VERBAND DER INTERNETWIRTSCHAFT E.V.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 B

Stellungnahme zu den Anträgen:

19/7698: Digitalisierung ernst nehmen – IT-Sicherheit stärken,
19/7705: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, und
19/1328: IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

Berlin, 4. April 2019

Die Digitalisierung ist in Deutschland und Europa auf dem Vormarsch. Immer mehr Geräte enthalten IT oder sind über Datenverbindungen mit dem Netz verbunden. Schätzungen des BMVI auf Grundlage des IT-Netzwerkausrüsters Cisco gehen davon aus, dass die Zahl vernetzter Geräte bis 2020 auf ca. 800 Millionen in Deutschland allein steigen wird. Schätzungen verschiedener Netzbetreiber gehen von insgesamt zwischen 35 Mrd. und 50 Mrd. vernetzten Geräten weltweit in den 2020ern aus. Mit der zunehmenden Vernetzung von IT-Systemen und der Übernahme immer neuer Funktionen und Aufgaben in immer mehr Einsatzgebieten kommt IT eine ständig wachsende Bedeutung zu. Mit diesem Wachstum steigt auch die Relevanz der Sicherheit dieser Systeme für alle Beteiligten. Der Themenkomplex der IT-Sicherheit wird deshalb von Staat, Wirtschaft und Gesellschaft zunehmend als relevantes Handlungsfeld der Politik gesehen.

Die Veröffentlichung der Cybersicherheitsstrategien von 2011 und 2016, das IT-Sicherheitsgesetz von 2015 und dessen Ergänzung im Jahr 2017, sowie die vom Bundesministerium für Verteidigung gestartete Initiative zum Cyber- und Informationsraum zeigen nur einige Ansätze dafür, wie die Bundesregierung mit diesen Bedrohungen umgeht.

Der Internetwirtschaft kommt im Rahmen dieser Überlegungen in mehrerlei Hinsicht wachsende Bedeutung zu. Zum einen bietet und liefert sie die Infrastrukturen und Dienste, die die digitale Welt ausmachen und ist damit Treiber der voranschreitenden Digitalisierung sind. Gleichzeitig kann sie Angriffsziel und Opfer von Angriffen werden, sie spielt damit eine Schlüsselrolle bei der Gestaltung von IT-Sicherheit in Deutschland.

Die Debatte um die Ausgestaltung von IT-Sicherheit hat sich in den vergangenen Jahren weiter differenziert und adressiert sowohl operative

Fragen zu konkreten Maßnahmen der IT-Sicherheit, als auch in zunehmendem Maße die dahinterliegenden Strukturen und Maßgaben. Beide werden in den zur Debatte stehenden Anträgen entsprechend gewürdigt. eco – Verband der Internetwirtschaft e.V. sieht in den folgenden Bereichen weiteren Diskussions- und Erörterungsbedarf:

(IT-)Sicherheitsarchitektur:
Die jüngsten Vorfälle wie die Doxing Attacke gegen Bundestagsabgeordnete, aber auch die allgemeine Entwicklung der Sicherheitsinstitutionen in Deutschland mit der Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) werfen die Frage nach der „organisatorischen Fitness“ der deutschen Sicherheitsbehörden für digitale Sicherheitslagen auf. Im Zentrum der Überlegungen steht immer wieder das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Eine zentrale Forderung, die auch in den drei vorliegenden Anträgen herausgearbeitet wird, ist die Unabhängigkeit des BSI und dessen Herauslösung aus dem Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat (BMI). Zentral an dieser Stelle ist, dass das BSI unabhängig von anderen Behörden arbeiten sollte und sich so alleine auf eine Förderung der IT Sicherheit statt deren Unterwanderung fokussieren kann.

Dies gilt umso mehr für Wechselwirkungen mit der ebenfalls im Geschäftsbereich des BMI betriebenen ZITiS. Beide Institutionen haben unterschiedliche Aufgaben, die möglicherweise zueinander in ein Spannungsverhältnis geraten könnten, wenn eine Stelle Schwachstellen sammeln, prüfen und deren Behebung einleiten soll, die andere möglicherweise jedoch Schwachstellen ausnutzt, um im Auftrag von Ermittlungsbehörden und Geheimdiensten in IT-Systeme einzudringen. Es ist offensichtlich, dass sich diese Gemengelage unterschiedlicher Aufgaben diametral gegenübersteht.

Es bedarf für die Funktion des BSI als zentrale Behörde für Cybersicherheit einer Klarstellung dahingehend, dass die Arbeit des BSI unabhängig von den Erwägungen anderer Stellen und Sicherheitsbehörden erfolgt und ausschließlich der Verbesserung der Sicherheit von IT-Systemen und Netzen verpflichtet ist.

