Offener Brief an die Deutsche Bundesregierung

AN:

Die Bundesregierung

IN KOPIE:

Parteizentrale Christlich Demokratische Union Deutschlands
Parteizentrale Christlich-Soziale Union in Bayern
Parteizentrale Sozialdemokratische Partei Deutschlands
Parteizentrale Bündnis 90/ Die Grünen
Parteizentrale Freie Demokratische Partei
Parteizentrale Die Linke

24. Juni 2021

Betreff: Cybersicherheitsstrategie für Deutschland 2021

Sehr geehrte Damen und Herren,

die Bundesregierung plant wenige Monate vor der Bundestagswahl die Verabschiedung der „Cybersicherheitsstrategie für Deutschland 2021“. Diese Strategie ist von enormer Bedeutung, weil sie für Jahre die Weichen stellt, wie der Staat die Cybersicherheit in Deutschland gewährleistet, welche Verpflichtungen auf Unternehmen zukommen und welchen Schutz Bürger:innen erhalten.

Die Unterzeichnenden fordern die Bundesregierung dazu auf, die Verabschiedung der Cybersicherheitsstrategie auf die nächste Legislatur zu vertagen oder zumindest die Ausweitung der Befugnisse für die Sicherheitsbehörden ersatzlos zu streichen. Entscheidende Teile der Strategie sind bereits seit langem innerhalb der Bundesregierung hochumstritten und erhalten massive Kritik durch Vertreter:innen der deutschen Industrie, Wissenschaft und der Zivilgesellschaft.
Sollte die Strategie in ihrer jetzigen Form verabschiedet werden, würde dies auf Jahre eine Cybersicherheitspolitik zementieren, für die es keinen ausreichenden Rückhalt in Wirtschaft und Gesellschaft gibt und deren Maßnahmen wenig Aussicht darauf haben, die IT- und Cybersicherheit in Deutschland zu verbessern. Die Grabenkämpfe um die Ausrichtung der nationalen Cybersicherheitspolitik würden so fortgeführt – zu Lasten der Sicherheit in Deutschland.

Im aktuellen Entwurf der Cybersicherheitsstrategie finden sich eine Reihe an Maßnahmen, die auf Kosten der IT-Sicherheit die Überwachung durch deutsche Sicherheitsbehörden vorantreiben. Dazu gehört zum Beispiel die „Entwicklung technischer und operativer Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation [...]", die Umgehung von sicherer Implementierung starker Verschlüsselung (lies: Hintertüren). Es handelt sich hierbei um eine Maßnahme, gegen die sich die deutsche Industrie, Wissenschaft, Zivilgesellschaft und Politik bereits 2019 in einem Offenen Brief ausgesprochen hat, weil sie ausländischen Nachrichtendiensten und Cyberkriminellen mehr nutzen würde als unseren Sicherheitsbehörden. Hinzu kommen die internationale Signalwirkung und die Auswirkungen für besonders schutzbedürftige Bevölkerungsgruppen, die so ein Vorhaben hätte.

Weiterhin fordert die Cybersicherheitsstrategie unter anderem Befugnisse zur Aktiven Cyberabwehr; eine Maßnahme die so umstritten ist, dass sich sogar die aktuelle Bundesregierung selbst dagegen entschieden hat sie voranzutreiben. Es handelt sich hierbei nicht etwa um eine minimale Befugniserweiterung, sondern um ein Legislativvorhaben, welches sehr wahrscheinlich in einer Grundgesetzänderung münden wird. Es ist damit definitiv ein Vorhaben, über dessen Platz in einer Strategie eine neue Bundesregierung entscheiden sollte.

Ein weiteres Problemfeld wird durch den geplanten Ausbau der Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) verdeutlicht: fehlende Kontroll- und Schutzmaßnahmen. Es gibt seit Jahren eine Kontroverse darüber, ob die „Hackerbehörde" aufgrund ihrer Aufgaben statt eines Ministererlasses mit einem Errichtungsgesetz auf solide rechtliche Grundlage gestellt werden sollte, auch wenn es rechtlich nicht zwingend notwendig ist. Hierzu findet sich in der Strategie kein Wort.

Dieser Punkt zieht sich wie ein roter Faden durch die Strategie. Denn überhaupt fehlt der Strategie die im Koalitionsvertrag versprochene „gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" sowie die wirksame juristische und administrative Kontrolle, bei Ausweitung der Befugnisse der Sicherheitsbehörden. Dass die Bundes- und Landesregierungen statt dem Ausbau der Überwachungsbefugnisse die Kontroll- und Schutzmaßnahmen stärken müssten, zeigte jüngst der Skandal um die Datensammlung von Politiker:innen durch den Verfassungsschutz in Sachsen.

Dies stellt nur eine kleine Auswahl der problematischen Maßnahmen dar, die auf den über 120 Seiten, vor allem im Kapitel 8.3 der Strategie genannt werden.

Erschwerend kommt hinzu, dass die Bundesregierung erstmals Maßnahmen zum Controlling in eine Cybersicherheitsstrategie integrieren möchte. Was an sich eine begrüßenswerte Maßnahme ist, wird dadurch höchst problematisch, dass sich die aktuelle Bundesregierung daran nicht mehr halten muss, sondern es der kommenden Bundesregierung auferlegt. Ein Vertrag zu Lasten Dritter.

