Deutscher Bundestag **Drucksache 19/16049**

19. Wahlperiode 17.12.2019

Antrag

der Abgeordneten Dr. Konstantin von Notz, Katrin Göring-Eckardt, Britta Haßelmann, Katharina Dröge, Tabea Rößner, Dieter Janecek, Agnieszka Brugger, Jürgen Trittin, Dr. Franziska Brantner, Margit Stumpp, Margarete Bause, Gerhard Zickenheiner, Luise Amtsberg, Canan Bayram, Matthias Gastel, Anja Hajduk, Kai Gehring, Katja Keul, Stephan Kühn (Dresden), Christian Kühn (Tübingen), Monika Lazar, Dr. Tobias Lindner, Dr. Irene Mihalic, Filiz Polat, Dr. Manuela Rottmann, Manuel Sarrazin, Stefan Schmidt, Markus Tressel und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Maßnahmen zur Gewährleistung der Integrität digitaler Infrastrukturen, Geräte und Komponenten – Für eine größere digitale Souveränität Deutschlands und Europas

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Der Schutz und die Sicherstellung der Integrität digitaler Infrastrukturen sowie der Privatheit der Kommunikation von Bürgerinnen und Bürgern, Unternehmen und Behörden sind zentrale, nationalstaatliche wie gesamteuropäische Aufgaben.

Ihre Bedeutung wächst angesichts weltweit zunehmender Konflikte um digitale Infrastrukturen und Zugriffe auf Informationen. Die weiter wachsende technische Komplexität und Vielfalt der zum Einsatz kommenden kommerziellen, weltweit produzierten IT-Systeme und der verwendeten, meist nicht auf IT-Sicherheit angelegten Hard- und Software erschwert die Durchsetzung hoher Schutzanforderungen, wo es diese heute schon gibt. Trotz jahrelanger, intensiver Diskussionen und zahlreicher Vorschläge von Sachverständigen, Zivilgesellschaft, Wissenschaft, Unternehmen und Opposition wird die Bundesregierung ihrer sich aus diesen Risiken erwachsenden, direkt auch aus dem Grundgesetz abzuleitenden Schutzverantwortung bis heute noch immer nicht gerecht.

Wie eklatant ihre Versäumnisse sind, zeigt vor allem die seit Monaten anhaltende Diskussion um den Ausbau des 5G-Netzes und die Rolle einzelner Unternehmen als Zulieferer zentraler Komponenten, genauso aber die Diskussionen um extrem unsichere vernetzte Geräte des sogenannten „Internet of Things“ (IoT) sowie um die Rechtswidrigkeit der Speicherung teils hochsensibler Daten in Drittstaaten.

Bis heute gibt es kein funktionierendes System, das die Überprüfbarkeit der Integrität eingesetzter Hard- und Software von unabhängiger Seite gewährleistet, kaum Mindeststandards für den Einsatz von Geräten des „Internet of Things“ (IoT), kein ausreichendes Haftungsregime, keine – mit angemessenen Sanktionsmechanismen ausgestatteten – unabhängigen Aufsichtsstrukturen, keine positiven Anreize wie gute Auditierungs-

juris Lex QS
21052024 ()

und Zertifizierungsverfahren, jedoch etliche ungeklärte Rechtsfragen und Unsicherheiten für Anbieter und Endkunden.

Die jahrelange Untätigkeit der Bundesregierung und die bewusste Nichtregulierung des digitalen Wandels sind verheerend. Die Folge sind weiterhin extrem unsichere digitale Infrastrukturen und Geräte, erhebliche Abhängigkeiten von einigen wenigen Anbietern sowie fehlende Rechtssicherheit für Verbraucher wie Unternehmen. Vertrauen in die Privatheit von Kommunikation sowie in die Integrität digitaler Infrastrukturen, Geräte und Anwendungen kann so nicht entstehen.

Dies ist nicht nur für die IT-Sicherheit von Nachteil. Auch werden große Chancen für den Wirtschaftsstandort vergeben, beispielsweise für die dringend notwendige Stärkung der digitalen Souveränität Deutschlands und Europas.