Alle davon abweichenden Maßgaben schwächen die Rolle des Amtes und das Vertrauen in digitale Dienste. Im Sinne einer stringenten Digitalisierung ist dies

nicht hilfreich, da so letzten Endes auch das Vertrauen in staatliche Behörden und deren Zuverlässigkeit untergraben wird. Die Festschreibung des BSI als obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern wird dem möglicherweise aufgrund der vorgetragenen Vorbehalte nicht mehr gerecht.

In diesem Licht steht auch die Arbeit des Nationalen Cyberabwehrzentrums (NCAZ). Als Koordinierungsstelle für die IT-Abwehr steht es sowohl direkt durch die Zusammenarbeit mit dem BfV als auch durch die Zusammenarbeit mit weiteren Geheimdiensten und Ermittlungsbehörden vor der Frage, welchen Beitrag es zur Verbesserung der IT-Sicherheit leisten soll. Das Beispiel des groß angelegten Hacks auf das Auswärtige Amt und das Bundesverteidigungsministerium unterstreichen grundsätzlich, dass es neben der Arbeit des BSI auch in allen anderen Verfassungsorganen eine proaktive Auseinandersetzung mit dem Thema und darüber hinaus auch der Austausch über organisationsübergreifende Ereignisse sinnvoll sein kann.

In diesem Kontext wird immer wieder auch die Forderung nach einer Neuzuordnung des BSI in den Geschäftsbereich eines noch zu schaffenden Bundesministeriums für Digitales diskutiert. Ein solches Ministerium hat durchaus den Vorteil, der bestehenden Zersplitterung bei der Regulierung von Netzen und Diensten entgegenzuwirken, wenn der entsprechende fachliche Zuschnitt korrekt erfolgt. Je nach Themenschwerpunkt hat man bei zentralen Fragen der Digitalisierung mit bis zu vier verschiedenen Bundesministerien zu tun, die sehr unterschiedliche, teilweise widersprüchliche Ziele verfolgen. Aber auch bei einer solchen Neuzuordnung muss der Grundsatz gelten, dass das BSI in seiner Arbeit unabhängig sein muss und über etwaig bestehende Zweifel, die durch die Zusammenarbeit mit Sicherheitsbehörden entstehen, erhaben sein muss. Da das hier in Rede stehende Digitalministerium aller Voraussicht nach keine geheimdienstlichen Aufgaben übernimmt, wären die Zweifel, die derzeit in Bezug auf das BMI im Zusammenhang mit ZITiS bestehen, ausgeräumt.

Zuletzt sei noch auf die Ausstattung und Ausrüstung von Polizeibehörden eingegangen. Diese müssen dringend sowohl personell als auch technisch besser ausgestattet sein und für die Herausforderungen der Strafverfolgung im Netz besser geschult werden. Die Erfahrungen, die eco in Workshops mit Strafverfolgern und Ermittlungsbehörden gemacht hat, zeigen, dass hier noch dringender Informations- und Nachschulungsbedarf besteht. Inwieweit eine organisatorische Umgestaltung der Ermittlungsarbeit in Form einer Bündelung bestimmter Arbeiten bei den Zentralen Anlaufstellen für Cybercrime (ZACs)

hilfreich sein kann, kann nicht abschließend beurteilt werden. Zu überlegen ist hierbei, ob es darüber hinaus nicht auch sinnvoll wäre, wenn grundsätzlich eine Verbreiterung der IT-Kompetenzen von Polizeibeamten erfolgen würde.

Strukturelle Verbesserung der IT-Sicherheit:
Eine maßgebliche Frage ist der Umgang mit Schwachstellen, über die öffentliche Stellen Kenntnis erlangen. Derzeit gibt es keine klaren Maßgaben, wie mit solchen Schwachstellen umgegangen wird. Grundsätzlich sollten solche Schwachstellen den Unternehmen mitgeteilt werden, in deren Systemen oder Produkten sie bestehen. Wenn Behörden Sicherheitslücken in IT-Systemen für sich behalten, bspw. um besser mit Hilfe eigener Software Überwachungsmaßnahmen durchzuführen oder um gezielt schädliche Systeme oder Akteure ausschalten zu können (Hackback), schädigt dies das Vertrauen von Nutzerinnen und Nutzern in die Verwendung dieser Dienste. Es gefährdet zudem auch deren Sicherheit. Es ist daher dringend angezeigt, dass alle staatlichen Stellen ihnen bekannte Sicherheitslücken zwingend melden und zwecks einer Schließung derselben in die Datenbank bekannter Sicherheitslücken (CVS) überführen müssen.

