

Es gilt das gesprochene Wort!

Hinweis: Diese Rede kann hier als Video abgerufen werden:
<http://www.landtag.ltsh.de/aktuelles/mediathek>

LANDTAGSREDE – 07.Oktober 2026

Kianusch Stender

Bei Cybersicherheit darf Schleswig-Holstein nicht nur nach Berlin zeigen

TOP 13: Lehren aus Cyberangriffen systematisch nutzen – Einrichtung eines nationalen Cyber Incident Review Boards prüfen (Drs. 20/4719)

Ich möchte einmal mit einem Beispiel aus meinem Wahlkreis beginnen: Die Mürwiker in Flensburg sind ein großer sozialer Dienstleister mit Arbeits- und Wohnangeboten für Menschen mit Behinderung. 2021 wurden sie Opfer eines massiven Ransomware-Angriffs. Plötzlich ging praktisch nichts mehr: Daten und Systeme waren nicht mehr verfügbar. Die Angreifer forderten 2,3 Millionen Euro Lösegeld. Die Mürwiker haben sich richtigerweise entschieden, nicht zu zahlen. Aber damit war das Problem natürlich nicht gelöst. Die Wiederherstellung hat am Ende ungefähr genauso viel gekostet wie das geforderte Lösegeld. Die Folgen dieses Angriffs wirken bis heute nach.

Ich will, dass wir alles in unserer Macht Stehende tun, um Unternehmen wie diesen zu helfen. Ja Minister Madsen, ich bin auch nicht für eine Vollkasko-Mentalität, wo der Staat alles abwendet, was irgendwie an äußeren Einflüssen auf Unternehmen einprasselt. Aber das hier ist etwas anderes: Es gibt eine geopolitisch so angespannte Lage, der ein mittelständisches Unternehmen nicht alleine begegnen kann. Cyberangriffe in Deutschland werden in der Regel aus dem außereuropäischen Ausland heraus gelenkt und nehmen Ausmaße an, die unserer Volkswirtschaft zu einem relevanten Teil schaden. Und da müssen wir als Staat uns einmischen und unterstützen.

Deshalb ist der Ansatz dieses Antrags richtig: Wir müssen Cyberangriffe nicht nur abwehren. Wir müssen aus ihnen lernen. Genau deshalb halte ich die Einrichtung eines Review Boards auf Bundesebene für sinnvoll. Es fehlt in Ihrem Antrag aber die Landesebene in Gänze – und das hier im Landtag. Auch wir können und müssen uns stärker engagieren in der Prävention von Cyberangriffen. Deshalb bitte ich darum, dass wir den Antrag in den Innen- und Rechtsausschuss und mitberatend in den Wirtschafts- und Digitalisierungsausschuss überweisen und dort nochmal im Rahmen einer Anhörung darüber sprechen, inwieweit wir selbst weiter tätig werden sollten.

Das Beispiel der Mürwiker zeigt aber noch ein zweites Problem: Wer hilft einer solchen Einrichtung eigentlich dabei, sich für den nächsten Angriff besser aufzustellen? Das Land hat zwar Fördermöglichkeiten für Investitionen in Digitalisierung und IT-Sicherheit. Aber die Mürwiker fallen aufgrund ihrer Beschäftigtenzahl aus dieser Förderung heraus. Sie sind also zu groß für den Fördertopf – aber gleichzeitig natürlich kein Großkonzern, der mal eben Millionenbeträge für zusätzliche Cybersicherheit aus der Portokasse bezahlen kann.

Genau solche Fälle zeigen, dass wir eine Förderlücke haben. Unser Ziel muss sein, dass sich solche Organisationen so resilient aufstellen können, dass ein erfolgreicher Angriff nicht den gesamten Betrieb über Monate oder sogar Jahre zurückwirft.

Und die Mürwiker sind kein Einzelfall. Ich habe die Landesregierung in mehreren Kleinen Anfragen gefragt, wie groß das Problem bei uns eigentlich ist. Allein bei Ransomware-Angriffen auf privatwirtschaftliche Unternehmen waren der Polizei 2024 27 Fälle und 2025 29 Fälle bekannt. Gleichzeitig sagt die Landesregierung selbst ausdrücklich, dass von einem relevanten Dunkelfeld auszugehen ist. Unternehmen zeigen solche Fälle regelmäßig nicht an, um nicht zugeben zu müssen, dass es Sicherheitslücken gibt.

Und auch die finanziellen Dimensionen sind erheblich. Allein in den dem LKA bekannten Fällen wurden 2024 Lösegeldforderungen von insgesamt rund 546.000 Euro gestellt. 2025 waren es sogar rund 608.000 Euro. Zusammen also mehr als 1,1 Millionen Euro – und auch das ist nur das Hellfeld. Die Landesregierung berichtet selbst davon, dass Unternehmen Lösegeld zahlen, ohne dass dies dem LKA bekannt wird.

Wir haben durchaus Strukturen, die funktionieren. Zum Beispiel die Zentrale Ansprechstelle Cybercrime beim LKA. Und deren Zahlen zeigen auch, dass sie gebraucht wird: 2024 gab es 297 Kontaktaufnahmen durch Firmen, Behörden, Vereine und andere Institutionen, 2025 waren es 304. Aber wir haben daneben beispielsweise auch den Servicepoint Cybersecurity, der Unternehmen mit Beratung und Vernetzung unterstützen soll. Und wenn man sich dessen Internetauftritt heute anschaut, bekommt man nicht unbedingt den Eindruck, dass wir dort auf der Höhe der Zeit sind: Im Impressum wird noch der ehemalige Geschäftsführer der WTSH als Verantwortlicher genannt. Der Copyright-Hinweis endet 2022. Und bei den vergangenen Veranstaltungen findet sich auf der Seite aktuell gerade einmal eine einzige Veranstaltung.

Das passt für mich nicht zu einer Bedrohungslage, von der wir gleichzeitig sagen, dass sie immer größer wird.

Andere Länder sind da weiter. NRW hat beispielsweise ein eigenes Kompetenzzentrum für Cybersicherheit in der Wirtschaft aufgebaut, das Unternehmen bei Prävention und

Cyberresilienz unterstützt. Deshalb sollten wir heute nicht nur nach Berlin zeigen. Wir sollten diesen Antrag im Ausschuss nutzen, um uns auch unsere eigenen Strukturen genauer anzusehen. Denn auch wir in Schleswig-Holstein können noch einiges besser machen.