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. Berlin Story Bunker GmbH
6. Bits & Bäume Berlin
7. Boxcryptor
8. Bundesverband IT-Sicherheit e. V. (TeleTrusT)
9. Bundesverband Smart City e. V.
10. cnetz – Verein für Netzpolitik e. V.
11. Chaos Computer Club e. V.
12. Chaos Computer Club Darmstadt e. V.
13. Chaos Computer Club Stuttgart (CCCS e. V.)
14. CYBEReinhardt GmbH
15. Cryptomator
16. D64 – Zentrum für digitalen Fortschritt e. V.
17. DACONIS GmbH.
18. DENIC eG
19. Deutsche Vereinigung für Datenschutz (DVD e.V.)
20. Digitalcourage e.V.
21. Digitale Gesellschaft e.V.
22. eco Verband der Internetwirtschaft e. V.
23. edataconsulting GmbH
24. EnjoyVenture Management GmbH
25. European Society for Digital Sovereignty e. V.
26. Facebook
27. Feilner-IT
28. FlokiNET Ehf
29. Förderverein Informationstechnik und Gesellschaft (Fitug e. V)
30. Forschungsnetzwerk Sicherheit & Polizei
31. Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit (FONAS) e. V.
32. Forum Informatiker:innen für Frieden und gesellschaftliche Verantwortung e. V.
33. Freiburger Institut für angewandte Sozialwissenschaft e. V.
34. Freie Software Freunde e. V.
35. Gesellschaft für Informatik e. V.
36. JP Berlin
37. Koordinierungskreis des Netzwerks für Gute Arbeit in der Wissenschaft
38. lachenmair.info - IT consulting
39. LOAD e. V. - Verein für liberale Netzpolitik
40. mail.de GmbH

41. mailbox.org
42. mediaTest digital GmbH
43. Netzbegrünung e. V.
44. Netzwerk Datenschutzexpertise
45. Niedersachsen.digital e. V.
46. OmniCert Umweltgutachter GmbH
47. Open Source Business Alliance - Bundesverband für digitale Souveränität e.V.
48. p≡p Stiftung
49. Piratenpartei Deutschland
50. Reporter ohne Grenzen e. V.
51. SaveTheInternet
52. SerNet GmbH
53. Stiftung Neue Verantwortung e. V.
54. Tutao GmbH
55. Unternehmerverbände Niedersachsen e. V.
56. Wikimedia Deutschland e. V.
57. WorkSimple GmbH

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

1. Prof. Dr. Clemens Arzt, Hochschule für Wirtschaft und Recht Berlin*
2. Sebastian Aspermaier, IT Systemadministrator*
3. Dr. Volker Baier, NCC Group*
4. Dr.-Ing. Rainer Becker, Product Security Officer*
5. Kirsten Bock, privacyDE*
6. Prof. Dr. Eric Bodden, Universität Paderborn und Fraunhofer IEM*
7. Andreas Bogk, CISO*
8. Karoline Busse, Niedersächsisches Studieninstitut für kommunale Verwaltung e. V.*
9. Anna Cardillo, Rechtsanwältin und Datenschutzexpertin*
10. Alexander Couzens, Informatiker*
11. Dr.-Ing. Daniel Demmler, Universität Hamburg*
12. MdB Anke Domscheit-Berg, netzpolitische Sprecherin der Linksfraktion im Bundestag*
13. Diplom-Informatiker (FH) Jan Fader*
14. Dr.-Ing. Tobias Fiebig, Technische Universität Delft*
15. Prof. Dr. Lars Fischer, HS Bremerhaven*
16. Dr. Friederike von Franqué, wissenschaftliche Beraterin*
17. Dr. Michael Friedewald, Innovationsforscher*
18. Matthias H. Fröhlich, IT-Berater*
19. Dr.-Ing. Kai Gellert, Bergische Universität Wuppertal*
20. Alexander Georgiev, Informatiker*
21. Prof. Dr. Peter Gerwinski, Hochschule Bochum*

