Der Chef der Staatskanzlei | Postfach 7122 | 24171 Kiel

Vorsitzender des Wirtschafts- und
Digitalisierungsausschusses
Herrn
Claus Christian Claussen, MdL
Landeshaus
24105 Kiel

Minister

Schleswig-Holsteinischer Landtag
Umdruck 20/5961

22. Januar 2026

Sachstand Informationssicherheit in der Landesverwaltung

Sehr geehrter Herr Vorsitzender,

die Landesregierung hat umfangreich in ihrem "Bericht über die Cybersicherheit unserer Infrastruktur" (Drucksache 20/1584, 07. November 2023) sowie ergänzend mit Schreiben vom 2. April 2025 (Umdruck 20/4680) umfassend über die Maßnahmen zum Stand und zur Fortentwicklung der Informations- und Cybersicherheit der Landesverwaltung informiert.

Inzwischen sind weitere umfassende Maßnahmen zur Erhöhung der Informationssicherheit ergriffen worden, über die ich Sie gern informiere. Vorweg möchte ich betonen, dass die Entwicklungen auch in diesem Aufgabenfeld einem dynamischen Pfad folgen und daher die notwendigen Maßnahmen einer ständigen Anpassung bedürfen.

Folgende konkrete Schritte und Maßnahmen wurden seit der letzten schriftlichen Berichterstattung eingeleitet und umgesetzt:

- Schleswig-Holstein ist seit Ende Oktober 2025 NIS-2-notifiziert. Hierfür wurde eine neue Informationssicherheitsleitlinie in Kraft gesetzt.
- Die Landesregierung hat die Eckpunkte zur Informations- und Cybersicherheitsstrategie beschlossen, welche aktuell weiter ausgearbeitet wird.
- Das CERT Nord wurde zum CSIRT (Cyber Security Incident Response Team) weiterentwickelt. Es verwaltet nun Sicherheitsmeldungen sowohl für die Landesverwaltung als auch für die schleswig-holsteinischen Kommunen. Das ist ein wichtiger Schritt hinzu einer ganzheitlichen Betrachtung über die

Verwaltungsebenen hinweg und bietet Unterstützung für die kommunale Ebene. Es berät alle Behörden bei konkreten Sicherheitsvorfällen.

- Ferner wurden gemeinsam mit Dataport Sicherheits-Teams beauftragt, die bei kritischen Sicherheitsvorfällen vor Ort in den Behörden Detektion und Wiederherstellung initiieren können.
- Durch die Umsetzung der Open-Source-Strategie mit der Einführung von Open Xchange, Nextcloud und LibreOffice auf den Arbeitsplätzen besteht ein höherer Schutz vor fehleranfälliger Software, da Sicherheitslücken auch unabhängig vom Hersteller durch Quellcodeanalyse erkannt werden und schneller behoben werden können.
- Im Zentralen IT-Management wurde die Rolle der Chief Information Security Officer (CISO) a deutlich gestärkt, die mit ihrem Team und durch die enge Vernetzung mit dem IT-Betrieb und den Informationssicherheitsbeauftragten der Ressorts sowie dem ITV.SH Regeln und Prozesse zum Einsatz neuer IT-Verfahren entwickelt und überprüft. Das Team umfasst derzeit 6 Mitarbeiterinnen und Mitarbeiter.
- Für alle zentralen IT-Leistungen der Landesverwaltung wird aktuell das Informationssicherheitsmanagement unter anderem auch mit Fokus auf kommenden Entwicklungen im Umfeld NIS-2 geändert. Dies umfasst einheitliche Störungsmeldungen, unabhängige Systemüberwachung und landesweit bekannt gemachte Verfahren zur Meldung von Sicherheitsvorfällen an das CERT Nord und Dataport.
- Durch eine enge Vernetzung der Beratung bei Dataport werden die Anforderungen an die Sicherheit der Kommunen aus dem Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) und die Anforderungen an die Landesbehörden gemeinsam durch die CISO und das ZIT gebündelt, um Synergien zu nutzen und mittelfristig eine gemeinsame Sicherheitsarchitektur zu implementieren. Hierbei wird der ITVSH als „kommunale Kopfstelle“ eng auf Augenhöhe eingebunden.
- Im ZIT wird für die Ressorts und die Kommunen ein erweitertes Schwachstellen-Management erprobt und soll 2026 in Produktion gehen. Somit werden über das hohe Schutzniveau im Dataport-Rechenzentrum hinaus nun auch in den lokalen Netzen Gefahren besser erkannt und können sowohl zentral als auch in der Hoheit der einzelnen Verwaltung bewertet und beseitigt werden.
- Es wird eine Angriffserkennung auf den Endgeräten eingeführt (Managed Endpoint Detection and Protection). Ziel der Umsetzung ist es, nicht nur die Resilienz an den Außengrenzen des Landesnetzes weiter zu verbessern, sondern auch innerhalb des sicheren Netzes mit Gefährdungen noch besser umgehen zu können.
- In Abstimmung mit dem Krisenmanagement des MIKWS wird ein infrastrukturunabhängiger Notfall-Arbeitsplatz entwickelt. Als mobile IT-Ausstattung wird ein Netzwerk mit Kommunikationsservern, elementar nötigen Daten und zunächst bis zu 100 Arbeitsplätzen aufgebaut. Dies kann sowohl z.B. bei einem regionalen Ausfall, wie einen Hackerangriff auf eine Verwaltung, als auch bei einem umfangreichen Kriseneintritt, wie einer Bedrohung zahlreicher Landesliegenschaften durch Stromausfall oder ‚verseuchtem‘ IT-Netz, in dem die Handlungsfähigkeit der Ministerinnen und Minister und ihrer Stäbe gestört ist, eingesetzt werden.

- Darauf aufbauend wird 2026 das Notfall- und Business Continuity Management erweitert. Nach einer Störung wird somit ein möglichst schneller umfassender IT-Betrieb für alle Mitarbeitenden wieder hergestellt bzw. im optimalen Ausbau haben Störungen aufgrund einer infrastrukturellen Dopplung zentraler Systeme keinen Einfluss auf die Verfügbarkeit.
- Die Landesregierung hat dem BSI den Abschluss einer Kooperationsvereinbarung angeboten, um über die gesetzlich verankerte Zusammenarbeit z.B. bei Lagebildern oder der Meldung kritischer Unternehmen hinaus eine Zusammenarbeit auf Verwaltungsebene zu etablieren. Hierdurch kann der Bund Erfahrungen aus der Praxisnähe und dem innovativen Open-Source-Ansatz Schleswig-Holsteins erwerben, das Land profitiert im Gegenzug von Fachinformationen und einer engen Einbindung in die Weiterentwicklung des BSI-Grundschutzes.
- Die CISO vertritt das Land in der LAG Cybersicherheit der Innenministerkonferenz und ist eingebunden in die bundesweite Vernetzung und den Aufbau von Koordinierungsstellen für ein Flächennetzwerk Cybersicherheit. Hierdurch soll auch bundesweit eine einheitliche Resilienz gegen Cyberangriffe geschaffen werden. Die Koordinierung umfasst eine enge Abstimmung mit den Gefahrenabwehrbehörden des Bundes und der Länder, wie z. B. Verfassungsschutz, polizeiliche Prävention und Repression, daneben auch Katastrophenschutz sowie zivile Verteidigung.

Der Landesregierung ist bewusst, dass die Informationssicherheit auch zukünftig ein weiter dynamisch wachsendes Themenfeld bleibt, in dem neue und angepasste Maßnahmen erforderlich sind, um den Stand der Technik zu halten und den Schutz unserer digitalen Infrastruktur auszubauen. Insbesondere die digitale Resilienz braucht erhebliche Anstrengungen, die auch über die rein informationstechnischen Aufgaben hinausgehen.

Mit freundlichen Grüßen

gez. Dirk Schrödter