Während parlamentarische Initiativen zur Erhöhung der IT-Sicherheit und Verringerung digitaler Abhängigkeiten im Deutschen Bundestag seit langem vorliegen (vgl. u. a. Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 21.03.18 „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“ auf BT-Drs. 19/1328), hat die Bundesregierung beinahe jedwede Regulierung vernachlässigt. Das von ihr vor Jahren in Aussicht gestellte IT-Sicherheitsgesetz 2.0 liegt bis heute nicht vor. Gleiches gilt für die angekündigte Änderung des Telekommunikationsgesetzes (TKG). Die Anregungen, die während umfassender Anhörungen zur IT-Sicherheit sowohl des Innenausschusses als auch des Ausschusses „Digitale Agenda“ des Bundestags auch in dieser Wahlperiode unterbreitet wurden, hat man nicht aufgenommen.

Dringend notwendig bleiben u. a. klare Kriterien für den Einsatz von Komponenten und Geräten in digitalen Infrastrukturen, gerade hinsichtlich des Schutzes besonders kritischer Netz-Bereiche, und unabhängige Aufsichtsstrukturen.

Um Gefahrenlagen konkret bewerten zu können, müssen neben technischen, auch rechtliche und weitere sicherheitsrelevante Aspekte für den Schutz von Grund- und Menschenrechten, Demokratie und Rechtsstaatlichkeit in die Prüfung einbezogen werden. So sollten beispielsweise auch die Rechtsstaatlichkeit der Herkunftsstaaten, staatliche Durchgriffsrechte, Produktionsprozesse sowie Verbindungen zwischen beteiligten Unternehmen und Regierungen sowie geostrategische Aspekte bei der Bewertung über die Zulassung eines Anbieters eine Rolle spielen.

Um eine solche Prüfung geordnet durchzuführen, sollte der Prüfvorbehalt in der Investitionsprüfung im Rahmen der Außenwirtschaftsverordnung (AWV) so ausgeweitet werden, dass davon nicht nur Übernahmen kritischer Infrastrukturen, sondern auch die Beteiligung eines Investors bzw. die Kooperation mit einem Unternehmen aus einem Drittstaat im Zusammenhang mit dem Aufbau kritischer Infrastruktur erfasst wird. Auch auf die Notwendigkeit, auch hier gesetzgeberisch tätig zu werden, um auf diesem Weg der Gefahr neuer Abhängigkeiten entschlossen zu begegnen, wurde wiederholt hingewiesen.

Wer Schlüsselkomponenten für digitale Infrastrukturen wie das 5G-Netz liefert, erhält damit weitreichende potentielle Zugänge zu unseren Energienetzen, der Finanzwelt, zu Krankenhäusern, Unternehmen und privaten Wohnungen. Die mit 5G-Netzen realisierbaren Digitalisierungsprojekte der Zukunft schaffen nochmals ungleich höhere Risiken für Angriffe auf IT-Sicherheit und die Privatheit von Kommunikation als dies bislang ohnehin bereits der Fall war. Gerade im Zuge des weiteren Ausbaus digitaler Infrastruktur wird eine Vielzahl von neuen Telekommunikations- und Diensteanbietern neben den klassischen Mobilfunkunternehmen entstehen, die nur Teile der oder Dienste auf der Netzinfrastruktur betreiben und auf kostengünstige Infrastruktur-Anbieter angewiesen sind.

Angesichts einer zunehmend unübersichtlichen Weltlage und der Abschottung einzelner autoritär geführter Staaten, besteht die ernstzunehmende Gefahr, dass diese Staaten Zugänge für Spionage und Sabotage nutzen und bei etwaigen Auseinandersetzungen nicht davor zurückschrecken, auch zivile digitale Infrastrukturen anzugreifen oder

juris Lex QS
21052024 ()

lahmzulegen. Allein auf Vertrauen basierende „No Spy"-Abkommen ohne tatsächliche Sanktionsmechanismen bei Zuwiderhandlungen werden der Problematik nicht gerecht. Auf neue Gefahrenlagen mit potentiell weitreichenden Folgen muss vielmehr sehr viel stärker als bislang von der Bundesregierung reagiert und durch den Gesetzgeber geantwortet werden.

