Schleswig-Holstein

Schrödter offen für Cyber-Sicherheitsgremium

[12.10.2026] Digitalisierungsminister Dirk Schrödter unterstützt die Prüfung eines nationalen Cyber Incident Review Boards, das schwerwiegende Cyber-Angriffe systematisch untersuchen und daraus Handlungsempfehlungen ableiten soll. In einer Landtagsrede verwies er auf die wachsende Bedrohung digitaler Infrastrukturen und stellte die bereits ergriffenen Sicherheitsmaßnahmen Schleswig-Holsteins vor.

Die zunehmende Zahl und Intensität von Cyber-Angriffen auf Behörden, Unternehmen und kritische Infrastrukturen erfordert nach Auffassung von Schleswig-Holsteins Digitalisierungsminister Dirk Schrödter eine systematische Aufarbeitung schwerwiegender Sicherheitsvorfälle. In einer Landtagsdebatte vergangene Woche über die mögliche Einrichtung eines nationalen Cyber Incident Review Boards betonte er, dass IT- und Cyber-Sicherheit inzwischen die gleiche Priorität wie die Sicherheit im Straßenverkehr habe.

Ein solches Gremium könnte Cyber-Vorfälle mit gesamtstaatlicher Relevanz unabhängig untersuchen, Ursachen und Zusammenhänge analysieren sowie konkrete Handlungsempfehlungen für Politik, Verwaltung, Wirtschaft und Betreiber kritischer Infrastrukturen entwickeln. Die gewonnenen Erkenntnisse sollten anschließend in die nationale Cyber-Sicherheitsstrategie einfließen.

Bestehende Strukturen einbinden

Schrödter verwies auf vergleichbare Untersuchungsstellen in der Luft- und Schifffahrt, die Unfälle systematisch aufarbeiten, um künftige Risiken zu reduzieren. Eine entsprechende Institution für den digitalen Raum existiere bislang nicht. Die Einrichtung eines Cyber Incident Review Boards müsse allerdings mit bestehenden und geplanten Strukturen abgestimmt werden. Insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der geplante Cyberdome der Bundesregierung seien dabei einzubeziehen. Entscheidend seien klare Zuständigkeiten und kurze Abstimmungswege.

Schleswig-Holstein baut Cybersicherheit aus

Zugleich stellte Schrödter die Maßnahmen vor, mit denen Schleswig-Holstein seine digitale Widerstandsfähigkeit stärken will. Das Land ist seit Oktober 2025 NIS-2-notifiziert und hat eine neue Informationssicherheitsleitlinie eingeführt. Darüber hinaus wurden Eckpunkte einer umfassenden Informations- und Cybersicherheitsstrategie beschlossen. Das CERT Nord wurde zu einem Computer Security Incident Response Team (CSIRT) weiterentwickelt, das Sicherheitsmeldungen von Land und Kommunen gebündelt bearbeitet. Bei kritischen Sicherheitsvorfällen unterstützen spezialisierte Teams die betroffenen Behörden direkt vor Ort. Ergänzend baut das Land sein Schwachstellenmanagement und die Angriffserkennung auf Endgeräten aus.

Weitere Maßnahmen umfassen den Einsatz souveräner Open-Source-Lösungen, die Trennung kritischer IT-Systeme sowie den Aufbau eines unabhängigen Notfall-Arbeitsplatzes mit eigener Kommunikations- und IT-Infrastruktur. Land und Kommunen arbeiten zudem an einer gemeinsamen Sicherheitsarchitektur.

Erkenntnisse aus Angriffen besser nutzen

Neben technischen Schutzmaßnahmen setzt Schleswig-Holstein auf eine engere Zusammenarbeit mit dem BSI, der Innenministerkonferenz und weiteren Sicherheitsbehörden. Gemeinsame Lagebilder und abgestimmte Reaktionsmechanismen sollen die Widerstandsfähigkeit staatlicher IT-Infrastrukturen erhöhen.

Ein nationales Cyber Incident Review Board könnte diese Zusammenarbeit nach Schrödters Vorstellungen ergänzen und dazu beitragen, Erkenntnisse aus schwerwiegenden Angriffen über einzelne Organisationen und Verwaltungsebenen hinaus nutzbar zu machen. Ob und in welcher Form ein solches Gremium eingerichtet werden sollte, müsse nun geprüft werden.

(al)

Stichwörter: Politik, Cybersicherheit, Schleswig-Holstein