LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/5056**

12.02.2019

Antrag

der Fraktion BÜNDNIS 90/DIE GRÜNEN

IT-Sicherheit in NRW stärken – Freiheit sichern

I. Ausgangslage

Das neue Jahr 2019 bescherte der Öffentlichkeit die Nachricht von einem weiteren groß angelegten und gezielten Hacking- und Doxing-Skandal, der sich im Dezember des Vorjahres ereignete. Durch ihn wurden die zuvor geklauten Daten von rund 1.000 Personen des öffentlichen Lebens in sozialen Netzwerken veröffentlicht. Neben privaten Telefonnummern, Kontodaten, Rechnungen und privaten Fotos wurden auch Chatverläufe zum Beispiel mit Familienangehörigen öffentlich gemacht. Ziel der Angriffe und Veröffentlichungen war es, die Betroffenen bloßzustellen und einzuschüchtern.

Das Netzwerk der Bundesregierung registriert täglich Hunderte Angriffe. Gleiches gilt für Mittelständler, Konzerne, Verbände und selbst Einzelpersonen werden täglich Opfer von Hackerangriffen. Der jüngste Doxingfall größeren Ausmaßes von Dezember 2018 ist allerdings keine neue Erscheinung. Er ereignete sich, nachdem in der Bundesrepublik und in NRW bereits mehrere gravierende Angriffe registriert worden waren: Im Mai 2017 wurde der Einsatz der Ransomware „WannaCry“ bekannt. Sie sorgte dafür, dass ca. 230.000 Computer von Unternehmen, Einrichtungen und von Verbraucherinnen und Verbrauchern in ca. 150 Ländern verschlüsselt wurden und erst gegen Zahlung eines „Lösegeldes“ in der Kryptowährung Bitcoin entschlüsselt wurden. Anfang 2018 wurde bekannt, dass das IT-Netz der Bundesregierung von Unbefugten vermutlich über ein Jahr lang infiltriert und ausgespäht wurde – mit bislang unbekannten Folgen für die Sicherheit der Bundesrepublik.

Der Fall von „WannaCry“ zeigt, dass strategisch eingesetzte Angriffe dieser Art einen flächendeckenden Effekt und schlimmstenfalls verheerende Konsequenzen haben können und dass IT- und Datensicherheit ganz konkret dem Schutz elementarer Rechte der Bürgerinnen und Bürger in Nordrhein-Westfalen und andernorts dient – wie etwa dem Leben oder der körperliche Unversehrtheit. Von „WannaCry“ waren u.a. Einrichtungen betroffen, die der kritischen Infrastruktur zuzurechnen sind. In Großbritannien etwa waren in Krankenhäuser Magnetresonanztomographie-Apparaturen und Kühlschränke für Blutkonserven betroffen. In Spanien war ein Telekommunikationsunternehmen Ziel der Schadsoftware. Ebenso denkbar wären Angriffe auf Einrichtungen der Strom- oder Wasserversorgung mit gravierenden Folgen für die Bevölkerung.

Datum des Originals: 12.02.2019/Ausgegeben: 12.02.2019

Der jüngste Hacking- und Doxing-Skandal zeigt zwei weitere Gefahrenaspekte: Zum einen die Gefahr der Verletzung von Persönlichkeitsrechten von Bürgerinnen und Bürgern oder der rechtswidrigen Veröffentlichung wichtiger, unter Umständen vertraulicher Informationen von Wirtschaft oder der öffentlichen Verwaltung. Zum anderen offenbart der Skandal Gefahren für unsere Demokratie: Durch die Veröffentlichung privater Daten oder privater Korrespondenz sollten Personen des öffentlichen Lebens und Politikerinnen und Politiker gezielt unter Druck gesetzt oder der Lächerlichkeit preisgeben werden. Dies kann zu einem veränderten Kommunikationsverhalten von Abgeordneten führen und die freie Kommunikation von Mandatsträgerinnen und Mandatsträgern beeinträchtigen.

