Presseinformation

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. 024.19 / 24.01.2019

Es gilt das gesprochene Wort!

TOP 25 – Mündlicher Bericht Cybersicherheit

Dazu sagt der netzpolitische Sprecher der Landtagsfraktion von Bündnis 90/Die Grünen,

Rasmus Andresen:

Hacks haben nicht nur persönliche Konsequenzen, sondern können auch unsere Demokratie gefährden

Sehr geehrte Damen und Herren,

vielen Dank für den Bericht, Herr Minister.

Private Handynummern, Chatverläufe mit den engsten Familienmitgliedern, Rechnungen, Geschäftsgeheimnisse, Ausweisdokumente und private Fotos. Hacks und Leaks sind in Deutschland Alltag. Angesichts von Collection #1 und 773 Millionen betroffener Emailadressen ist der Doxxing-Skandal vom Anfang des Jahres schon fast wieder Schnee von gestern. Da aber „Personen des öffentlichen Lebens“ betroffen waren, schrie die ganze Medienrepublik lautstark auf.

Der ein paar Tage später bekannt gewordene Datenklau beim Kreis Schleswig-Flensburg oder die Nachricht, dass Unternehmen bei uns in Schleswig-Holstein zum Teil Lösegeld zahlen, damit ihre Daten nicht geleaked werden, waren nur am Rande Thema.

Wir brauchen eine grundsätzliche Debatte zum Thema Datensicherheit. Hacks haben nicht nur persönliche Konsequenzen, sondern können auch unsere Demokratie gefährden. Menschen, die sich engagieren, werden eingeschüchtert und Wahlen beeinflusst. Bund, Land und Kommunen müssen die Daten schützen, die uns anvertraut werden. Und es müssen Strukturen geschaffen werden, die die Cybersicherheit von uns allen massiv erhöht.

Für IT Sicherheit gibt es nicht eine Lösung, sondern wir müssen mehrere Maßnahmen ergreifen. Statt Feuerlöscher brauchen wir besseren Brandschutz. Wir Grüne haben da-

für immer wieder Vorschläge vorgelegt. Die Bundesregierung hat diese regelmäßig abgelehnt.

Aber als wäre das nicht genug, der Staat handelt grob fahrlässig, wenn er IT-Sicherheitslücken durch die Sicherheitsbehörden bewusst offen hält, um selbst leichteren Zugang zu vertraulicher Kommunikation zu bekommen. Auch Gegenangriffe, so genannte Hack-Backs, oder Massenüberwachungsinstrumente wie die Vorratsdatenspeicherung führen nicht zu mehr, sondern zu weniger Sicherheit.

Was hingegen hilft, sind gut ausgestattete Behörden und gemeinsame Datenschutz- und IT-Sicherheitsstandards. Bei Dataport wird gute Arbeit geleistet und auch unsere IT-Sicherheit im Landeshaus scheint zu funktionieren. Allerdings, wenn selbst das Sicherheitsnetz des Bundestages angegriffen wird, sollten auch wir immer wieder unseres prüfen. Die Meldungen, dass von den aktuellen Datenleaks überdurchschnittlich viele Politiker*innen aus Schleswig-Holstein betroffen sind, sollte uns erst Recht zu denken geben.

Es geht aber nicht ausschließlich um Regierungs- und Abgeordnetenkommunikation. Auch die IT-Sicherheit von Polizei und Justiz muss immer wieder überprüft werden. In der Kommunikation mit öffentlichen Behörden muss verschlüsselt kommuniziert werden können. Land, Behörden und Kommunen müssen hier Vorreiter werden. Statt Abhängigkeit von großen Softwarekonzernen, brauchen wir mehr Open Source. Es ist gut, dass wir letztes Jahr die Landesregierung beauftragt haben eine Umstellung der Landes-IT auf Open Source voranzutreiben.

Aber auch jede*r einzelne muss privat und am Arbeitsplatz mehr für die eigene IT-Sicherheit tun. Wer dasselbe Passwort seit zehn Jahren und für mehrere Geräte verwendet, muss sich nicht wundern, wenn sensible Daten in der Öffentlichkeit landen.

2018 war ein entscheidendes Jahr für den Datenschutz. Die Frist zur Umsetzung der Vorgaben des IT-Planungsrats ist abgelaufen, die Datenschutzgrundverordnung in Kraft getreten und mit ihr zahlreiche Verbesserungen im Bereich Datenschutz. Wir müssen die Umsetzung dieser Bestimmungen weiter vorantreiben. Beauftragte für Informationssicherheit, IT-Sicherheitslinien, Schulungen und Fortbildung, die Umsetzung der Empfehlung für einen IT-Grundschutz des BSI, zwei-Faktor Authentifizierung, um nur einige Beispiele zu nennen.

Im letzten Jahr ist viel über die Datenschutzgrundverordnung geschimpft worden. Und ja, vieles daran ist lästig. Aber gemeinsame Regeln für Datenschutz und IT-Sicherheit sind unerlässlich. Wir brauchen diese gemeinsamen Regeln in der EU. Beispielsweise durch die ePrivacy-Verordnung, die sicherstellen soll, dass unsere Onlinekommunikation nicht einfach von Digitalkonzernen oder Staaten überwacht werden kann.

Wir müssen, aber auch dafür sorgen, dass IT-Sicherheit vor Ort gelebt wird. Mit Jan Philipp Albrecht haben wir für diese Aufgaben genau den richtigen Minister.

Vielen Dank.

***