Eine entsprechende Meldepflicht wurde bereits mit dem IT-Sicherheitsgesetz (IT-SG) den Betreibern kritischer Infrastrukturen (KRITIS) auferlegt und mit dem NIS-Richtlinien-Anpassungsgesetz von 2017 auf Betreiber von Clouddiensten und Onlinemarktplätze ausgeweitet. Staatliche Stellen stehen aus Sicht des eco hier ebenso in der Pflicht, Ihren Teil zur Verbesserung der IT-Sicherheit aller Beteiligten zu leisten

Dies wirft auch die Frage auf, wie mit Software verfahren wird, die zur Ausspähung von Informationen auf Endgeräten von Nutzern durch Ermittlungsbehörden und Geheimdienste (Staatstrojaner) eingesetzt wird.

Zwar bieten Staatstrojaner gegenüber der flächendeckenden, anlasslosen Vorratsdatenspeicherung den Vorteil, dass sie zumindest theoretisch zielgerichtet eingesetzt werden können, auch wenn sich hier die Frage nach einer möglichen nicht intendierten Weiterverbreitung stellt. Ihre Einsatzszenarien werfen jedoch eine Reihe grundlegende Fragestellungen auf, die bis heute nicht geklärt wurden.

Diese Ermittlungswerkzeuge müssen auf den Endgeräten der Zielpersonen installiert werden. Hierzu liegen keine Erkenntnisse vor, wie genau dies geschieht. Das wirft die Frage auf, ob und inwieweit hier möglicherweise

schadhafte Auswirkungen durch die Ausnutzung von Sicherheitslücken in Kauf genommen werden, über die Ermittlungsbehörden und Geheimdienste verfügen. Zahlreiche weitere Sicherheitsmaßnahmen, wie beispielsweise die Stärkung der Verschlüsselung von Diensten, würden so untergraben.

Der Einsatz von Verschlüsselung ist ein zentraler Baustein für mehr Sicherheit in digitaler Kommunikation. Ihr Einsatz sollte daher auf keinen Fall durch Regelungen zur Bereitstellung von „Generalschlüsseln“ durch Betreiber von Diensten oder durch vorgegebene Übergabe- und Ausleitungsschnittstellen untergraben werden. Die Praxis zeigt zudem, das derartige Schlüssel in keinem Fall dauerhaft geheim gehalten werden können.

Auf dem Markt befinden sich verschiedene offen zugängliche Verschlüsselungslösungen, sowie Dienste, die eigene Verschlüsselungs-technologien zum Einsatz bringen. Eine Festlegung auf eine bestimmte Verschlüsselungstechnologie oder einen bestimmten Standard durch den Staat, bspw. bei Ausschreibungen, sollte kritisch geprüft werden und mit Blick auf die dynamischen Entwicklungen im Markt eher zurückgestellt werden.

Die Problematik unterschiedlicher – tendenziell gleichwertiger – Sicherheitslösungen stellt sich auch bei der Frage der Anerkennung von Normen und Standards mit Bezug auf IT-Sicherheit. Die Debatte um die TR-Router des BSI und deren Akzeptanz bei TK-Unternehmen und Kabelnetzbetreibern mit eigenen Standards einerseits, sowie den Herstellern der Geräte andererseits zeigt, dass Normierung im Sinne einer einheitlichen Definition von zwingend einzuhaltenden technischen Standards und Spezifikationen in der bisherigen Form u.U. nicht zielführend ist.

Auch die Verpflichtung zur Veröffentlichung des Quellcodes unter einer bestimmten öffentlichen Lizenz (Open Source) ist nicht zwingend und ausschließlich mit einer Verbesserung der IT-Sicherheit verbunden, wenngleich es im Prinzip zu einer Verbesserung des Sicherheitsniveaus beitragen kann, wenn der Quellcode einer Überprüfung zugänglich ist und so nachvollzogen werden kann. Dies ermöglicht allerdings zugleich auch, dass Schwachstellen in Quellcodes von allen Akteuren, auch böswilligen, identifiziert und ausgenutzt werden können. Es sollte daher grundsätzlich im Ermessen von Entwicklern und Herstellern liegen, wie sie ihre Software lizenzieren wollen und mit wem sie für welche Zwecke ihren Quellcode teilen wollen. Escrow-Verfahren mit beschränktem Zugang, wie Beispielsweise im derzeitigen IT-Sicherheitsgesetz für das BSI vorgesehen, können hier ebenfalls zum Einsatz kommen.

Robuster Rechtsrahmen für IT-Sicherheit:
In der Gesamtschau stellt sich die Frage, wie ein Rechtsrahmen für IT-Sicherheit auszugestalten wäre. Der Schutz personenbezogener Daten nimmt hierbei eine besondere Stellung ein.

