATT nimmt seine Aufgaben im hier beschriebenen Rahmen wahr.

Im MWVATT sind Kontaktpersonen für KRITIS und Katastrophenschutz benannt. Im Sektor Telekommunikation sind damit auch Funktionen verbunden zur Ermittlung und Darstellung der Lage Telekommunikation, gegebenenfalls der Herstellung einer Verbindung zur BNetzA, zur Deutschen Telekom AG sowie zu Anbietern von Telekommunikationsdienstleistungen. Die BNetzA berichtet seit Beginn des derzeitigen Ukraine-Krieges regelmäßig dem Bundesministerium für Digitales und Verkehr (BMDV) zur Sicherheit der Telekommunikationsnetze und -dienste. Die Berichte werden den Ländern zur Verfügung gestellt.

3.18. Cybersicherheit in der Lebensmittelversorgung

Im MWVATT besteht eine Zuständigkeit im Bereich der Ernährungsnotfallvorsorge nach dem Ernährungssicherstellungs- und -vorsorgegesetz (ESVG). Die im Gesetz enthaltenen Verordnungsermächtigungen erlauben es dem zuständigen Bundesministerium, Vorschriften für die Sicherstellung der Grundversorgung sowie die Vorsorge für eine Versorgungskrise zu erlassen, §§ 4, 11 ESVG. Ferner kann der Bund eine Bundesanstalt für zentral zu erledigende Aufgaben sowie Aufgaben des Bundes gründen, soweit keine anderweitige Zuständigkeit gesetzlich festlegt ist, Art. 87 III GG i. V. m. § 3 III ESVG.

Dieses Gesetz sowie Rechtsverordnungen, die aufgrund dieses Gesetzes erlassen werden, werden von den Ländern grundsätzlich als eigene Angelegenheit ausgeführt, wenn die Regelungen nicht Zwecken der Verteidigung dienen und deshalb im Auftrag des Bundes durchgeführt werden, Art. 83, 87b II GG i. V. m. § 3 I ESVG. Das Land bestimmt die zuständigen Behörden, Art. 84 GG i. V. m. § 3 II ESVG. Bis zum Erlass einer Rechtsverordnung nach § 4 I ESVG können die zuständigen Behörden die notwendigen Maßnahmen treffen, die zur einstweiligen Sicherstellung der Grundversorgung unmittelbar geboten sind.

Überdies bestehen weitreichende Vorschriften über die Auskunftspflicht von Ernährungsunternehmen mit entsprechenden Überwachungsbefugnissen und über die Datenübermittlung zwischen den Behörden, vgl. §§ 9, 13, 15 ESVG.

Die betreffenden Einrichtungen der Lebensmittelversorgung im Land nehmen ihre Aufgaben der Informations- und Cybersicherheit eigenverantwortlich wahr. Zwar bestehen Vorschriften über die Auskunftspflicht von Ernährungsunternehmen mit entsprechenden Überwachungsbefugnissen, § 15 ESVG. Zudem ermöglicht § 6 I Nr. 2 ESVG eine hoheitliche Aufsicht unter Maßgabe der dort benannten Voraussetzungen. Eine aufsichtsbehördliche Funktion besteht für Aspekte der

Informations- und Cybersicherheit jedoch nicht. Eine initiative Übermittlung von Meldungen zu Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen an die Landesbehörde ist im ESVG derzeit nicht vorgesehen.

In § 2 Abs. 10 BSIG ist definiert, dass es im Bereich der Ernährung Kritische Infrastrukturen gibt. Diese sind Einrichtungen, Anlagen oder Teile davon, die dem Sektor Ernährung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Für diese gelten hinsichtlich der Informations- und Cybersicherheit dann u. a. die Vorgaben des BSIG.

Auf das BSIG aufbauend stellt § 4 BSI-KritisV konkret fest, dass im Sektor Ernährung das hier in Rede stehende Geschäftsfeld – die Lebensmittelversorgung – unter Maßgabe der dort referenzierten Kategorien und Schwellenwerte eine kritische Dienstleistung ist.

Im MWVATT sind Kontaktpersonen benannt und üben die folgenden Funktionen aus:

- Beauftragte für den Katastrophenschutz
- Ansprechstelle Kritische Infrastrukturen

3.19. Bisherige Aktivitäten des "Servicepoint Cybersecurity"

Im Sommer 2019 vereinbarten das Land Schleswig-Holstein, die IHK Schleswig-Holstein, der ASWN e.V. sowie DiWiSH die SicherheitsPartnerschaft SH. Unter diesem Dach wurde auf Initiative des MWVATT noch im selben Jahr der Servicepoint Cybersecurity gestartet. Dieser dient Unternehmen in Schleswig-Holstein als zentrale, unabhängige Anlaufstelle bei Anfragen zu präventiven Maßnahmen der Informations- und Cybersicherheit sowie bei akuten Angriffen.

Der Servicepoint Cybersecurity nimmt nach Kontaktierung bei akuten Vorfällen das betreffende Szenario mithilfe eines standardisierten Fragebogens zunächst systematisch auf. Darauf aufbauend übernimmt der Servicepoint Cybersecurity eine unabhängige "Scharnierfunktion", indem er die akute Aufgabenstellung ohne Nennung des Anfragers an die teilnehmenden IT-Security-Unternehmen leitet, die daraufhin Angebote zur Unterstützung unterbreiten können. Diese Angebote übermittelt der Servicepoint Cybersecurity wiederum dem Anfrager. Die operative Umsetzung dieser Aktivitäten liegt im Lead der (ehrenamtlichen) DiWiSH-Fachgruppenleitung IT-Security.