Im Namen guter Regierungsführung und effektiver IT- und Cybersicherheitspolitik fordern die Unterzeichnenden die Bundesregierung dazu auf alle Maßnahmen, die den Ausbau von Überwachungsbefugnissen statt der Stärkung der IT-Sicherheit zum Ziel haben ersatzlos zu streichen – im aktuellen Entwurf vom 9. Juni 2021 betrifft das mindestens die Maßnahmen 8.3.1, 8.3.7, 8.3.8, 8.3.9, 8.3.11, 8.3.12, 8.3.14, 8.4.7.

Unterzeichnende Industrie, Organisationen und Verbände

1. Adacor Hosting GmbH
2. AG KRITIS
3. Arbeitskreis Soziale Bewegungen und Polizei des Instituts für Protest- und Bewegungsforschung
4. AStA TU Berlin
5. Bits & Bäume Berlin
6. Boxcryptor
7. cnetz – Verein für Netzpolitik e. V.
8. Chaos Computer Club e. V.
9. Chaos Computer Club Darmstadt e. V.
10. D64 – Zentrum für digitalen Fortschritt e. V.
11. Digitalcourage e.V.
12. Digitale Gesellschaft e.V.
13. eco Verband der Internetwirtschaft e. V.
14. EnjoyVenture Management GmbH
15. European Society for Digital Sovereignty e. V.
16. Feilner-IT
17. FlokiNET Ehf
18. FONAS e.V.
19. Forschungsnetzwerk Sicherheit & Polizei
20. Forum Informatiker:innen für Frieden und gesellschaftliche Verantwortung e. V.
21. Freiburger Institut für angewandte Sozialwissenschaft e. V.
22. Gesellschaft für Informatik e. V.
23. JP Berlin
24. Koordinierungskreis des Netzwerks für Gute Arbeit in der Wissenschaft
25. LOAD e. V. - Verein für liberale Netzpolitik
26. mail.de GmbH
27. mailbox.org
28. mediaTest digital GmbH
29. Netzwerk Datenschutzexpertise
30. Niedersachsen.digital e. V.
31. Reporter ohne Grenzen e. V.
32. SaveTheInternet
33. SerNet GmbH
34. Skymatic GmbH
35. Stiftung Neue Verantwortung e. V.
36. Tutao GmbH
37. Unternehmerverbände Niedersachsen e. V.
38. Wikimedia Deutschland e. V.

Unterzeichenende Vertreter:innen* aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft

1. Prof. Dr. Clemens Arzt, Hochschule für Wirtschaft und Recht Berlin*
2. Alexander Couzens, Informatiker*
3. Prof. Dr. Eric Bodden, Universität Paderborn und Fraunhofer IEM*
4. Karoline Busse, Niedersächsisches Studieninstitut für kommunale Verwaltung e. V.*
5. Dr.-Ing. Tobias Fiebig, Technische Universität Delft*
6. Dr. Frederike von Franqué, wissenschaftliche Beraterin*
7. Dr. Michael Friedewald, Forum Privatheit*
8. Dr.-Ing. Kai Gellert, Bergische Universität Wuppertal*
9. Prof. Dr. Steffen Großmann, Großmann & Köhn Unternehmensberatung*
10. Dr. Daniel Guagnin, VDI/VDE-IT*
11. Dipl.-Ing. Markus Ihle, Abteilungsleiter IT-Sicherheit*
12. Dipl. Wirt.-Inf. Oliver Jaeckel-Bender
13. Prof. Dr. Tibor Jager, Bergische Universität Wuppertal, Lehrstuhl für IT Security and Cryptography*
14. Frank Knischewski, DTS Systeme GmbH* und Vizepräsident von Niedersachsen.digital*
15. Prof. Dr. Anja Lehmann, Hasso-Plattner-Institut*
16. Peter Leppelt, Mitglied des digitalRat.niedersachsen*
17. Michael Lohmann, bevutaIT*
18. Daniel Maslowski, LABOR e. V. Bochum*
19. Staatssekretär für Digitalisierung Stefan Muhle, Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung*
20. Britta Müller, Stadt Wuppertal*
21. Michael Niewöhner, IT Security Consultant*
22. Dipl. Inf. Thomas Reinhold, Informatik, Wissenschaft und Technik für Frieden und Sicherheit, TU Darmstadt*
23. Prof. Dr. Konrad Rieck, Technische Universität Braunschweig*
24. Karsten Rohrbach, Experte für Application Security*
25. Folker Schmidt, c-base*
26. PD Dr. Jan-Felix Schrape, Universität Stuttgart*
27. Prof. Dr. Dominique Schröder, Lehrstuhl für Angewandte Kryptographie, Friedrich-Alexander-Universität Erlangen-Nürnberg*
28. Dr. Matthias Schulze, Stiftung Wissenschaft und Politik*
29. Prof. Peter Schwabe, Max Planck Institute for Security and Privacy*
30. Manuel Soler Hahn, Geraffel*
31. Dr. Dr. Peter Ullrich, TU Berlin, Zentrum Technik und Gesellschaft* und Netzwerk für Gute Arbeit in der Wissenschaft*
32. Prof. Dr. Nils Zurawski, Surveillance Studies Forschungsnetzwerk, Universität Hamburg*

**Zugehörigkeiten dienen ausschließlich der besseren Zuordnung.*