22. Daniel Di Giacomo, Geraffel*
23. Christian Gießler, Softwareentwickler*
24. Prof. Dr. Steffen Großmann, Großmann & Köhn Unternehmensberatung*
25. Dr. Daniel Guagnin, VDI/VDE-IT*
26. Stephan Hagel M.Sc., Justus-Liebig-Universität Gießen*
27. Peter Hartmann, CISO*
28. PD Dr. Jessica Heesen, Universität Tübingen*
29. Sven Holter
30. Johannes Hubertz, Senior Systems Engineer, Sysfive.com GmbH*
31. Dipl.-Ing. Markus Ihle, Abteilungsleiter IT-Sicherheit*
32. Dipl. Wirt.-Inf. Oliver Jaeckel-Bender
33. Prof. Dr. Tibor Jager, Bergische Universität Wuppertal, Lehrstuhl für IT Security and Cryptography*
34. Steven Kleemann, Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) Berlin Institute for Safety and Security Research (FÖPS Berlin)*
35. Frank Knischewski, DTS Systeme GmbH* und Vizepräsident von Niedersachsen.digital*
36. Alexander Kulbartsch, Freie Software Freunde e. V.*
37. Verena Lang, Security Risk & Certification Manager*
38. Jens Lange, Stadt Kassel* und IT-SiBe-Forum.de*
39. Prof. Dr. Anja Lehmann, Hasso-Plattner-Institut*
40. Christian Leinen, leinen.it*
41. Peter Leppelt, Mitglied des digitalRat.niedersachsen*
42. Michael Lohmann, bevutaIT*
43. Daniel Maslowski, LABOR e. V. Bochum*
44. Andrej Meuer, Cyber Security Analyst*
45. Maurice Meyer, Bytes and Nibbles*
46. Rainer Miguletz, Energieelektroniker*
47. Cedric Mössner, Dozent für Kryptowährungen, Kryptographie und Programmierung*
48. Staatssekretär für Digitalisierung Stefan Muhle, Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung*
49. Britta Müller, Stadt Wuppertal*
50. Gerd Müller, Softwareentwicklung DATEV eG*
51. Johannes Nehlsen, Universität Würzburg*
52. Michael Niewöhner, IT Security Consultant*
53. Rainer Rehak, Weizenbaum-Institut für die vernetzte Gesellschaft – Das Deutsche Internet-Institut*
54. Dipl. Inf. Thomas Reinhold, Informatik, Wissenschaft und Technik für Frieden und Sicherheit, TU Darmstadt*
55. Prof. Dr. Konrad Rieck, Technische Universität Braunschweig*
56. Markus Matthias Ring, Informatiker*
57. Karsten Rohrbach, Experte für Application Security*
58. Prof. Dr. Tanja Schilling, Albert-Ludwigs Universität Freiburg*
59. Prof. Dr. Sebastian Schinzel, FH Münster*

60. Folker Schmidt, c-base*
61. Claus Scholl, CIO*
62. PD Dr. Jan-Felix Schrape, Universität Stuttgart*
63. Prof. Dr.-Ing. Thomas Schreck, Hochschule München*
64. Prof. Dr. Dominique Schröder, Lehrstuhl für Angewandte Kryptographie, Friedrich-Alexander-Universität Erlangen-Nürnberg*
65. Dr. Matthias Schulze, Stiftung Wissenschaft und Politik*
66. Prof. Dr. Peter Schwabe, Max Planck Institute for Security and Privacy*
67. Sebastian Schwartz, Business Attack* und Wissenschaft und Technik für Frieden und Sicherheit, TU Darmstadt*
68. Snoopy, Snoopy EDV-Beratung*
69. Manuel Soler Hahn, Geraffel*
70. Daniel Stein, Grüne Kassel*
71. Carolin Desirée Toepfer, cdt digital GmbH*
72. Prof. Dr. Peter Trapp, Hochschule München*
73. Peter Turczak, WIWA Wilhelm Wagner GmbH & Co.KG*
74. Leah Ullmann, Software Developerin*
75. Dr. Dr. Peter Ullrich, TU Berlin, Zentrum Technik und Gesellschaft* und Netzwerk für Gute Arbeit in der Wissenschaft*
76. Hanno Wagner, Informationssicherheitsbeauftragter*
77. Dr.-Ing. Sebastian Werner, CTO, Navigance GmbH*
78. Michael Wiesner, Michael Wiesner GmbH*
79. Benedikt Wildenhain M. Sc., Hochschule Bochum*
80. Lilith Wittmann, Informatikerin*
81. Prof. Dr.-Ing. David Zellhöfer, Hochschule für Wirtschaft und Recht Berlin*
82. Prof. Dr. Nils Zurawski, Surveillance Studies Forschungsnetzwerk, Universität Hamburg*

**Zugehörigkeiten dienen ausschließlich der besseren Zuordnung.*