Darüber hinaus bieten der Servicepoint Cybersecurity bzw. die SicherheitsPartnerschaft SH Informations- und Sensibilisierungsveranstaltungen an

bzw. beteiligen sich an solchen. In diesem Zusammenhang wurden u. a. folgende Veranstaltungen im Bereich Cybersicherheit durchgeführt:

- "Cybersecurity in der Praxis" am 13.02.2020 mit 41 Teilnehmenden in Kiel
- "Angriffswege und Kriminalistik", geplant am 21.04.2020 (abgesagt)
- "Wir sind auf ZAC" am 08.09.2020 mit 120 Teilnehmenden online
- "Resilienz für Unternehmen – den Notfall vorausplanen!" am 02.11.2020 mit 32 Teilnehmenden online
- "Sicherheitslücke 'Log4j' – Gefahr für mein Unternehmen" am 08.02.2022 mit 100 Teilnehmenden online
- "Fischbowl I" am 05.05.2022 mit 70 Teilnehmenden online
- "Fischbowl II" am 27.09.2022 mit 56 Teilnehmenden online
- "Forum Wirtschaftsschutz" am 30.08.2023 mit 130 Teilnehmenden in Kiel

Der Servicepoint Cybersecurity wurde bisher nicht stark nachgefragt. In dem Zeitraum Ende 2019 bis 2021 wurde der Servicepoint weniger als fünf Mal angefragt, ebenso in den Jahren 2022 bis 2023.

Diese Nachfrage blieb deutlich hinter den Erwartungen zurück. Hauptgründe dafür sieht die Landesregierung in folgenden Bereichen:

- Bekanntheit des Angebots mit seinen Möglichkeiten (und Grenzen) ist bei der Zielgruppe begrenzt
- Abgrenzung des Angebots zu anderen Angeboten des Landes wie der Zentralen Ansprechstelle Cybercrime oder Angeboten anderer Akteure wie dem BSI ist nicht hinreichend deutlich
- Angebot basiert auf ehrenamtlicher Tätigkeit insbesondere der betreffenden Fachgruppenleitung im DiWiSH, die primär mit anderen Aufgaben betraut ist
- Verhältnis präventiver und reaktiver Bestandteile des Angebots samt der Frage einer möglichen Fokussierung wurden nicht konsequent geklärt
- Befürchtungen innerhalb der Zielgruppe hinsichtlich der Wahrung der Vertraulichkeit; Bedenken, dass bei Inanspruchnahme der Unterstützung durch regionale Akteure dem Betroffenen die Kontrolle über die Kommunikation seiner Betroffenheit entgleiten könnte

Aufgrund der bisherigen mangelnden Nachfrage arbeitet das MWVATT seit einiger Zeit an einer Neuausrichtung des Servicepoint Cybersecurity (zunächst als

präventives „Informationsportal“ für Unternehmen im Bereich Cybersicherheit). Dies bedarf entsprechender Ressourcen. Mögliche Optionen werden derzeit geprüft. Eine Umsetzung soll möglichst kurzfristig erfolgen als integrierter Bestandteil der Cybersicherheitsarchitektur SH, siehe unten, Kapitel 4.2, Vorhaben der Landesregierung.

3.20. Aktivitäten der Landesregierung im Bereich der Bedrohung durch Desinformation

Die Landesregierung sieht wachsende Risiken durch Desinformation. Bei Desinformation handelt es sich um das gezielte Verbreiten von Falschinformationen mit dem Ziel, die Gesellschaft, einzelne Gruppen oder Einzelpersonen im Sinne politischer oder wirtschaftlicher Interessen zu täuschen. Desinformation ist kein neues Phänomen – auch in der analogen Welt gab es immer wieder beispielsweise Versuche der politischen Einflussnahme durch Falschbehauptungen. In der heutigen digitalen Welt gibt es aber neue Formen und Verstärkungen von Desinformation, deren Auswirkungen erheblich stärker sein können als in der Vergangenheit:

- Die Reichweite des Internet ist weltumspannend, während beispielsweise gedruckte Zeitungen oder Flugblätter oft auf lokale oder regionale Verfügbarkeit beschränkt sind.
- Die schier unermessliche Informationsmenge im Internet, insbesondere auch auf den großen Plattformen der sogenannten Sozialen Medien, erzeugt Rahmenbedingungen und Dynamiken, die eine Verbreitung von Desinformation begünstigen können ("*information overflow*").
- Neue und sich rasant weiterentwickelnde technische Möglichkeiten bergen neben enormen Chancen auch neue Missbrauchsmöglichkeiten – beispielsweise durch den Einsatz von Methoden der Künstlichen Intelligenz zur gezielten Fälschung von Bild-, Video- und Audiomaterialien bei sogenannten "*Deep Fakes*".
- Durch Identitätsdiebstahl in der digitalen Welt bestehen neue Möglichkeiten, beispielsweise Falschbehauptungen im Namen bzw. unter der Identität einer anderen Person zu verbreiten.
- Staatliche und nichtstaatliche Akteure können die heutigen technischen Möglichkeiten auf systematische Weise zu Zwecken der Desinformation nutzen, teils in gezielten Kampagnen.

Durch Desinformation bestehen Risiken nicht nur für einzelne Personen oder Einrichtungen, sondern auch für die Stabilität der freiheitlichen demokratischen Grundordnung. Denn Desinformation zielt teilweise darauf ab, Vertrauen in staatliche

Einrichtungen und Mechanismen zu untergraben, den Ausgang demokratischer Wahlen zu beeinflussen oder antidemokratische Weltbilder zu stärken und zu verbreiten.

Die Landesregierung sieht Bedrohung durch Desinformation als ein Querschnittsthema an. Es handelt sich nicht primär um ein Cybersicherheitsthema, aber es beinhaltet Aspekte der Informations- und Cybersicherheit – beispielsweise bei Verbreitung von Falschinformationen über ein "gehacktes" Medienprofil eines Mandatsträgers oder einer Mandatsträgerin in deren Namen oder bei technischen Entwicklungen, aufgrund derer die Integrität von Informationen beeinträchtigt werden kann.

Maßnahmen gegen die Bedrohung durch Desinformation werden in Schleswig-Holstein primär durch die zuständigen Stellen in den Sicherheitsbehörden im Rahmen ihres jeweiligen Auftrags umgesetzt, insbesondere Verfassungsschutz sowie Landeskriminalamt und andere polizeiliche Dienststellen.

Hierzu gehört seitens des Verfassungsschutzes[8] wesentlich die Sammlung und Auswertung sach- und personenbezogener Informationen über:

- Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern der Verfassungsorgane des Bundes oder eines Landes zum Ziele haben,
- sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht,
- Bestrebungen im Geltungsbereich des Grundgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, und
- Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind.

Im Rahmen der Strafermittlung und -verfolgung und des Staatsschutzes nehmen die polizeilichen Dienststellen ihre jeweiligen Aufgaben wahr und setzen entsprechende Maßnahmen um.