Um IT-Sicherheit zu erhöhen, die digitale Souveränität Deutschlands und Europas zu stärken und auf Gefahren eines weiter zunehmenden staatlichen Protektionismus zu reagieren, ist eine auf vielfältige digitale Ökosysteme angelegte Strategie zu verfolgen, bei der die Resilienz und Redundanz digitaler Infrastrukturen im Mittelpunkt steht und der verstärkte Einsatz von Eigenentwicklungen und freier und offener Software als Ziel verfolgt werden (vgl. Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 08.02.19 „Offen für die Zukunft: Offene Standards für eine gerechte und gemeinwohlorientierte Gestaltung der Digitalisierung" auf BT-Drs. 19/7589).

Werden heute die Weichen im Bereich der IT-Sicherheit richtig gestellt, wird dies mittel- und langfristig auch zu einem Wettbewerbsvorteil für deutsche und europäische Anbieter und einer Stärkung des Wirtschaftsstandorts führen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

Maßnahmen auf nationaler Ebene:

- die Empfehlungen der EU-Kommission zur Sicherheit von 5G-Netzwerken vom 26. März 2019 (C(2019) 2335 final) umzusetzen und das von der EU-Kommission und der EU Agentur für Cybersicherheit für 5G erstellte Risk Assessment vom 9. Oktober 2019 zu berücksichtigen;
- schnellstmöglich eine Änderung des Telekommunikationsgesetzes (TKG) vorzulegen, um zukünftig klar zu definieren, welche Geräte und Komponenten in welchen Bereichen digitaler Infrastrukturen unter welchen konkreten technischen, rechtlichen und sonstigen Voraussetzungen eingesetzt werden dürfen;
- bei der Prüfung potentieller Gefahren für die Integrität digitaler Infrastrukturen und Geräte, gerade in besonders kritischen Bereichen, und in den zeitnah vorzulegenden Kriterien- und Sicherheitskatalog neben technischen, zwingend auch rechtliche und weitere sicherheitsrelevante Aspekte für den Schutz von Demokratie, Menschenrechten und Rechtsstaatlichkeit einzubeziehen und hierbei u. a. auch Produktionsprozesse, rechtlichen Rahmenbedingungen in den jeweiligen Ländern sowie die Vertrauenswürdigkeit berührende Verbindungen von Unternehmen zu Regierungen zu berücksichtigen;
- zu garantieren, dass der Kriterien- und Sicherheitskatalog zukünftig von einer noch zu schaffenden, unabhängigen Stelle fortlaufend dynamisch an Bedürfnisse neuer Technologien und Gefahrenlagen angepasst wird, um eine größtmögliche Transparenz und Nachvollziehbarkeit der Kriterien, die für alle Anbieter und Betreiber gleichermaßen gelten müssen, die Integrität digitaler Infrastrukturen garantieren und Rechtssicherheit für Unternehmen und Verbraucher schaffen;
- den Prüfvorbehalt in der Investitionsprüfung so auszuweiten, dass davon auch die Beteiligung eines Investors bzw. die Kooperation mit einem Unternehmen aus einem Drittstaat im Zusammenhang mit dem Aufbau kritischer Infrastruktur erfasst wird;
- schnellstmöglich ein IT-Sicherheitsgesetzes 2.0 vorzulegen, das unter anderem verpflichtende Mindeststandards für alle vernetzten Geräte des „Internet of Things", andere IT-Geräte sowie Komponenten, nicht nur für kritische Infrastrukturen, definiert, beispielsweise hinsichtlich Mindestvorgaben für die Bereitstellung von Sicherheitsupdates, Regelungen zur Einführung verpflichtender Gütesie-

juris Lex QS
21052024 ()

gel sowie neue Haftungsregelungen und das insgesamt statt wie bisher, rein reaktiv anzusetzen, einen proaktiven Ansatz verfolgt und Investitionen in gute und sichere IT-Sicherheit belohnt statt Opfer von IT-Angriffen nachträglich zusätzlich bestraft (vgl. Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN zum ersten IT-Sicherheitsgesetz vom 10.06.2015 auf BT-Drs. 18/5127);

