SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 20/4719**
20. Wahlperiode 18. August 2026

Antrag

der Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN

Lehren aus Cyberangriffen systematisch nutzen – Einrichtung eines nationalen Cyber Incident Review Boards prüfen

Der Landtag wolle beschließen:

Cyberangriffe auf Unternehmen, öffentliche Einrichtungen und kritische Infrastrukturen nehmen kontinuierlich zu und verursachen erhebliche wirtschaftliche und gesellschaftliche Schäden. Die wirksame Prävention und Bewältigung von Cybervorfällen setzt voraus, dass aus besonders schwerwiegenden Angriffen systematisch Lehren gezogen und diese Erkenntnisse allen relevanten Akteuren zugänglich gemacht werden.

Die australische Regierung hat hierfür ein unabhängiges Cyber Incident Review Board eingerichtet. Dieses analysiert bedeutende Cybervorfälle, identifiziert strukturelle Schwachstellen und entwickelt Empfehlungen zur Verbesserung der Cybersicherheit, ohne dabei den Fokus auf individuelle Schuldzuweisungen zu legen. Ziel ist ein kontinuierlicher Lernprozess zur Stärkung der Resilienz von Staat, Wirtschaft und Gesellschaft.

Auch auf europäischer Ebene wird mit der Cybersolidaritätsverordnung der Ausbau gemeinsamer Fähigkeiten zur Erkennung, Bewältigung und Nachbereitung erheblicher Cybervorfälle vorangetrieben. Der strukturierte Austausch von Erfahrungen und Erkenntnissen aus Cybervorfällen gewinnt damit zunehmend an Bedeutung.

Der Landtag bittet die Landesregierung,

- sich gegenüber der Bundesregierung sowie im Bundesrat für die Prüfung und Schaffung eines unabhängigen nationalen Cyber Incident Review Boards einzusetzen und dieses im Kontext des Cyberdomes anzusiedeln;
- darauf hinzuwirken, dass ein solches Gremium schwerwiegende Cybervorfälle mit gesamtstaatlicher Relevanz systematisch untersucht, Ursachen und Wirkzusammenhänge analysiert sowie Handlungsempfehlungen für Politik, Verwaltung, Wirtschaft und Betreiber kritischer Infrastrukturen entwickelt;
- sich dafür einzusetzen, dass die Arbeit eines solchen Gremiums nach dem Vorbild bestehender Untersuchungsstellen in anderen sicherheitsrelevanten Bereichen unabhängig, transparent und vorrangig lernorientiert erfolgt und nicht der individuellen Schuldzuweisung dient;
- darauf hinzuwirken, dass Erkenntnisse aus der Arbeit eines solchen Gremiums in die nationale Cybersicherheitsstrategie sowie in die Umsetzung europäischer Vorgaben, insbesondere der Cybersolidaritätsverordnung, einfließen;
- zu prüfen, wie die im Land vorhandenen Kompetenzen aus Wissenschaft, Wirtschaft, Verwaltung und Cybersicherheitsbehörden in die Arbeit eines solchen Gremiums eingebunden werden können.

Begründung:

Die digitale Transformation von Staat, Wirtschaft und Gesellschaft führt zu einer zunehmenden Abhängigkeit von funktionierenden und sicheren Informations- und Kommunikationstechnologien. Gleichzeitig steigt die Zahl schwerwiegender Cyberangriffe auf öffentliche Einrichtungen, Unternehmen und Betreiber kritischer Infrastrukturen kontinuierlich an. Ransomware-Angriffe, Datendiebstähle und Angriffe auf digitale Lieferketten verursachen erhebliche wirtschaftliche Schäden und können die Funktionsfähigkeit staatlicher und gesellschaftlicher Strukturen beeinträchtigen.

Die wirksame Stärkung der Cybersicherheit erfordert nicht nur die Abwehr akuter Bedrohungen, sondern auch die systematische Auswertung bereits eingetretener Vorfälle. Während in Bereichen wie Luftfahrt, Schienenverkehr oder Schifffahrt unabhängige Untersuchungsstellen seit langem dazu beitragen, aus Schadensereignissen zu lernen und die Sicherheit des Gesamtsystems zu verbessern, existiert ein vergleichbarer Mechanismus für besonders schwerwiegende Cybervorfälle in Deutschland bislang nicht.

Mit der Einrichtung eines Cyber Incident Review Board hat Australien einen innovativen Ansatz gewählt, um aus bedeutenden Cybervorfällen strukturiert Erkenntnisse zu gewinnen. Das Gremium untersucht ausgewählte Vorfälle unabhängig und mit dem Ziel, systemische Schwachstellen zu identifizieren sowie Empfehlungen zur Verbesserung der Resilienz von Staat, Wirtschaft und Gesellschaft zu entwickeln. Dabei steht ausdrücklich nicht die individuelle

Schuldzuweisung im Vordergrund, sondern die Stärkung der kollektiven Lernfähigkeit und die Vermeidung vergleichbarer Vorfälle in der Zukunft.

Auch auf europäischer Ebene gewinnt dieser Ansatz an Bedeutung. Die Cybersolidaritätsverordnung der Europäischen Union verfolgt das Ziel, die Fähigkeiten der Mitgliedstaaten zur Erkennung, Bewältigung und Nachbereitung erheblicher Cybervorfälle zu stärken sowie den Austausch von Informationen, Erfahrungen und bewährten Verfahren zu fördern. Darüber hinaus leisten das Netzwerk der Computer Security Incident Response Teams (CSIRTs Network) sowie weitere europäische Kooperationsstrukturen wichtige Beiträge zur operativen Zusammenarbeit. Ein nationales Cyber Incident Review Board könnte diese bestehenden Strukturen sinnvoll ergänzen, indem es die systematische Analyse schwerwiegender Vorfälle und die Ableitung strategischer Handlungsempfehlungen institutionell verankert.

Vor diesem Hintergrund erscheint es sinnvoll, dass sich die Landesregierung gegenüber der Bundesregierung und im Bundesrat für die Prüfung und Schaffung eines unabhängigen nationalen Cyber Incident Review Boards einsetzt. Ziel sollte es sein, die Resilienz Deutschlands gegenüber Cyberbedrohungen durch einen institutionellen Lernprozess nachhaltig zu stärken und Erkenntnisse aus schwerwiegenden Cybervorfällen systematisch für die Verbesserung der Cybersicherheit nutzbar zu machen.

Uta Wentzel
und Fraktion

Sebastian Bonau
und Fraktion