Aus sicherheitspolitischer Sichtweise sind Desinformationskampagnen den hybriden Bedrohungen zuzuordnen, wenn sie direkt oder indirekt durch staatliche oder

[8] Für nähere Ausführungen und weitere Informationen vgl. Verfassungsschutzbericht 2022, Landtags-Drs. 20/1021.

nichtstaatliche Akteure gesteuert werden. Derartige Aktivitäten haben ihrer Natur nach einen ausgeprägt Landes- und Staatsgrenzen überschreitenden Charakter. Entsprechend besteht hoher Bedarf für Vernetzung zwischen Bund und Ländern. Diese Vernetzung findet teils in spezifischen Arbeitsgruppen und -formaten statt, teils in bestehenden Gremienstrukturen, in denen Schleswig-Holstein vertreten ist. Beispielhaft seien hier Gremien der Innenressorts wie die LAG Cybersicherheit der Innenministerkonferenz genannt.

Die Landesregierung unterstützt Forschung an Hochschulen des Landes, deren Ergebnisse gerade bei neuen technischen Entwicklungen helfen, gezielte Maßnahmen gegen Desinformation umzusetzen. Das betrifft beispielsweise Forschung zur Erkennung von "*Deep Fakes*" mit Methoden der Künstlichen Intelligenz.

Gerade hinsichtlich der Erkennung von Desinformation auch durch Bürgerinnen und Bürger ist Aufklärung und Medienkompetenz erforderlich. Die Landesregierung unterstützt entsprechende Maßnahmen und Projekte. Beispielsweise hat Digitalisierungsminister und Chef der Staatskanzlei Dirk Schrödter jüngst im Rahmen des Digitalisierungpreises "Best of Digitales.SH" 2023 das Projekt "Deepfake Detective" ausgezeichnet. Mit Hilfe einer *Virtual-Reality*-Anwendung von holoNative aus Kiel wird die Wahrnehmung für manipuliertes Bildmaterial anhand von unterschiedlichem Videomaterial geschult. Die Jury lobte das Projekt besonders für die gelungene Umsetzung eines digitalen Bildungsangebotes, bei dem Schülerinnen und Schüler für die Wichtigkeit des Themas sensibilisiert werden.

Die Landesregierung beabsichtigt, ihre Aktivitäten hinsichtlich der Bedrohung durch Desinformation weiter zu verstärken. Zur Steuerung und Wahrnehmung der betreffenden Aufgaben in der Landesverwaltung sind entsprechende Ressourcen erforderlich.

3.21. Darstellung der gesamtstaatlichen Cybersicherheitsarchitektur in den Bereichen Prävention, Detektion und Reaktion, insbesondere mit Blick auf die kritische Infrastruktur

3.21.1. Überblick

Gefährdungen der Informations- und Cybersicherheit machen nicht an Landesgrenzen halt. Deshalb findet bereits heute eine vielfältige Zusammenarbeit diverser Akteure in Bund und Ländern statt. In allen diesen Kontexten werden Aspekte der Handlungsebenen Prävention, Detektion und Reaktion behandelt, wenngleich in unterschiedlicher Weise und in unterschiedlichen Anteilen.

Nachfolgend werden die derzeit wichtigsten dieser Architekturelemente im Sinne der Fragestellung dargestellt. Der Übersicht halber wird eine Auswahl vorgenommen.

3.21.2. Länder- und Bund-Länder-Gremien

Mehrere dauerhafte Gremienstrukturen im Themenbereich haben sich etabliert. Im Kontext der Fragestellung sind das primär die AG Informationssicherheit des IT-Planungsrates sowie die LAG Cybersicherheit der Innenministerkonferenz.

3.21.2.1. AG Informationssicherheit

Die AG Informationssicherheit (AG InfoSic) ist eine dauerhafte Arbeitsgruppe des IT-Planungsrates. Dieser basiert auf Art. 91c GG sowie dem darauf gründenden IT-Staatsvertrag. Die AG InfoSic arbeitet primär an strategischen Themen und entsprechender Stärkung der Informations- und Cybersicherheit im Bund-Länder-Kontext.

Die AG InfoSic setzt sich primär aus den Landes-CISOs (bzw. im Einzelfall anderen Vertreterinnen oder Vertretern aus dem betreffenden CISO-Funktionsbereich) zusammen. Beratend können auch Vertreterinnen und Vertreter des BSI, der Föderalen IT-Kooperation (FITKO), der kommunalen Spitzenverbände sowie einiger weiterer Akteure an den Sitzungen teilnehmen. Der Vorsitz wechselt jährlich unter den Mitgliedern, die Geschäftsstelle ist beim BSI angesiedelt.

Die AG InfoSic tagt regelmäßig dreimal jährlich vor den Sitzungen des IT-Planungsrates, um diese im Themenfeld vorbereiten zu können. Zudem finden je nach Bedarf Sondersitzungen statt.

Ein Schwerpunkt der Tätigkeit ist die Fortschreibung der übergreifenden Leitlinie für Informationssicherheit in der öffentlichen Verwaltung sowie die Begleitung der Umsetzung durch Bund und Länder. Im Umsetzungsplan der Leitlinie sind Maßnahmen in fünf Handlungsfeldern festgelegt:

- Informationssicherheitsmanagement
- Absicherung IT-Netzinfrastruktur öffentliche Verwaltung
- Einheitliches Sicherheitsniveau für Ebenen-übergreifende IT-Verfahren
- Gemeinsame Abwehr von IT-Angriffen
- IT-Notfallmanagement als Teil des ganzheitlichen Notfallmanagements

Daneben werden Einzelthemen bearbeitet, ggf. Empfehlungen abgegeben u. ä. Zudem hat der jeweilige Vorsitz bis zu einem gewissen Grad die Möglichkeit, eigene Akzente zu setzen. So wurde beispielsweise unter Schleswig-Holsteinischem Vorsitz im Jahr 2021 die Intensivierung der Verzahnung und Kooperation von AG InfoSic und LAG Cybersicherheit (siehe nachfolgenden Abschnitt) als ein übergreifendes Thema vorangetrieben.

Die AG InfoSic unterstützt und finanziert regelmäßig zwei Fachtagungen für das Informationssicherheitsmanagement im öffentlichen Sektor:

- Jahrestagung für Informationssicherheitsbeauftragte aus Ländern und Kommunen des IT-Planungsrates, Nürnberg
- Kommunaler IT-Sicherheitskongress der kommunalen Spitzenverbände unter Federführung des Deutschen Landkreistages, Berlin

Schleswig-Holstein bringt sich in der AG InfoSic aktiv ein. Unter anderem hat Schleswig-Holstein den Vorsitz in folgenden Unterarbeitsgruppen inne:

- Gemeinsame Erkennung und Abwehr von Cyberangriffen
- IT-Notfallmanagement als Teil des ganzheitlichen Notfallmanagements/ *Business Continuity Managements*

Die AG InfoSic ist ein wesentlicher Akteur hinsichtlich der Setzung von Mindeststandards für die Informationssicherheit, die vom IT-Planungsrat verbindlich beschlossen werden können.

3.21.2.2. LAG Cybersicherheit

Die Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) der Innenministerkonferenz ist ein weiteres ständiges Gremium des Austausches. In diesem Gremium hat der Bund ein ständiges Gastrecht, stimmberechtigt sind die Länder.

In der LAG Cybersicherheit besteht eine Besonderheit darin, dass naturgemäß auch eine Befassung mit Themen aus den CISO-Funktionsbereichen stattfindet. Diese sind allerdings nicht in allen Ländern dem Innenressort zugeordnet – sondern beispielsweise in Schleswig-Holstein der Staatskanzlei. Umso wichtiger ist intensive Abstimmung, für die sich Schleswig-Holstein regelmäßig einsetzt, siehe auch vorangehenden Abschnitt.

Auch in die Arbeit der LAG Cybersicherheit bringt Schleswig-Holstein sich aktiv ein.

3.21.3. Verwaltungs-CERT-Verbund

Die Landes-CERTs sowie das CERT Bund haben sich im Verwaltungs-CERT-Verbund (VCV) zusammengeschlossen. Dabei handelt es sich um einen geschlossenen Verbund. Im Rahmen der Zuständigkeiten und Befugnisse findet hier ein vertraulicher Informationsaustausch in Angelegenheiten der Prävention, Detektion und Reaktion statt. Dieser Austausch bezieht sich auch auf akute Vorfälle oder sicherheitsrelevante Ereignisse.

Im Verbund bestehen Meldepflichten an den VCV für Sicherheitsvorfälle und sicherheitsrelevante Ereignisse nach bestimmten Kriterien ("VCV-Meldestandard"). Ein wesentliches Ziel dieser Meldungen ist der Schutz anderer Mitglieder des Verbundes bei akut drohenden Gefährdungen. Diese Meldungen werden via CERT in den Verbund eingesteuert.

Auch deshalb ist es wichtig, Vorfälle und sicherheitsrelevante Ereignisse unverzüglich via Informationssicherheitsmanagement an das eigene CERT zu melden. Entsprechende Regelungen werden im Rahmen des jeweiligen Sicherheitsvorfallmanagements des Bundes und der Länder getroffen.

Über das jeweilige Landes-CERT als Schnittstelle zum VCV haben die CISO-Funktionsbereiche der Länder Zugang zum CERT Bund und umgekehrt.

Schleswig-Holstein bringt sich mit dem CERT Nord aktiv in die bewährte Zusammenarbeit von Bund und Ländern im Verwaltungs-CERT-Verbund ein.

3.21.4. Nationales Cyber-Abwehrzentrum (NCAZ, Cyber-AZ)

Das Nationale Cyber-Abwehrzentrum (NCAZ, Cyber-AZ) ist ursprünglich als ein Austausch- und Analysegremium mehrerer Sicherheitsbehörden des Bundes gegründet worden.

Eine Beteiligung aller Länder ist derzeit nicht vorgesehen. Indirekt können bestimmte relevante Informationen jedoch bereits heute an Länder verteilt werden. Denn das CERT Bund ist im Cyber-AZ vertreten und kann bestimmte, dafür vorgesehene relevante Informationen via VCV an die Länder steuern.

3.21.5. Informationsaustausch KRITIS

Die KRITIS-Regulierung findet weitgehend bundesrechtlich statt. Insbesondere enthalten das BSI-Gesetz (BSIG) und die BSI-Kritis-Verordnung (BSI-KritisV) entsprechende Regelungen.

Im Jahr 2011 haben sich der Bund und die Länder auf eine einheitliche Einteilung der Kritischen Infrastrukturen (KRITIS) in neun Sektoren verständigt. Die Einteilung stellt eine gemeinsame Grundlage von Staat und Wirtschaft beim Schutz Kritischer Infrastrukturen dar. Auf Bundesebene wurden die neun KRITIS-Sektoren in verschiedene Branchen unterteilt. Im Zuge der Novellierung des BSIG im Jahr 2021 kam mit der „Siedlungsabfallentsorgung“ ein neuer Sektor hinzu. Die Einteilung der Kritischen Infrastrukturen in die einzelnen Sektoren und Branchen unterliegt einem stetigen Evaluierungsprozess, der die Entwicklungen des politischen Diskurses widerspiegelt. Die zehn Sektoren sind:

- Wasser

- Energie
- Ernährung
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheit
- Informationstechnik und Telekommunikation
- Siedlungsabfallentsorgung
- Kultur und Medien
- Staat und Verwaltung

Innerhalb der Sektoren und Branchen erbringen die Infrastrukturbetreiber zur Versorgung der Allgemeinheit sogenannte kritische Dienstleistungen. Der Ausfall einer solchen kritischen Dienstleistung würde zu erheblichen Versorgungsengpässen, zu Gefährdungen der öffentlichen Sicherheit oder zu vergleichbaren Folgen führen. Es ist Aufgabe der Betreiber Kritischer Infrastrukturen ─ seien es Unternehmen oder Behörden ─ für einen sicheren und zuverlässigen Betrieb ihrer Anlagen und Einrichtungen zu sorgen. Den Bestimmungen und Schwellenwerten der BSI-KritisV unterliegen insbesondere Einrichtungen der Sektoren Kultur und Medien sowie Staat und Verwaltung jedoch nicht.

Betreiber entsprechender Einrichtungen der kritischen Infrastruktur haben sich bei Erfüllung der Kriterien beim BSI als zentraler Stelle zu registrieren. Zudem sind Meldepflichten der KRITIS-Betreiber zu bestimmten Sicherheitsvorfällen oder anderen sicherheitsrelevanten Ereignissen gegenüber dem BSI zu erfüllen, nicht gegenüber einer Landesbehörde.