- die Verantwortung für die IT-Sicherheit aus dem Bundesministerium des Innern, für Bau und Heimat herauszulösen, um den effektiven Grundrechtsschutz zu stärken. Darüber hinaus ist für die Benennung klarer Zuständigkeiten innerhalb der Bundesregierung im Bereich der IT-Sicherheitspolitik zu sorgen, um den Dauerzustand eines Gegeneinanders verschiedener Ministerien zu verhindern und überfällige Grundsatzentscheidungen, beispielsweise zum Thema Verschlüsselung, treffen zu können;
- die Unabhängigstellung zumindest von Teilen des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus dem Verantwortungsbereich des Bundesministeriums des Innern, für Bau und Heimat zu vollziehen, um eine tatsächlich unabhängige Beratung von Bürgerinnen und Bürgern wie Unternehmen sicherzustellen. Darüber hinaus muss die weitere Stärkung unabhängiger Aufsichtsstrukturen wie des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontinuierlich fortgesetzt werden. Kleine und mittlere Unternehmen müssen bei sicherheitstechnischen Herausforderungen durch ein dezentrales und unabhängiges IT-Beratungsnetzwerk unterstützt und Haftungsanreize für alle in der IT-Wertschöpfungskette verantwortlichen Stellen gestärkt werden;
- eine eindeutige ministeriell-koordinierenden Zuständigkeit für „hybride Bedrohungen“ (hybrid threats) zur systematischen Beobachtung potentieller Bedrohungen und Angriffe zu schaffen, insbesondere auf zivile und für das staatliche Wohl relevante digitale Infrastrukturen und zur Erstellung eines an realen Gegebenheiten orientierten Lagebilds. Zur Bewertung einer etwaigen Zurechenbarkeit von Angriffen (Attribution) bedarf es zudem einer eigenständigen, fachlich unabhängigen Organisationseinheit, die nach klaren rechtlichen Vorgaben und Definitionen arbeitet;
- bestehende Haftungsregelungen zu überprüfen und neue gesetzliche Regelungen vorzulegen, um Besonderheiten und Risiken vernetzter IT-Systeme stärker berücksichtigen zu können. Regelungsbedarf besteht beispielsweise bei der Haftung im Falle von Sicherheitsverletzungen wie fahrlässig implementierter oder nicht beseitigter Sicherheitslücken von Herstellern (Produktsicherheitsgesetze, Produkthaftung, Produzentenhaftung, Schutzgesetze), der Verkäufer-Haftung bei Hard- und Software (Gewährleistung, Fehlerbegriff, zugesicherte Eigenschaft, berechtigte Erwartung des Käufers) sowie von Dienstleistern (Sicherheitspflichten und berechtigte Sicherheitserwartungen der Nutzer). Zu verhindern ist, dass häufig komplex gelagerte Streitfälle von geteilter und oftmals nicht konkret feststellbarer Verantwortung von Herstellern und Diensteanbietern einseitig zu Lasten der Nutzerinnen und -nutzer ausgehen;
- insgesamt eine auf vielfältige digitale Ökosysteme, Resilienz und Redundanzen angelegte IT-Strategie zur Verringerung riskanter, einseitiger Abhängigkeiten und zur Stärkung der IT-Sicherheit zu verfolgen, in dem u. a. offene und überprüfbare Standards gestärkt werden. Durch die Überprüfbarkeit der verwendeten Systeme ist freie, quelloffene Software als zentraler Baustein für eine sichere und zukunftsfähige IT-Landschaft, beispielsweise bei der weiteren IT-Konsolidierung, sehr viel stärker zu unterstützen. So sind u. a. Vorgaben bei öffentlichen IT-Beschaffungen anzupassen und eine stärkere Kooperation zwischen Bund und Ländern, beispielsweise über den IT-Planungsrat sicherzustellen. Um die Qualität freier und

juris Lex QS
21052024 ()

offener Software zu verbessern, ist ein Fonds für die Prämierung der Identifizierung, Bekanntmachung und Behebung von Fehlern in offener Software zu schaffen und die Forschungsförderung zu stärken;

- schnellstmöglich eine Cloud-Lösung zu schaffen, auf der Daten unter Beachtung höchster Sicherheitsstandards durchgehend Ende-zu-Ende-verschlüsselt rechtssicher gespeichert werden können, auch, um Alternativen zur rechtswidrigen Speicherung teils hochsensibler Daten auf Servern in Drittstaaten ohne ausreichende Schutzmechanismen zu schaffen;
- in Kooperation mit den Ländern Maßnahmen zu ergreifen, die Bürgerinnen und Bürger in geeigneter Form über bestehende IT-Sicherheitsrisiken aufklären und darauf abzielen, sie zu befähigen, Risiken einzuschätzen, sie bei der Suche nach sicheren Alternativen zu unterstützen und Sicherheitstechniken selbstbestimmt anwenden zu können;