Diese Gefahren lassen sich nur durch ein hohes Maß an IT- und Datensicherheit eindämmen. IT- und Datensicherheit werden aus dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) abgeleitet und haben damit Verfassungsrang. Sie bedeuten Schutz der Bürgerinnen und Bürger im Netz, Schutz der Wirtschaft und nicht zuletzt Schutz unserer Demokratie. Aus dem IT-Grundrecht folgt daneben eine Pflicht des Staates, diese IT-Sicherheit zu schützen. Dass akuter Handlungsbedarf besteht und die Landesregierung zu schnellen Maßnahmen gezwungen ist, zeigt der jüngste Datenleak-Skandal.

Wer in einer „Digitalisierung-first-Bedenken-second“-Logik den digitalen Bevölkerungsschutz als Bedenkenträgerei abqualifiziert, setzt Bürgerinnen und Bürger, Wirtschaft und die öffentliche Verwaltung erheblichen Gefahren aus. Stattdessen muss die Landesregierung für einen sicheren Umgang mit Daten sensibilisieren bzw. die Angebote ausweiten, für die strenge Einhaltung von IT-Sicherheit werben und in der Landesverwaltung penibel für eine sichere IT-Infrastruktur sorgen.

Dafür müssen auch auf Landesebene Strukturen ausgebaut und neue geschaffen werden, die wirksam helfen, die Cybersicherheit zu erhöhen. Für Einbruchsschutz gibt es seit langem die unter Rot-Grün eingeführte Kampagne der Polizei NRW „Riegel vor! Sicher ist sicherer.“ Jede Polizeibehörde bietet Bürgerinnen und Bürgern ein umfangreiches Beratungs- und Informationsangebot an. Es muss ein vergleichbares Angebot einer umfassenden Präventionsstrategie für Bürgerinnen und Bürger und die Wirtschaft in NRW zum Schutz von Endgeräten, IT-Systemen und Daten vor Angriffen, Datenklau und Datenmissbrauch geschaffen werden.

Dabei können Hochschulen und Forschungseinrichtungen helfen. NRW ist eines der führenden Bundesländer in Sachen IT-Sicherheit und belegt in der modernen IT-Sicherheitsforschung einen der weltweiten Spitzenplätze. Forscherinnen und Forscher, zum Beispiel am Horst Görtz Institut der Ruhr-Universität Bochum oder der Westfälischen Hochschule, unterstützen Unternehmen und Institutionen dabei, immer komplexere IT-Systeme sauber zu halten, Sicherheitslücken rechtzeitig zu erkennen und zu schließen, branchenabhängige Risiken richtig einzuschätzen und Maschinen in vernetzten Fabriken gegen Angriffe von außen abzusichern. Hochschulen und Forschungseinrichtungen, wie etwa die TU Dortmund, die RWTH Aachen, die Hochschule Niederrhein, die Universität Bonn oder das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie, entwickeln Konzepte, damit kritische Infrastrukturen wie Krankenhäuser, Kraftwerke oder Telekommunikationsnetze geschützt werden können. Zudem erarbeitet die NRW-Wissenschaft, etwa die Universität Münster, Ansätze, den Datenschutz in Internet und sozialen Netzwerken weiterzuentwickeln sowie Identitätsdiebstahl zu erschweren.

Um die Menschen in jeder Phase ihrer Ausbildung abzuholen, müssen Angebote nicht nur in Schulen und Hochschulen geschaffen und erweitert werden, sondern auch in der beruflichen Bildung und der gemeinwohlorientierten Weiterbildung.

Um die gleichen Schutzstandards wie in der analogen Welt auch in der digitalen Welt zu gewährleisten, brauchen wir ein unabhängiges Beratungsnetzwerk. Informationsangebote müssen gebündelt und ergänzt werden – Betroffene brauchen eine Hotline als Anlaufstelle für erste Hilfe bei gehackten Konten, IT-Systemen und Geräten.

Um Quellentelekommunikationsüberwachung zu ermöglichen, nimmt die Koalition von CDU und FDP bewusst in Kauf, dass die geschützte Vertraulichkeit und Integrität von IT-Systemen verletzt werden können. Die bewusst offengehaltenen Lücken in der Software von IT-Systemen und Verbraucherendgeräten können auch von Kriminellen für ihre illegalen Zwecke genutzt werden. Die Koalition von CDU und FDP setzt damit Bürgerinnen und Bürger, Wirtschaft, Einrichtungen der kritischen Infrastruktur (wie etwa Krankenhäuser, Wasserversorgungseinrichtungen, Energieunternehmen pp.), die eigene Verwaltung und paradoxerweise auch die Sicherheitsbehörden selbst einem unkalkulierbaren Sicherheitsrisiko aus. Da bisher keine technisch und verfassungsrechtlich sichere Spähsoftware existiert, muss die Befugnis zur Quellen-Telekommunikationsüberwachung aus dem Polizeigesetz gestrichen werden.