Schon während des Gesetzgebungsprozesses des 2021 beschlossenen Zweiten IT-Sicherheitsgesetzes ("IT-SiG 2.0") des Bundes haben Bund und Länder sich beraten hinsichtlich einer Verbesserung des Informationsaustausches bei Länderbetroffenheit nach KRITIS-Vorfällen. Schleswig-Holstein hat sich bei diesen Verhandlungen aktiv eingebracht. Inzwischen haben die Abstimmungen zu einer tatsächlichen Verbesserung des Informationsaustausches und einem aus Schleswig-Holsteinischer Sicht positiven Ergebnis geführt.

3.21.6. Umsetzung der NIS-2-Richtlinie

Der Kreis der betroffenen Einrichtungen und Anlagen der kritischen Infrastruktur wird mit der Umsetzung der sogenannten NIS-2-Richtlinie der EU deutlich ausgeweitet. Die Richtlinie unterscheidet zwischen "wichtigen" und "wesentlichen" (besonders

wichtigen) Einrichtungen und stellt jeweils spezifische Anforderungen an Maßnahmen der Informations- und Cybersicherheit in diesen Einrichtungen.

Neu ist unter anderem, dass auch Einrichtungen der öffentlichen Verwaltung stärker als bisher bestimmten Anforderungen unterliegen werden. Dabei wird unterschieden zwischen Bundes- und Landesebene.

Auf Bundesebene werden – neben den weiterhin auf Bundesebene zu treffenden Regularien für die anderen Sektoren – Anforderungen an Einrichtungen der Bundesverwaltung gestellt. Hierfür befindet sich ein Gesetzentwurf des "NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes" (NIS2UmsuCG) derzeit in Ressortabstimmung im Bund.

Auf Landesebene ist für den Bereich der öffentlichen Verwaltung ein risikobasiertes Identifizierungskonzept zu erstellen, mit dem betreffende Einrichtungen ermittelt werden. Wesentliches abstraktes Kriterium ist, vereinfacht formuliert, dass bei einem längeren Ausfall kritischer Dienste einer Einrichtung ein erheblicher Folgeschaden droht. Einrichtungen, bei denen dieses der Fall ist, sollen den Anforderungen hinsichtlich Informations- und Cybersicherheitsmaßnahmen unterliegen.

Der IT-Planungsrat hat die Zuständigkeit für eine Befassung mit dem Identifizierungskonzept für die Landesebene und entsprechende Beschlussfassung, mit der im November 2023 zu rechnen ist.

3.21.7. Umsetzung der CER-Richtlinie

Eng mit der Umsetzung der NIS-2-Richtlinie verbunden ist die Umsetzung der sogenannten CER-Richtlinie (Resilienzrichtlinie, *Critical Entities Resilience*). Hierbei ist eine komplementäre Regulierung vorgesehen:

- die NIS-2-Richtlinie befasst sich mit Anforderungen an die Informations- und Cybersicherheit von Anlagen der kritischen Infrastruktur
- die CER-Richtlinie befasst sich mit Anforderungen an die physische Sicherheit von Anlagen der kritischen Infrastruktur

In der Praxis lassen sich beide Bereiche nicht immer klar voneinander trennen. Wenn beispielsweise jemand Unbefugtes mit einem USB-Stick in der Hand ein Elektrizitätswerk betritt und den USB-Stick in einen Computer einstöpselt, sind sowohl Informationssicherheit als auch physische Sicherheit betroffen. Zudem ist es von enormer Wichtigkeit, dass betroffene Einrichtungen von beiden Richtlinien bzw. deren Umsetzungsgesetzen möglichst widerspruchsfrei reguliert werden. Schließlich soll der Erfüllungsaufwand für betroffene Einrichtungen möglichst minimiert werden, beispielsweise durch einheitliche Meldepflichten nach beiden Richtlinien.

Die Landesregierung setzt sich in diesem Sinne für eine möglichst gut verzahnte Umsetzung beider Richtlinien auf Bundesebene ein.

Zudem setzt sich die Landesregierung für eine angemessene Beteiligung der Länder ein, da diverse Länderzuständigkeiten insbesondere der Gefahrenabwehr berührt sind.

3.21.8. BSI-Zentralstellenkonzept

Schleswig-Holstein arbeitet seit langem eng mit dem BSI zusammen. Das übergreifende Informations- und Cybersicherheitsmanagement unter Leitung des CISOs ist die zentrale Schnittstelle zum BSI. Die Zusammenarbeit von Bund und Ländern muss sich angesichts der heutigen und absehbaren Gefährdungslage noch intensivieren. Sollten dafür Änderungen in der grundgesetzlichen festgeschriebenen Kompetenzordnung notwendig sein, wird sich die Landesregierung einer Diskussion nicht verschließen. Orientierungspunkt ist dabei die konsequente Ausrichtung am Subsidiaritätsprinzip. Aufgaben sollten auf der Ebene verortet werden, auf der sie am besten erledigt werden können. Zu Möglichkeiten der konkreten Ausgestaltung im Miteinander von zentralen und dezentralen Stellen steht die Landesregierung bereits jetzt in einem konstruktiven Austausch auch mit dem BSI. Die Landesregierung spricht sich nachdrücklich dafür aus, den begonnenen fachlich-strategischen Dialog zu intensivieren und das gemeinsame Vorhaben zur Optimierung der Bund-Länder-Zusammenarbeit fortzusetzen. Es gilt, dass Informations- und Cybersicherheit nur gemeinsam hergestellt und aufrechterhalten werden kann.

Neben der Zusammenarbeit mit dem Bund gestaltet Schleswig-Holstein auch die länderübergreifende Zusammenarbeit im Bereich der Informations- und Cybersicherheit aktiv mit – besonders eng kooperieren wir mit den anderen Trägerländern des gemeinsamen IT-Dienstleisters Dataport AöR.

4. Ausblick

Nachfolgend wird ein Ausblick auf mögliche Hauptbedrohungen in den nächsten Jahren sowie auf aktuelle Vorhaben der Landesregierung zur Verbesserung der Informations- und Cybersicherheit gegeben.