Maßnahmen auf europäischer Ebene:

- die deutsche Ratspräsidentschaft nutzen, um eine an den Werten und Grundrechten der Europäischen Union ausgerichtete, gut koordinierte europäischen Digitalpolitik zu forcieren, die die technologische Souveränität Europas stärkt, Freiheit, Demokratie, Rechtsstaatlichkeit, Offenheit, Überprüfbarkeit, Beteiligung und Innovationsfähigkeit ins Zentrum stellt und sich auch international klar gegen Protektionismus und für eine gemeinwohlorientierte Gestaltung des digitalen Wandels einsetzt;
- Maßnahmen zum Schutz digitaler Infrastrukturen und zur Stärkung von Rechtsstaatlichkeit und Grundrechten zu stärken (vgl. auch Forderungen des Antrags der Fraktion BÜNDNIS 90/DIE GRÜNEN „Für wehrhafte Demokratien in Europa – Rechtsstaatlichkeit und Grundrechte in den Mitgliedsländern der EU stärken“ vom 30.01.2019 auf BT-Drs. 19/7436) sowie Erkenntnisse über die Vertrauenswürdigkeit von Herstellern, Diensteanbietern und Produkten auf EU-Ebene zusammenzuführen, zu bewerten und entsprechende Handlungsempfehlungen und Beschlüsse abzustimmen;
- hierfür bestehende Kooperationsformen wie die durch Richtlinie (EU) 2016/1148) eingerichtete der NIS Cooperation Group, deren Aufgabe darin besteht, ein hohes gemeinsames Sicherheit- und Schutzniveau für Netz- und Informationssysteme in der Europäischen Union zu erreichen und die strategische Zusammenarbeit und Kooperation der Mitgliedstaaten zu unterstützen, sehr viel stärker als bislang zu nutzen, um ambitionierte Risikomanagementmaßnahmen abzustimmen;
- sich auf EU-Ebene im Rahmen der Verordnung zur Reform von ENISA (Europäische Agentur für Netz- und Informationssicherheit) und der Entwicklung eines Zertifizierungsrahmens der Sicherheit von Informations- und Kommunikationstechnik für klare und verbindliche IT-Mindeststandards und die schnellstmögliche Umsetzung der mit dieser Verordnung bereitgestellten Instrumente etwa der Festlegung von Sicherheitsstufen für bestimmte Produkte und Dienste und die für eine Zertifizierung notwendigen Checklisten einzusetzen;
- auch auf europäischer Ebene schnellstmöglich die Voraussetzungen dafür zu schaffen, dass unabhängige staatliche Stellen durch angemessen intensive Prüfung und Zertifizierung zumindest von Kernbereichen digitaler Technologien und Infrastrukturen wie etwa Cloud-Diensten und Netzwerktechnik eine eigene Beurteilungs- und Steuerungsfähigkeit bei der IT-Sicherheitsentwicklung erlangen;
- schnellstmögliche eine europäische Cloud-Lösung zu schaffen, auf der Akteure aus allen gesellschaftlichen Bereichen Daten unter Beachtung höchster (IT-)Sicherheitsstandards durchgehend Ende-zu-Ende-verschlüsselt rechtssicher speichern können;

juris Lex QS
21052024 ()