II. Feststellungen

Der Landtag stellt fest,

1. das Internet soll ein freier digitaler Raum bleiben, den die Menschen sicher zur Kommunikation, zur Information, zur Speicherung von Daten, für ihre berufliche Arbeit, für private Zwecke – kurz: zu ihrer persönlichen Entfaltung – nutzen können.

2. IT-Sicherheit und die Sicherheit von Daten auf Endgeräten, in IT-Systemen und beim Surfen im Netz sind unabdingbare Voraussetzungen für die Funktionsfähigkeit von Demokratie und Rechtsstaat im digitalen Zeitalter.

3. der Staat hat die Aufgabe, die verfassungsrechtlich verankerten Grundrechte zu achten und für den IT-Schutz der Bürgerinnen und Bürger und der Wirtschaft zu sorgen.

III. Beschluss

Der Landtag fordert die Landesregierung auf,

1. in einem unabhängigen Beratungsnetzwerk für Sicherheit in der Informationstechnik alle bestehenden Informations- und Beratungsangebote von öffentlichen Stellen des Landes (z.B. Verbraucherzentrale, Landesbeauftragte für Datenschutz und Informationsfreiheit, Cybercrime-Kompetenzzentrum im LKA, Hochschulen und Forschungseinrichtungen) zu bündeln. Die Landesregierung muss mit eigenen kurz-, mittel- und langfristigen Strategien für neue Angebote zur Aufklärung über Sicherheitsrisiken und Schutzmaßnahmen sowie zur Weiterbildung sorgen und bestehende ergänzen. Es reicht nicht aus, sich hinter Angeboten des BSI zu verstecken.

2. Schulen, Ausbildungsstätten und Hochschulen weiter kurz-, mittel- und langfristig in die Lage zu versetzen und dazu anzuhalten, geeignete Lern- und Sensibilisierungsmaßnahmen effektiv anzubieten und durchzuführen. Es müssen geeignete Informations- und Schulungsangebote für Bürgerinnen und Bürger jedes Alters und angepasst an die jeweiligen IT-Kenntnisse, für kleine und mittlere Unternehmen (KMU), Vereine und Verbände geschaffen werden.

3. eine „Task-Force Internet-Betrug“ als Frühwarnsystem einzurichten. Die Landesregierung muss darüber hinaus eine Erste-Hilfe-Maßnahme für akute Fälle von Hacking, Leaking, Doxing und Internetbetrug für Betroffene schaffen und eine entsprechende Hotline für Bürgerinnen und Bürger sowie für die Wirtschaft bereitstellen.

4. durch Förderprogramme Unternehmensgründungen und Hochschulausgründungen im Bereich der Stärkung der Internetsicherheit zu unterstützen. Hier gibt es viel Bedarf beispielsweise für anwenderfreundliche Verschlüsselungsmöglichkeiten für Kommunikation der Bürgerinnen und Bürger im Alltag und in der Wirtschaft.

5. die im Dezember 2018 durch Schwarz-Gelb eingeführte Befugnis der Quellentelekommunikationsüberwachung aus dem Polizeigesetz zu streichen. Es gibt keine Rechtfertigung dafür, Befugnisse, die unabwägbare Gefahren erzeugen, statt sie zu verhindern, beizubehalten. Da bisher keine technisch und verfassungsrechtlich sichere Spähsoftware existiert, darf der Staat die Risiken für die IT-Sicherheit insgesamt nicht eingehen.

6. bis Ende 2019 einen Gesetzentwurf zur Einbringung in den Bundesrat zu erarbeiten, der Betreiber von großen Internetplattformen dazu verpflichtet, Notfallkontakte bereitzuhalten, damit Nutzerinnen und Nutzer sozialer Netzwerke und Medien umgehend ihre Profile sperren können.

Monika Düker
Arndt Klocke
Verena Schäffer
Mehrdad Mostofizadeh
Matthi Bolte-Richter

und Fraktion