4.1. Antizipierte Bedrohungen 2030 (ENISA)

Die Agentur der Europäischen Union für Cybersicherheit (ENISA)[9] hat eine Analyse und Bewertung veröffentlicht, welche Hauptbedrohungen für das Jahr 2030 zu erwarten sein könnten.

[9] Ursprüngliche Bezeichnung: *European Union Network and Information Security Agency* (ENISA).

Top 10 Bedrohungen; ENISA Report: Identifying emerging cyber security threats and challenges for 2030, März 2023

4.1.1. Kompromittierung der Lieferkette durch Software-Abhängigkeit

Anbieter von Software – Hersteller, Lieferanten und Dienstleister – implementieren unbewusst oder sogar bewusst Schwachstellen (Hintertüren) in Software, welche eine Sicherheitslücke darstellen. Diese Lücken könnten ausgenutzt werden, um Informationen zu erlangen, zu verfälschen oder die Verfügbarkeit der Systeme zu beeinträchtigen. Durch die aus guten Gründen starke Zunahme der Verwendung von Open-Source-Bibliotheken, um einzelne Programmfunktionen zu integrieren, entstehen verstärkt Abhängigkeiten von deren Sicherheitsniveau. Eine Manipulation oder Schwachstelle innerhalb dieser Bibliotheken könnte dadurch weitreichende Auswirkungen für die Vielzahl der nutzenden Anwendungen haben.

4.1.2. Fortschrittliche Desinformationskampagnen

Durch gefälschte, aber sehr realistisch wirkende Medieninhalte, vor allem Videos, Audioinhalte oder Bilder ("*Deep Fakes*") sowie durch den Diebstahl oder die Nachahmung von digitalen Identitäten könnten falsche Informationen und Meinungen verbreitet werden. Das kann zu einer Manipulation von Entscheidungen führen (beispielsweise Wahlentscheidungen) oder Misstrauen verursachen.

4.1.3. Zunahme digitaler Überwachung, Verlust der Privatsphäre

Die Möglichkeiten zur Erfassung von persönlichen Daten – wie beispielsweise Bewegungsprofile, biometrische Gesichtsdaten oder auch einfach Videoaufnahmen durch Überwachungskameras in öffentlichen und privaten Bereichen – nehmen stark zu. Das erfordert, dass die Gesetze und Regularien zum Schutz personenbezogener

Daten durchgesetzt und weiterentwickelt werden, um dem Stand der Technik zu entsprechen.

Darüber hinaus besteht auch eine Gefahr für die im gesetzlichen Rahmen ordnungsgemäß erhobenen und gespeicherten Daten. Diese immer größer werdenden Datenmengen müssen dauerhaft zuverlässig vor beispielsweise Identitätsdiebstahl oder anderen unberechtigten Zugriffen einschließlich Manipulation geschützt werden.

4.1.4. Menschliche Fehlhandlungen und ausgenutzte Altsysteme in Cyber-physischen Ökosystemen

Das sogenannte Internet der Dinge (*Internet of Things*, IoT) durchdringt beispielsweise mit Sensorik immer größere Teile der Verkehrs-, Strom- und Wassernetze sowie der industriellen Infrastruktur. Auf diese Weise lassen sich die Effizienz steigern und intelligente Entscheidungsfindung verbessern. Damit werden Nutzer aber auch eine immer höhere Anzahl an Geräten für den Betrieb benötigen.

Diese Geräte dauerhaft zuverlässig zu verwalten und zu warten (allgemeines Management, Fehlerbehebungen, Sicherheitsaktualisierungen und physische Instandhaltung) wird nicht nur durch die hohe Anzahl und den rasanten Anstieg an Geräten erschwert. Auch wird der Fachkräftemangel zu fehlendem Know-How bei der Verwaltung und Wartung dieser Geräte führen. Dies wiederum kann sowohl falsche Nutzung zur Folge haben als auch zu Ausfällen der kritischen Systeme selbst durch verzögerte oder ausbleibende Wartung führen. Durch die notwendige Vernetzung der Geräte und die Kritikalität der Systeme (beispielsweise Stromnetzüberwachung oder Steuerung eines Umspannwerkes) bilden diese ein besonderes Angriffsziel, was durch unterschiedliche Methoden zu Störungen oder Ausfällen führen kann.

4.1.5. Verstärkung gezielter Angriffe (z. B. Ransomware) durch Daten smarter Geräte

Angreifer könnten sich als Einstiegspunkt den Zugang über mit dem Internet verbundene "*Smart Devices"* verschaffen, welche nicht angemessen gewartet wurden oder schlicht noch die Standard- bzw. Werkseinstellungen (Nutzername und Passwort) nutzen. Entsprechende weitere Information können von dem Gerät erbeutet werden und für die Authentifizierung und den Zugang zu sensiblen Daten und Informationen innerhalb eines Netzwerkes genutzt werden.

Durch eine automatisierte Datenerfassung der Geräte, wie beispielsweise Verhaltensprofile für künstliche Intelligenz, können Angreifer diese Datensammlungen nutzen, um ihr Verhalten zu adaptieren und so länger unerkannt im Netzwerk bleiben und mehr sensible Daten stehlen oder verfälschen.

4.1.6. Fehlende Analyse und Kontrolle weltraumgestützter Infrastruktur und Objekte

Die Anzahl privater Unternehmen, welche Zugang zum Weltraum anbieten, steigt an. Diese Unternehmen bauen auch eine Infrastruktur im Weltraum auf, die für eine Bereitstellung von Diensten im privaten und öffentlichen Sektor genutzt wird. Diese Infrastruktur bietet ein erhöhtes Bedrohungspotential.

Es mangelt noch an Verständnis, Analyse und Kontrolle hinsichtlich von Sicherheits- und Abwehrmechanismen dieser Infrastruktur gegenüber Angreifern. So könnten Angreifer die Schnittstellen zwischen privaten und öffentlichen Systemen und Infrastruktur ausnutzen, um gezielt Zugang zu der kritischen Infrastruktur (beispielsweise Ortungssysteme wie GPS) zu erhalten und diese zu stören. Mit der entsprechenden Infrastruktur agierende Personen könnten dafür gezielt ins Visier genommen werden.