- die Entwicklung eines europäischen 5G-Konsortiums zu ermöglichen und zu unterstützen, das sowohl die großen, auf dem Markt etablierten Akteure als auch kleinere Hardware- und Softwarefirmen zusammenbringt und Anreize und Förderungsmöglichkeiten für den Aufbau eines gemeinsamen Ökosystems für Innovation schafft;
- das große Know-how im Bereich der IT-Sicherheit in Deutschland und Europa durch eine gezielte Forschungsförderung zu nutzen und stärken. Öffentliche Forschungsaktivitäten müssen in Zusammenarbeit mit der EU-Kommission und anderen Mitgliedsländern verstetigt und intensiviert werden, um im internationalen Wettbewerb um die besten IT-Sicherheitskonzepte Expertinnen und Experten in Deutschland und Europa mitzuhalten. Bestehende, diesen Zielen widersprechende rechtliche Regelungen, die zu einer großen Unsicherheit in der praktischen IT-Sicherheitsforschung führen, müssen evaluiert, ggf. geändert und zurückgenommen werden. Zukünftige Leuchtturmprojekte müssen dauerhaft zu wichtigen Säulen einer kohärenten Gesamtstrategie für eine anwendungsorientierte IT-Sicherheits-Forschung in Deutschland und Europa gemacht werden;
- die Fachkräftesicherung vorzuanbringen, um gut ausgebildete Fachkräfte, sei es zur Verhinderung von IT-Angriffen, sei es für die Forschung und Entwicklung von Sicherheitssystemen und -strategien zur Verfügung zu haben. Gerade angesichts eines Wettbewerbs um die besten Fachkräfte mit der freien Wirtschaft muss die Attraktivität der öffentlichen Hand als Arbeitgeber ständig weiterentwickelt werden. Um dies zu gewährleisten, ist der Ausbau geeigneter Aus- und Weiterbildungsstrukturen erforderlich. Insgesamt müssen Ausbildungssysteme im Bereich der Informations- und Kommunikationstechnologie möglichst praxisnah sein und IT-Sicherheitsaspekte angesichts gestiegener, sich stetig wandelnder Herausforderungen verstärkt beachtet werden. Bei der Fachkräfteausbildung muss der bestehende Gender Gap im Bereich der Informations- und Kommunikationstechnologien entschlossen angegangen werden;

Maßnahmen auf internationaler Ebene:

- ihr Engagement auf internationaler Ebene zum Schutz digitaler Infrastrukturen und Kommunikation massiv zu verstärken und sich an den wichtigen Diskussionen in den einschlägigen Standardisierungsgremien angemessen zu beteiligen, Protektionismus, eine sehr weitreichende Überwachung und Kompromittierung digitaler Infrastrukturen sowie eine zunehmende Militarisierung ziviler Netzinfrastruktur zu verhindern;
- anzuerkennen, dass aufgrund der Besonderheiten digitaler Ökosysteme, der Interdependenz von Netzwerkstrukturen sowie großer Zuordnungs- und Abgrenzungsprobleme von IT-Angriffen („Attribution“) eine Politik der Abschreckung und „Hackbacks“ mit zahlreichen potentiell gravierenden negativen Folgen bis hin zur militärischen Konfrontation und unkalkulierbaren Risiken für die Zivilgesellschaft behaftet und daher zum Scheitern verurteilt ist. Die Bundesregierung muss sich stattdessen sehr viel stärker als bisher auf internationaler Ebene für einen Verhaltenskodex einsetzen, der einen klaren Rechtsrahmen setzt und eine Gefährdung ziviler (Netz-)Infrastrukturen durch digitale Angriffe ausschließt;
- sich dafür einzusetzen, dass in einem Multi-Stakeholder-Prozess neue, konkretisierende Regelungen und Vereinbarungen zum Schutz digitaler Infrastrukturen und privater Kommunikation erarbeitet werden. Hierzu hat sich die Bundesregierung bereits vielfach verpflichtet, beispielsweise im Rahmen ihres Engagements in der Freedom Online Coalition. Hierzu gehört beispielsweise, die Regulierung des Exports von Zensur- und Überwachungstechnik weiter zu verbessern, den staatlichen Ankauf, das Offenhalten und die Nutzung von bislang nicht öffentlich bekannten Sicherheitslücken („Zero-Day-Exploits“) international zu ächten und

juris Lex QS
21052024 ()

sich gegen das verfassungsrechtlich bedenkliche Instrument digitaler Gegenangriffe („Hackback“) auszusprechen, da ein nicht zu gewinnender Rüstungswettlauf und die weitere Militarisierung des Internets die Folge wäre.

Berlin, den 17. Dezember 2019

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Begründung

Angesichts jahrelanger Diskussionen um die IT-Sicherheit, des anstehenden Ausbaus des 5G-Netzes, des Einsatzes von Millionen Geräten des „Internet of Things“ (IoT) in Privathaushalten und Unternehmen, aber auch weitreichender Datenskandale und IT-Angriffe in den letzten Jahren, u. a. auf das Regierungsnetz und den Deutschen Bundestag, müsste eine gute IT-Sicherheitspolitik politisch längst höchste Priorität genießen und einen Schwerpunkt der Innen-, Außen-, Sicherheits-, Industrie- und Wirtschaftspolitik der Bundesregierung bilden.

Vor dem Hintergrund jahrelanger Diskussionen über die Integrität digitaler Infrastrukturen und eingesetzter Komponenten sowie der Notwendigkeit staatlicher Regulierung sind die Versäumnisse der Bundesregierung nur durch ein weitgehendes Desinteresse und eine falsche politische Prioritätensetzung zu erklären.

Statt ihrer Schutzpflicht für die Vertraulichkeit und Integrität informationstechnischer Systeme und dem Grundrecht auf Privatheit von Kommunikation gerecht zu werden, stellt die Bundesregierung selbst eine Gefahr für die IT-Sicherheit dar.

Notwendig ist eine Kehrtwende der Bundesregierung hinsichtlich ihrer IT-Sicherheitspolitik: Digitale Infrastrukturen müssen effektiv geschützt, Mindeststandards für den Einsatz von Geräten anbieterunabhängig definiert, offene Rechtsfragen geklärt, ein neues Haftungsregime etabliert und unabhängige Aufsichtsstrukturen gestärkt werden. Darüber hinaus muss die Bundesregierung von die IT-Sicherheit gefährdenden Maßnahmen wie „Hackbacks“, anlassloser Massenüberwachung, dem Handel mit Sicherheitslücken und „Zero Day Exploits“, der Ausweitung von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung sowie der Zusammenarbeit mit dubiosen IT-Sicherheitsfirmen Abstand nehmen.

Insgesamt sind Abhängigkeiten von einzelnen Anbietern auch heute schon hoch.

Neben der technischen Überprüfbarkeit eingesetzter Hard- und Software durch unabhängige Aufsichtsstrukturen und die Offenlegung von Quellcode, sind auch rechtliche Rahmenbedingungen in den jeweiligen Ländern und Verbindungen von Unternehmen zu Regierungen zwingend stärker zu berücksichtigen.

Im Zweifelsfall ist der Sicherheit von Infrastrukturen, privater Kommunikation und der Integrität eingesetzter Geräte und Komponenten Vorrang einzuräumen. Bisherige, regulative Versäumnisse und sich daraus ergebende etwaige Verzögerungen und Kostensteigerungen dürfen nicht ausschlaggebendes Kriterium sein.

Vielmehr müssen nachvollziehbare Kriterien aufgestellt werden, die für alle Anbieter und Betreiber gleichermaßen gelten, die Integrität digitaler Infrastrukturen garantieren und Rechtssicherheit für Unternehmen und Verbraucher schaffen.

Auch der Umstand, dass schon in heutigen Netzen teilweise sehr relevante Abhängigkeiten bestehen und Komponenten einzelner Anbieter mit erheblichen Anteilen verbaut sind, darf nicht automatisch dazu führen, dass andere Kriterien angelegt werden. Vielmehr müssen derart große Abhängigkeiten auch in bestehenden Netzen schrittweise reduziert und Alternativen gestärkt werden.

Wo Führung und die überfällige Klärung zentralen Zukunftsfragen der digitalen Gesellschaft durch die Bundesregierung gefordert wären, sind bislang ein hochnotpeinliches, monatelanges Hin und Her, anhaltende Grabenkämpfe zwischen verschiedenen Ministerien und Sicherheitsbehörden sowie eine Politik, die noch immer nicht die Bedeutung der IT-Sicherheit in unserer vernetzten Gesellschaft verstanden hat, zu beobachten. Hierdurch wird der Blick auf echte Lösungen und eine größere digitale Souveränität Deutschlands und Europas verstellt.

juris Lex QS
21052024 ()

EU-Kommissionspräsidentin Ursula von der Leyen hat Recht, wenn sie mit Blick auf Regulierung im Digitalen an Folgendes erinnert: „Es ist unsere Pflicht, an einem besseren System zu arbeiten, das auf unseren Werten von Freiheit, Demokratie und Rechtsstaatlichkeit basiert." Dieser Verpflichtung muss auch die Bundesregierung im Jahr 2019 endlich gerecht werden. Neben notwendigen Schritten zur Erhöhung der (IT-)Sicherheit auf nationaler Ebene, brauchen wir ein entschlossenes, gemeinsames Handeln auf europäischer und internationaler Ebene.

