



Presseinformation

Nr. 26.309

07.10.2026

Es gilt das gesprochene Wort!

TOP 13 – Lehren aus Cyberangriffen systematisch nutzen – Einrichtung eines nationalen Cyber Incident Review Boards prüfen

Dazu sagt der digitalpolitische Sprecher der Landtagsfraktion von Bündnis 90/Die Grünen, **Sebastian Bonau**:

Jeder Cyberangriff liefert Erkenntnisse, die wir nutzen sollten

Sehr geehrte Frau Präsidentin,
liebe Kolleg*innen,

wenn im deutschen Luftraum ein schwerer Unfall passiert, beginnt nach der Bewältigung der akuten Lage eine zweite, ebenso wichtige Arbeit: Der Unfall wird aufgearbeitet. Was ist passiert? Was ist unmittelbar davor geschehen? Welche Sicherheitsmechanismen haben funktioniert und welche nicht? Und vor allem: Was müssen wir verändern, damit sich ein solcher Unfall möglichst nicht wiederholt?

Vergleichbare Untersuchungsstellen kennen wir auch aus dem Schienen- und Schiffsverkehr. Und ich finde: Was bei schweren Unfällen selbstverständlich ist, sollte auch bei schwerwiegenden Cybervorfällen selbstverständlich sein.

Denn Deutschland und Europa stehen im digitalen Fadenkreuz. Cyberangriffe sind längst keine abstrakte Gefahr mehr. Staatliche Akteure, organisierte Cyberkriminelle und professionell arbeitende Hackergruppen versuchen, Daten zu stehlen, Verwaltungen lahmzulegen und unsere digitale Infrastruktur anzugreifen.

Wir haben erlebt, was das konkret bedeuten kann. 2021 legte ein Ransomware-Angriff die Verwaltung des Landkreises Anhalt-Bitterfeld weitgehend lahm. Erstmals in Deutschland wurde wegen eines Cyberangriffs der Katastrophenfall ausgerufen. Und erst in diesem Sommer wurden bei einem Cyberangriff auf die Berliner Verwaltung in erheblichem Umfang Daten entwendet und anschließend veröffentlicht. Wir müssen davon ausgehen: Solche Vorfälle werden nicht die letzten sein. Deshalb reicht es nicht, einen Angriff abzuwehren, die Systeme wiederherzustellen und anschließend zur Tagesordnung überzugehen. Wir müssen aus diesen Angriffen lernen.

Als Schleswig-Holstein gehen wir bei der Digitalisierung an vielen Stellen einen eigenen Weg. Das wird hier im Haus von einer breiten politischen Einigkeit getragen. Bei der

Cybersicherheit müssen wir aber zugleich den Blick über unsere Landesgrenzen hinaus richten. Denn Cyberangriffe halten sich nicht an Landesgrenzen. Schwachstellen in einem Land können Erkenntnisse liefern, von denen Verwaltungen und Unternehmen in ganz Deutschland profitieren. Genau hier setzt unser Antrag an.

Australien hat mit dem Cyber Incident Review Board ein unabhängiges Gremium geschaffen, das bedeutende Cybervorfälle untersucht, nachdem die unmittelbare Gefahrenabwehr abgeschlossen ist. Das Entscheidende dabei ist der Ansatz: Es geht nicht darum, Schuldige zu suchen. Es geht darum, zu verstehen. Was ist passiert? Warum konnte ein Angriff erfolgreich sein? Wie haben Behörden und Unternehmen reagiert? Welche Strukturen haben funktioniert? Und welche Veränderungen sind notwendig, damit der nächste Angriff verhindert oder zumindest seine Folgen begrenzt werden können?

Aus diesen Erkenntnissen entwickelt das australische Board konkrete Empfehlungen für Staat und Wirtschaft. Diesen Ansatz wollen wir auch für Deutschland. Deshalb bitten wir die Landesregierung, sich auf Bundesebene für die Schaffung eines nationalen Cyber Incident Review Boards einzusetzen.

Ein solches Gremium soll schwerwiegende Cybervorfälle mit gesamtstaatlicher Bedeutung unabhängig, transparent und lernorientiert untersuchen und daraus Handlungsempfehlungen für Politik, Verwaltung, Wirtschaft und die Betreiber kritischer Infrastrukturen entwickeln. Damit würden wir zugleich einen Ansatz aufgreifen, den auch Europa verfolgt. Mit der Cybersolidaritätsverordnung wurde auf europäischer Ebene bereits ein Mechanismus geschaffen, mit dem schwerwiegende Cybervorfälle überprüft und bewertet werden können.

Wir wollen diesen Gedanken auf nationaler Ebene weiterführen. Jeder schwere Cyberangriff ist zunächst einmal ein Schaden. Für die Betroffenen, für Unternehmen, für unsere Verwaltungen und im schlimmsten Fall für unsere Kritische Infrastruktur. Aber jeder dieser Angriffe liefert uns auch Erkenntnisse. Erkenntnisse über Schwachstellen. Erkenntnisse über unsere Reaktionsfähigkeit. Erkenntnisse darüber, was wir beim nächsten Mal besser machen können. Diese Erkenntnisse dürfen wir nicht ungenutzt lassen.

Liebe Kolleg*innen,

lassen Sie uns deshalb als Schleswig-Holstein auch hier vorangehen. Lassen Sie uns dafür sorgen, dass wir Cybervorfälle nicht nur bewältigen, sondern systematisch aus ihnen lernen. Und lassen Sie uns damit die digitale Resilienz unseres Landes und Deutschlands nachhaltig stärken.

Ich bitte um Zustimmung zu unserem Antrag.

Vielen Dank.

**Landtagsfraktion
Bündnis 90/Die Grünen Schleswig-Holstein**

Pressesprecherin
Claudia Jacob

Landeshaus

Düsternbrooker Weg 70
24105 Kiel

T 0431 988 1503
M 0172 541 83 53

presse@gruene.ltsh.de
sh-gruene-fraktion.de