4.1.7. Zunahme fortschrittlicher hybrider Bedrohungen

Die Angriffsmethoden entwickeln sich stetig weiter und werden immer stärker kombiniert, um die entsprechenden Ziele zu erreichen. Cyberangriffe werden dadurch mehrschichtiger und ausgereifter, vor allem in der Kombination mit physischen und Offline-Angriffen. Durch die Einbeziehung großer Datenmengen (Big Data) und die Nutzung künstlicher Intelligenz und deren Mechanismen wie "*Deep Learning*" werden neue Methoden geschaffen bzw. sehr schnell angepasst, um bestehende Abwehrmechanismen umgehen zu können.

Die automatisierte Verknüpfung der Informationen von Online-Identitäten und sozialen Plattformen ermöglicht die Schaffung kreativer Angriffsmethoden, welche beispielsweise mit psychologisch geschickter Interaktion mit Zielpersonen ("*Social Engineering*") beginnen, darauf gezielte Angriffe von Systemen und Nutzerkonten aufbauen, um schließlich den Zugriff auf sensible Informationen oder kritische Infrastrukturen zu erlangen.

4.1.8. Fachkräftemangel

Die Anzahl an Tätigkeiten mit Relevanz für Informationssicherheit nimmt nicht nur durch die steigende Bedrohungslage zu, sondern auch aufgrund des gesteigerten Bewusstseins für die Wichtigkeit dieses Themas. Dem gegenüber steht aber das stark wachsende Problem des Fachkräftemangels: selbst bereits vorhandene Stellen können nicht besetzt werden oder der erforderliche Wissensstand kann nicht vollständig aufgewiesen werden. Angreifer könnten diese Wissens- und Kompetenzschwächen durch Analyse der Fähigkeiten und Defizite der Organisation (beispielsweise Stellenausschreibungen) gezielt ausnutzen, um genau an diesen Punkten Angriffe anzusetzen.

Ein wichtiger Faktor, der sich auf die Bedrohung 2030 auswirken wird, ist die Bereitschaft, Personal und Ressourcen aufzustocken, Wissenslücken zu schließen und Talente zu entwickeln.

4.1.9. Grenzübergreifende Dienstanbieter der Informations- und Kommunikationstechnik als ein einzelner Ausfallpunkt

Die technologische Verflechtung nimmt immer stärker zu, sodass die Grenze zwischen physischem und Cyber-Raum weiter verschwimmt. Die Sektoren der kritischen Infrastruktur sind immer mehr auf Dienstleister der Informations- und Kommunikationstechnik angewiesen, um sich mit dem Internet zu verbinden und somit die Kommunikation zwischen Personen, Geräten und Standorten zu ermöglichen. Diese Anbieter stellen ein immer populäreres Angriffsziel dar und werden auch in zukünftigen Konflikten immer mehr als „Waffen“ ausgenutzt. Daher müssen sie sich gegen staatlich geförderte, andauernde und hochentwickelte Angriffe wehren.

Die Störung oder der Ausfall eines einzelnen solchen Dienstleisters hat aufgrund der vielen verbundenen kritischen Dienste einen weitreichenden Einfluss.

4.1.10. Missbrauch künstlicher Intelligenz

Neben den enormen Vorteilen der Künstlichen Intelligenz stellt sie auch ein wichtiges Werkzeug für die Weiterentwicklung von Angriffsmethoden dar. Angreifer könnten künstliche Intelligenz nutzen, um aus Abwehrmechanismen und -verhalten zu lernen und diese zukünftig einfacher zu umgehen oder sogar wirkungslos werden zu lassen. Ebenso kann Künstliche Intelligenz genutzt werden, um Schadcode automatisiert sehr schnell zu ändern und zu verteilen und dadurch die Erkennung und Abwehr deutlich zu erschweren.

Weiterhin stellen Systeme der Künstlichen Intelligenz selbst ein Angriffsziel dar. Die Trainingsalgorithmen könnten manipuliert werden und somit ein fehlerhaftes oder gar negativ gerichtetes Verhalten provoziert werden.

Dem kann vor allem durch die Weiterentwicklung von KI gestützten Methoden zur Unterstützung hinsichtlich entsprechender Bedrohungen entgegengewirkt werden.

4.1.11. Weitere antizipierte Bedrohungen

- Zunahme der Cyberkriminalität mit Hilfe von digitalen Währungen
- Ausnutzung von elektronischen Gesundheits- und genetischen Daten
- Manipulation mittels "*Deep Fake*" in Verifikations-Software
- Angriffe mit Hilfe von Quantencomputern

- Ausnutzung schlecht gewarteter und veralteter Systeme innerhalb des überlasteten sektorübergreifenden Technologie-Ökosystems
- Schadsoftware zur Unterbrechung der Lebensmittelproduktionskette
- Technische Inkompatibilität der Blockchain-Technologien
- Störungen von öffentlichen Blockchains
- Physische Auswirkung durch natürliche und umweltbedingte Störungen auf kritische digitale Infrastrukturen
- Manipulation von Systemen zur Notfallreaktion

4.2. Digitale Resilienz in der Digitalen Vorzeigeregion Schleswig-Holstein – Stärkung der Informations- und Cybersicherheit

Diese antizipierten Bedrohungen unterstreichen, dass es sich beim Informations- und Cybersicherheitsmanagement um Daueraufgaben im Kernbereich der Verwaltungstätigkeit handelt. Einige der Bedrohungen bestehen auch heute schon, werden aber voraussichtlich künftig ein noch stärkeres Ausmaß haben. Andere Bedrohungen sind neu, beispielsweise aufgrund technischen Fortschritts, und erfordern möglicherweise neue Methoden der Prävention, Detektion und Reaktion.

Bürgerinnen und Bürger, unsere Unternehmen und unsere öffentlichen Verwaltungen müssen sich auch im digitalen Raum sicher bewegen können. Die Landesregierung misst der Informations- und Cybersicherheit höchste Priorität bei. Deshalb plant die Landesregierung konkrete Maßnahmen für eine erhebliche Stärkung der Informations- und Cybersicherheit und der Digitalen Resilienz zu ergreifen.

