Deutscher Bundestag **Drucksache 19/7705**

19. Wahlperiode 13.02.2019

Antrag

der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Doris Achelwilm, Gökay Akbulut, Simone Barrientos, Birke Bull-Bischoff, Brigitte Freihold, Nicole Gohlke, Dr. André Hahn, Ulla Jelpke, Jan Korte, Amira Mohamed Ali, Niema Movassat, Norbert Müller, Petra Pau, Friedrich Straetmanns, Katrin Werner, Sabine Zimmermann und der Fraktion DIE LINKE.

Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

In vielen Lebensbereichen sorgt die Digitalisierung für erhebliche Erleichterungen. Sie bietet die Chance für gerechte Zugänge, mehr Bürger*innenfreundlichkeit in der Verwaltung, Transparenz und vieles mehr.

Gleichzeitig werden immer größere Mengen an Daten gespeichert – die es zu schützen gilt. Durch das sog. Internet der Dinge (IoT) geraten Gegenstände des täglichen Gebrauchs ebenso in den Fokus potentieller Angreifer*innen wie kritische Infrastrukturen. Ein großer Teil der täglichen Kommunikation findet mittlerweile digital statt.

Bisher hat die Bundesregierung kein schlüssiges Konzept einer einheitlichen Strategie für mehr digitale Sicherheit vorgelegt. Die getroffenen Regelungen, Ausgestaltungen und Maßnahmen des Sicherheitsmanagements unterlaufen einander teilweise selbst. Solange der Widerspruch zwischen der scheinbaren Notwendigkeit des Besitzes von Sicherheitslücken einerseits und dem Willen, IT-Systeme durch die Schließung von Sicherheitslücken zu härten andererseits, nicht aufgelöst ist, werden die eigenen Anstrengungen stets konterkariert.

Für Gefahrenabwehr und Strafverfolgung in den Bereichen Internetkriminalität, IT-gestützter Spionage und Angriffen auf die digitale Infrastruktur sind allein die Polizeibehörden zuständig. Geheimdienste, zu deren Aufgaben Infiltration und Spionage gehören, sind für die Schließung von Sicherheitslücken ungeeignet.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. einen Gesetzentwurf vorzulegen, um das BSI in eine eigenständige Behörde umzuwandeln, die aus der Zuständigkeit des Bundesministeriums des Innern zu entlassen und deren Kernaufgabe die Erhöhung der digitalen Sicherheit für Alle ist;
2. einen Gesetzentwurf vorzulegen, um eine generelle Meldepflicht für Sicherheitslücken einzuführen;

3. die IT-Hersteller in die Pflicht zu nehmen und eine europäische Cyber-Design-Verordnung anzustreben, mit der verbindliche Vorgaben zur Produkthaftung, Produktsicherheit und Produktlebensdauer für mit dem Internet verbundene IT-Systeme etabliert werden;
4. Investitionen in Open-Source-Software und in Open-Source-basierte IT-Sicherheitstechnologien zu erhöhen und in den Behörden bevorzugt einzusetzen;
5. den Einsatz von Staatstrojanern zu unterbinden und Sicherheitslücken wie Backdoors oder Zero-Day-Exploits weder zu nutzen noch anzuschaffen;
6. den Export von Überwachungssoftware zu verbieten;
7. sog. Hackbacks durch staatliche Institutionen auszuschließen und zu ächten;
8. sich im Rahmen ihrer Möglichkeiten dafür einzusetzen, dass regelmäßige Weiterbildung zu Fragen der digitalen Sicherheit durch den verstärkten Einsatz von Zeit und Ressourcen in allen Bereichen des privaten und beruflichen Alltags ermöglicht wird und entsprechend mit den Ländern darauf hinzuwirken;
9. „Digitale Gewalt“ als eigenen Phänomen-Bereich zu erfassen, für den eigene Statistiken geführt werden und besonders geschulte Bereiche in den Strafverfolgungsbehörden und in der Justiz geschaffen werden;
10. mehr Ressourcen für Beratungsstellen für Opfer digitaler Gewalt bereitzustellen;
11. die deutsche Cyber-Sicherheitsstrategie strikt zivil, unter Ausschluss von Militär und Geheimdiensten auszurichten
12. im Rahmen der nationalen Förderprogramme zur Entwicklung von digitalen Sicherheitstechnologien vollständig auf eine strategische Ausrichtung auf „dual-use“-Technologien für die zivile und militärische Nutzung zu verzichten und sich auf EU-Ebene gegen jede Versuche zu wenden, den dual-use-Gedanken in Forschungsprogrammen wie „Horizon 2020“ bzw. „Horizon Europe“ oder in der zukünftigen Tätigkeit des EU-Kompetenzzentrums für Cyber-Sicherheitsforschung (Verordnungsentwurf auf Ratsdokument 5342/19, revidierte Fassung) zu verankern, wie es derzeit in den Gremien des EU-Rats diskutiert wird und
13. die Bundeswehr konsequent auf digitale Sicherheit ihrer eigenen Systeme auszurichten, auf deren Zuverlässigkeit und effektive Sicherung, und auf offensive Cyberfähigkeiten der Bundeswehr ebenso zu verzichten wie auf ihren Inlandseinsatz, auch zum Schutz kritischer Infrastruktur.

Berlin, den 12. Februar 2019

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion