Schleswig-Holstein

Maßnahmenpaket für Cyber-Sicherheit

[28.05.2026] Schleswig-Holstein baut die Cyber-Sicherheit für Land und Kommunen aus. Zum Schutzschirm gehören unter anderem ein erweitertes Schwachstellenmanagement, mobile IT für Krisenlagen und Vor-Ort-Supportteams. Digitale souveräne Arbeitsplätze und IT-Infrastruktur sichern Behörden weiter ab.

Land und Kommunen sehen sich zunehmend digitalen Angriffen ausgesetzt – die Anforderungen an die IT-Sicherheit in öffentlichen Verwaltungen steigen. Nun berichtet die Staatskanzlei des Landes Schleswig-Holstein über weitere Maßnahmen zur Stärkung der Informationssicherheit in der öffentlichen Verwaltung.

Staatskanzlei-Chef und Digitalisierungsminister Dirk Schrödter hatte vor kurzem den Wirtschafts- und Digitalisierungsausschuss des Landtages schriftlich über weitere Maßnahmen zur Stärkung der Informationssicherheit informiert. Auch schon im vergangenen Jahr hatte Schrödter dem Ausschuss ein Maßnahmenbündel vorgestellt. Mit umfassenden Maßnahmen werde die Informations- und Cybersicherheit sowie die digitale Resilienz Schleswig-Holsteins gestärkt. „Beides sind Querschnittthemen, die Sicherheit im digitalen Raum wird daher auch ressortübergreifend sowie im engen Austausch mit Kommunen, Ländern bis hin zur EU-Ebene angegangen“, so Schrödter.

Hilfe für Landesverwaltung und Kommunen

Schleswig-Holstein hat bereits zahlreiche konkrete Maßnahmen zur Stärkung der Informations- und Cyber-Sicherheit auf den Weg gebracht. So ist das Land seit Oktober 2025 für den EU-weiten Sicherheitsstandard nach der NIS-2-Richtlinie notifiziert. Grundlage dafür ist eine neue Informationssicherheitsleitlinie. Zudem hat die Landesregierung Eckpunkte für eine Informations- und Cyber-Sicherheitsstrategie beschlossen, die derzeit weiter ausgearbeitet wird. Die zentrale IT-Sicherheitseinrichtung CERT Nord wurde zum Cyber Security Incident Response Team (CSIRT) weiterentwickelt. Sie verwaltet Sicherheitsmeldungen für Landesverwaltung und Kommunen und berät bei konkreten Vorfällen.

Gemeinsam mit dem Landes-IT-Dienstleister Dataport wurden außerdem Sicherheitsteams beauftragt, die bei kritischen Lagen vor Ort unterstützen. „Durch die enge Vernetzung zwischen den einzelnen Landesbehörden, IT-Dienstleister, Kommunen und der Bundesebene ist die Architektur unser IT-Sicherheit in Schleswig-Holstein auch für die kommenden Jahre gut aufgestellt. Wir investieren als Land unter anderem auch in übergreifende Sicherheitsmaßnahmen, um die Kommunen zu entlasten“, sagte Minister Schrödter. So stünden den Schulen kostenfrei sichere Internetzugänge über das glasfaserbasierte Landesnetz zur Verfügung.

Strukturen für den Krisenfall

Im Zentralen IT-Management des Landes wurde die Rolle der Chief Information Security Officer gestärkt. Das CISO-Team entwickelt ressortübergreifend Regeln und Prozesse für neue IT-Verfahren. Zugleich bündelt das Land Sicherheitsanforderungen von Kommunen und Landesbehörden, um gemeinsame

Strukturen aufzubauen; der ITV.SH wird dabei eng einbezogen.

Für Ressorts und Kommunen erprobt das Land zudem ein erweitertes Schwachstellenmanagement, das noch 2026 in den Regelbetrieb gehen soll. Geplant sind auch eine Angriffserkennung auf Endgeräten, ein infrastrukturunabhängiger Notfall-Arbeitsplatz für Kabinett oder Krisenteams sowie eine mobile IT-Ausstattung mit Kommunikationsinfrastruktur, die etwa bei regionalen Ausfällen nach Cyber-Angriffen eingesetzt werden kann.

Digitale Souveränität als Sicherheitsbaustein

Darüber hinaus leiste der Weg Schleswig-Holsteins in die digitale Souveränität einen wichtigen Beitrag für die IT-Sicherheit im Land, so Schrödter. Durch die Umsetzung der Open-Source-Strategie mit der Einführung von Open-Xchange, Nextcloud, OpenTalk und LibreOffice auf den Arbeitsplätzen bestehe ein höherer Schutz vor fehleranfälliger Software, da Sicherheitslücken unabhängig vom Hersteller durch Quellcodeanalyse erkannt und schneller behoben werden können. Dazu trage auch der Umbau der System-Zugriffssysteme bei, wo zukünftig die Open Source Lösung Nubus von Univention zum Einsatz kommen werde. Hier nehme Schleswig-Holstein europaweit eine Vorreiterrolle ein.

Bereits im März 2026 wurde das Projekt zum Aufbau einer sicheren souveränen 5G-Kommunikationsarchitektur erfolgreich abgeschlossen. Die 5G-Campusnetze in Schleswig-Holstein sind ein zentraler Baustein für digitale Souveränität und Krisenprävention. Sie ermöglichen im Ernstfall Kommunikation, Datenerfassung und -übertragung und den Zugriff auf Fachverfahren und Daten im BSI-zertifizierten Rechenzentrum von Dataport. Damit bleiben Einsatzfähigkeit und Koordination der Behörden auch bei Ausfall der öffentlichen Netze gewährleistet.

(sib)

Stichwörter: IT-Sicherheit, Digitale Souveränität, Schleswig-Holstein