Die weiteren Herausforderungen, um die IT-Sicherheit neben den in den Forderungen skizzierten Punkten zu erhöhen, sind vielfältig:

Mit einer Verschlüsselungsoffensive müssen durchgehende Ende-zu-Ende-Verschlüsselung zum absoluten Standard bei allen staatlichen E-Government-Projekten gemacht werden. Die Forschung für ebenso sichere wie nutzerfreundliche Angebote ist stärker zu unterstützen. Bei allen E-Government-Angeboten sind beste IT-Sicherheitslösungen auf dem neuesten Stand der Technik wie durchgehende Ende-zu-Ende-Verschlüsselungen zu implementieren.

Datenschutz und IT-Sicherheit müssen zukünftig zusammen gedacht und überfällige gesetzgeberische Handlungen im Bereich des Datenschutzes, auch und gerade gegenüber marktmächtigen Plattformen, angegangen werden. Dazu zählt u. a. die aktive politische Begleitung der E-Privacy-Verordnung. Auch hinsichtlich der Umsetzung der EU-DSGVO bedarf es weiterer gesetzlicher Regelungen, u. a. zum Schutz von Beschäftigten. Genauso muss der höheren Schutzbedürftigkeit von Kindern und Jugendlichen Rechnung getragen werden. Innovative Datenschutzmodelle (by design/by default) sind als wichtiger Bestandteil einer guten digitalen IT-Sicherheits- und Standortpolitik stärker zu unterstützen. Gleiches gilt für proaktive Anreize für innovativen Datenschutz durch Auditierungs- und Zertifizierungsverfahren. Entsprechende Zertifizierungen und höchste IT-Sicherheitsstandards müssen Voraussetzung öffentlicher Förderung und Beschaffung sein. Zudem ist der Verzicht auf Grundrechte gefährdende, staatliche Maßnahmen wie den „Hackback" und anlasslose Massenüberwachungen unabdingbar. Die Quellen-Telekommunikationsüberwachung und Online-Durchsuchung dürfen zumindest so lange nicht angewandt werden, bis die Verfassungskonformität einwandfrei nachgewiesen ist. Eine Ausweitung auf den nachrichtendienstlichen Bereich ist klar abzulehnen. Das Sinnieren über die Schaffung genereller Hintertüren in Messenger-Diensten und allen Geräten des „Internet of Things" muss aufhören.

Zudem braucht es einer klaren Absage an den staatlichen Handel mit bislang nicht öffentlich bekannten Sicherheitslücken („Zero-Day-Exploits"), die Einführung einer generellen Meldepflicht für Sicherheitslücken sowie die Implementierung von Verfahren zur schnellstmöglichen Schließung von Sicherheitslücken im Zusammenspiel von Behörden, Unternehmen und Zivilgesellschaft (inkl. sog. „Bug Bounty"-Programme). Die Zusammenarbeit mit dubiosen, weitgehend unkontrollierbaren IT-Sicherheitsfirmen muss eingestellt und das Kontrollregimen für Exporte weiter verschärft werden. Auch braucht es rechtliche Klarstellungen bezüglich der Zusammenarbeit im sogenannten „Cyberabwehrzentrum" und hinsichtlich der genauen Aufgaben der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). Statt das im Telemediengesetz (TMG) verankerte Recht der Nutzerinnen und Nutzer auf eine anonyme und pseudonyme Nutzung von Telemedienangeboten zu hinterfragen, müssen Maßnahmen ergriffen werden, die den Schutz der Nutzerinnen und Nutzer gewährleisten und ausbauen.

Obwohl die Geltung des Völkerrechts im Kontext von digitalen Infrastrukturen und persönlicher Kommunikation auf allen internationalen Regelungsebenen anerkannt wird, läuft die seit den 1980er Jahren auf UN-Ebene erhobene Forderung, militärische und geheimdienstliche Aktivitäten in der zivilgesellschaftlichen digitalen Infrastruktur zu ächten, derzeit weitgehend ins Leere. Hier muss sich die Bundesregierung in einem Multi-Stakeholder-Prozess für neue, konkretisierende Regelungen und Vereinbarungen zum Schutz digitaler Infrastrukturen und privater Kommunikation einsetzen. Hierzu hat sie sich vielfach, beispielsweise im Rahmen ihres Engagements in der Freedom Online Coalition verpflichtet.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333

juris Lex QS
21052024 ()