Presseinformation

Es gilt das gesprochene Wort!

TOP 42 – Bericht über die Cybersicherheit unserer Infrastruktur

Dazu sagt der innen- und rechtspolitische Sprecher der Landtagsfraktion von Bündnis 90/Die Grünen,

Jan Kürschner:

Landtagsfraktion Schleswig-Holstein

Pressesprecherin
Claudia Jacob

Landeshaus
Düsternbrooker Weg 70
24105 Kiel

Zentrale: 0431 / 988 – 1500
Durchwahl: 0431 / 988 - 1503
Mobil: 0172 / 541 83 53

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

Nr. 023.24 / 24.01.2024

Wir dürfen nicht warten, bis es zu spät ist

Sehr geehrte Frau Präsidentin,
sehr geehrte Abgeordnete,

am Tag der russischen Invasion in die Ukraine gab es ebenfalls einen russischen IT-Angriff auf den Satellitennetzbetreiber VIASAT in den USA, wodurch dessen Satellitennetzwerk lahmgelegt wurde. Als direkte Folge davon gerieten mehrere Tausend Windkraftanlagen außer Kontrolle. Dieser Vorgang zeigt schmerzhaft: Unsere kritischen Infrastrukturen, nicht nur die Windkraftanlagen, sondern bspw. auch die Kritis-Infrastruktur im Meer, Stichwort Northstream oder auch die großen Datenkabel vor Sylt, die zentral für den transatlantischen Datenaustausch sind, sind extrem vulnerabel.

IT-Angriffe stellen längst ein Mittel in beinahe jeder zwischenstaatlichen Auseinandersetzung dar. Der Beginn des Angriffskriegs von Russland auf die Ukraine jährt sich bald zum zweiten Mal. Aktuell verzeichnet Deutschland viel mehr Cyberangriffe als vor dem Ukrainekrieg, die Zahl der registrierten Fälle hat sich im Jahr 2022 gegenüber dem Vorjahr um 27 Prozent gesteigert. Niemand soll sich der Illusion hingeben, es würde künftig weniger werden.

Wir müssen uns diesen sicherheitspolitischen Herausforderungen endlich mit aller Entschlossenheit gemeinsam stellen – übrigens auch als Parlament – zumindest, wenn wir nicht wollen, dass es uns ergeht wie dem Deutschen Bundestag 2015, der sich einem wochenlangen IT-Angriff Russlands ausgesetzt sah.

Wir wissen, dass die kritischen Infrastrukturen, die analogen und digitalen Lebensadern unserer Demokratie und unserer Wirtschaft, im Fokus russischer Angriffe stehen. Wer die Anhörung der Spitzen der drei Nachrichtendienste des Bundes neulich verfolgt hat, weiß: Auch die Warnungen unserer Sicherheitsbehörden und Nachrichtendienste könnten eindringlicher nicht sein.

Diesen großen sicherheitspolitischen Herausforderungen, nicht nur mit Blick auf Russland, sondern bspw. genauso mit Blick auf Technologieanbieter aus anderen autoritären Staaten, die in unsere hochsensiblen Telekommunikationsnetze drängen, gilt es rechtsstaatlich sehr entschlossen zu begegnen.

Meine Damen und Herren,
wir sind bei diesem Thema zu langsam. Überhaupt habe ich den Eindruck, dass der Krieg und seine Folgen von großen Teilen der Gesellschaft weitgehend ignoriert wird. Muss es immer erst hier knallen, bis richtig was passiert?

Wie nah und real die Gefahr von IT-Angriffen auch bei uns in Schleswig-Holstein ist, zeigt auch die Attacke auf die Stadtwerke Neumünster im letzten August: keine E-Mails, kein Telefon, kein Zugriff auf Kundendaten, keine Vertragsabschlüsse, Schwierigkeiten im Zahlungsmanagement, monatelange Nachwehen. Dieser Vorfall stellte nicht nur ein Ärgernis für die Bürger*innen dar, sondern hatte weitreichende und geschäftsschädigende Auswirkungen für die Stadtwerke Neumünster. Die durch IT-Angriffe verursachte Schäden für die Wirtschaft gehen auch laut des jüngsten BSI-Jahresberichts in die Milliarden!

Über Monate waren immer wieder auch die öffentlichen Verwaltungen zahlreicher Kommunen gänzlich unerreichbar – ein Desaster, gerade mit Blick auf die Bereitstellung von E-Government-Angeboten, die wir ja zu Recht massiv ausbauen.

Es gilt dringend, schnellstmöglich aufzuholen. Hier ist der Bund in der Verantwortung, wir als Land, Stichwort Gefahrenabwehr, sind es aber mindestens genauso.

Die Bundesregierung wird nun hoffentlich bald das sogenannte Kritis-Dachgesetz vorlegen, das einen ganzheitlichen, also sowohl auf physische als auch digitale Infrastrukturen abzielenden Schutz sicherstellt. Für uns Grüne ist es nicht nachzuvollziehen, dass dieses Gesetz noch nicht das Licht der Welt erblickt hat. Das ist fatal, denn der physische Schutz lässt sich von der Cyberabwehr nicht trennen. Beispiel: Die sabotierte Pipeline ist aktuell noch nicht als kritische Infrastruktur eingestuft.

Aber auch wir müssen uns unserer Verantwortung stellen und uns frühzeitig, also jetzt, auf die neue Situation einstellen, mit allen verantwortlichen Behörden frühzeitig in den Austausch treten und entsprechende Kontaktstellen im Land einrichten.

Umso wichtiger ist es, auf die bestehenden Kompetenzen im Land, auf das Landeskriminalamt und den Verfassungsschutz, und deren kostenlose Beratungsangebote hinzuweisen. Man kann den Verantwortlichen in den Unternehmen nur raten, dieses Angebot auch tatsächlich vorher in Anspruch zu nehmen, nicht erst, nachdem etwas passiert ist!

Vielen Dank!

****