Folgende Maßnahmen in den beschriebenen Handlungsfeldern sind geplant:

4.2.1. Ausbau des Informations- und Cybersicherheitsmanagements der Landesregierung

- Aufbau und Umsetzung der übergreifenden Kernprozesse des ISM der Landesverwaltung:
    - Sicherheitsvorfallmanagement, Risikomanagement, Audits und Revisionen, Schulungsplattform/-inhalte
    - IT-Notfallmanagement als Teil des ganzheitlichen *Business Continuity Managements* (BCM) mit Schnittstellen zum Krisenmanagement der Landesregierung; im ersten Schritt wird der Aufbau eines sogenannten Reaktiv-BCMS (*Business Continuity Management System*) gemäß kürzlich veröffentlichtem BSI-Standard 200-4 angestrebt

  - Ausbau und Weiterentwicklung des zentralen ISMS-Tools, sukzessive Einführung in weiteren Ressorts, bis Ende 2025 in allen Ressorts
  - Organisatorische und personelle Stärkung des übergreifenden ISM, Aufbau eines unabhängigen ISM fürs ZIT, ggf. Poolbildung für Aufgabenübertragungen anderer Ressorts ans ISM, BSI-Zertifizierungen

- Besetzung von Rollen:
  - ISB für das ZIT, angesiedelt im CISO-Funktionsbereich
  - Informationssicherheitskoordination mit auftraggeberseitigen Zuständigkeiten für jeweils einzelne IT-Verfahren bzw. -Infrastrukturen (Zuarbeit für IT-Verantwortliche und IT-Notfallbeauftragte)
- Ausbau des CERT Nord und des *Security Operations Centers* (SOC)
  - Erweiterung der Unterstützungsleistungen für das ISM der Landesverwaltung
  - Aufbau von CERT-Nord-Unterstützung für die Kommunen
  - Erweiterung CERT Nord als Teil eines Landes-CSIRTs, Beteiligung an einem mobilen Einsatzteam (MIRT, *Mobile Incident Response Team*), BSI-Kooperation
  - Ausbau des SOC als Teil eines CSIRTs, Aufbau mobiler Einsatzkapazitäten (MIRT)
- Unterstützung der Kommunen
  - Verstetigung des Projektes SiKoSH
  - Durchführung des Webinar-Formats "Roadshow Kommunen" gemeinsam mit dem BSI und unter Einbeziehung der Kommunalen Landesverbände und des ITV.SH
  - Förderprogramm "Kommunale Resilienz", ggf. auch für Schulen (fördern und fordern)
  - Anfertigung von Lagebildern zur Informations- und Cybersicherheit im Land einschließlich kommunaler Ebene
- Umsetzung der NIS2-Anforderungen auf Landesebene (soweit bereits schätzbar; abhängig von tatsächlichen rechtlichen Anforderungen, die noch zu klären sind)

  - erweiterte materielle Anforderungen an bestimmte Behörden
  - Aufbau aufsichtsbehördlicher ISM-Funktionen
- Ausbau und Konsolidierung der übergreifenden strategischen Rolle des Landes-ISM
  - Koordinierender, kooperativer, agiler Überbau über Initiativen der Landesregierung zur Informations- und Cybersicherheit
  - Formulierung der übergreifenden Landesstrategie Digitale Resilienz, damit auch Umsetzung einer Anforderung aus der NIS-2-Richtlinie
  - Aufbau und Förderung eines Resilienz-Ökosystems mit relevanten Akteuren rund um das Landes-ISM, Vernetzung

4.2.2. Fachkräftegewinnung und -bindung

Die Landesregierung wird sowohl die interne Weiterbildung als auch externe Fort- und Ausbildungen stärken, um Fachkräfte für das Informationssicherheitsmanagement zu gewinnen. Zudem wollen wir vorhandene und neu geschaffene bzw. umgewidmete Stellen attraktiv ausgestalten, um Fachkräfte langfristig zu halten.

4.2.3. Kooperationsvereinbarung mit dem BSI

Die Landesregierung wird die Verhandlungen mit dem BSI intensivieren mit dem Ziel, im Jahr 2024 eine Kooperationsvereinbarung abzuschließen. Gegenstand sollen Themenfelder der Zusammenarbeit sein wie beispielsweise gemeinsame Veranstaltungsreihen, Forschungsprojekte, Notfallübungen u. a.

4.2.4. Entwurf eines Gesetzes für Digitale Resilienz in Schleswig-Holstein (Informationssicherheitsgesetz)

Die Landesregierung wird Regelungen zur Informationssicherheit und zur Digitalen Resilienz konsolidieren und erweitern und dies in einer einheitlichen Grundlage verankern. In diesen sollen auch Regelungen zur Umsetzung der NIS-2-Richtlinie auf Landesebene enthalten sein.

4.2.5. Weiterentwicklung der SicherheitsPartnerschaft SH

Die Landesregierung wird die SicherheitsPartnerschaft SH konsolidieren und bedarfsgerecht weiterentwickeln. Das Angebot soll ein eigener Baustein – mit erhöhter Sichtbarkeit auch des Wirtschaftsressorts als Akteur – in der übergreifenden Informations- und Cybersicherheitsarchitektur des Landes sein. Die SicherheitsPartnerschaft SH soll mit anderen Angeboten der Landesregierung sinnvoll verzahnt und entsprechend koordiniert werden.

4.2.6. Förderung der Informations- und Cybersicherheitsforschung

Die Landesregierung wird Forschungskooperationen im Bereich Informations- und Cybersicherheit gezielt fördern. Zudem wird sie die begonnene länderübergreifende Vernetzung in diesem Bereich, beispielsweise mit der Länderplattform Cybersicherheitsforschung (LPC, Koordination Hessen) festigen und verstetigen.

4.2.7. Intensivierung der Zusammenarbeit mit Bund und Ländern

Die Landesregierung wird sich weiterhin aktiv in die Gremien und sonstigen Abstimmungen und Vorgänge zur Intensivierung der Zusammenarbeit von Bund und Ländern einbringen. Sie wird die bedarfsgerechte Weiterentwicklung des Verwaltungs-CERT-Verbundes vorantreiben, denn Informationssicherheit geht nur gemeinsam.

4.2.8. Förderung des Informationssicherheitsmanagements an Hochschulen

Die Landesregierung wird die Hochschulen beim Auf- und Ausbau eines systematischen Informationssicherheitsmanagements unterstützen.

4.2.9. Förderung des Informationssicherheitsmanagements an Schulen

Die Landesregierung wird die Schulen beim Auf- und Ausbau eines systematischen Informationssicherheitsmanagements unterstützen.