Mit der Datenschutz-Grundverordnung (DSGVO) hat die Europäische Union bereits einen Rechtsrahmen gestaltet und auch Maßgaben für mehr (IT-)Sicherheit in den Verordnungstext einfließen lassen. Sie implizieren, dass Datenverarbeitung auch unter „sicheren“ Rahmenbedingungen geschehen muss und bietet im Verbund mit den vorliegenden Regelungen zur IT-Sicherheit hohe Anforderungen an Anbieter von Diensten und Produkten. Zwar wäre hier noch eine Überprüfung der Einheitlichkeit der Meldewege und –pflichten zu überprüfen, um Dopplungen bei den Meldepflichten zu vermeiden. Grundsätzlich ist dieser Rechtsrahmen jedoch geeignet.

Inwieweit eine zusätzliche europäische Regelung zur Vertraulichkeit elektronischer Kommunikation einen Beitrag leisten kann, muss an dieser Stelle offenbleiben. Eine Regelung, die, analog zum deutschen Fernmeldegeheimnis, die Vertraulichkeit von Kommunikationsinhalten während des Datentransfers sicherstellt, könnte auf europäischer Ebene für Klarheit sorgen. Sinnvoll wäre hier den Regelungsbedarf zu prüfen und die bestehende Regulierung robust umzusetzen, ehe weitere Regelungen getroffen werden.

Vor dem Hintergrund der Bedeutung des Schutzes personenbezogener Daten und datensparsamer Ansätze bei Ermittlungen und bei staatlichem Handeln ist es auch wegen des massiven Eingriffs in die Vertraulichkeit der Kommunikation von Bürgerinnen und Bürgern dringend erforderlich, dass die Vorratsdatenspeicherung abgeschafft wird.

Darüber hinaus stellt sich die Frage, wie das oben beschriebene Spannungsverhältnis zwischen Ermittlungsbehörden und Geheimdiensten auf der einen Seite und Institutionen zur Stärkung von IT-Sicherheit auf der anderen Seite sinnvoll aufgelöst werden kann. Derzeit ist zu beobachten, dass zahlreiche, oftmals kritisch zu bewertende, Maßnahmen insbesondere im Geheimdienstbereich mit Verweis auf die Handlungsfähigkeit der Behörden nachträglich legalisiert werden. Dies war bei der Novelle des letzten Gesetzes über den Bundesnachrichtendienst Ende 2016 und auch bei dem jetzt bekannt gewordenen Entwurf eines Gesetzes zur Harmonisierung des

Verfassungsschutzrechts der Fall, welcher durch eine Änderung des Verfassungsschutzgesetzes sowie des BND-Gesetzes die Möglichkeiten der Dienste erneut deutlich ausweiten soll. Außer Acht gelassen werden dabei allerdings die negativen Auswirkungen auf das Vertrauen und die Integrität in Telekommunikation und digitale Dienste.

Darüber hinaus und je nach Angriffsvektor der Ermittlungsbehörden wirft dies auch die Frage auf, ob für die Durchführung der Maßnahmen nicht ein größeres Sicherheitsrisiko für die Allgemeinheit erzeugt und billigend in Kauf genommen wird, als in einer digitalisierten Gesellschaft akzeptabel.

Zu beobachten ist zudem, dass immer häufiger eine eigentlich originär staatliche Verantwortung auf Betreiber von Diensten und Netzen übertragen wird. Dies geschieht sowohl auf europäischer Ebene mit der derzeit diskutierten „Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte“ als auch in Deutschland beispielsweise mit dem vom Bundesrat diskutierten „Anti-Darknet-Gesetze“.

Beiden ist gemein, dass sie oftmals sehr unspezifische Anforderungen an Betreiber von Diensten und Netzen stellen, somit also einen recht frühen Übergang der Verantwortung implizieren könnten bei einer weiten Interpretation und Auslegung. Diese Verschärfungen des Strafrechts im IT-Bereich halten wir für nicht sinnvoll, da sie den problematischen Einsatz technisch nur bedingt tauglicher Maßnahmen wie Uploadfilter erfordern und zudem auch eine konsistente und proaktive Überwachung von Nutzern und deren Aktivitäten im Netz bedingen oder zumindest zur Folge haben. Dies ist sowohl aus bürgerrechtlicher Sicht als auch aus technischer Sicht nicht sinnvoll.

Die Verantwortung für Ereignisse im Netz mit Sicherheits- oder Strafrechtsrelevanz kann sinnvoll nur für solche Fälle zugeschrieben werden, die im Verantwortungs- und Einflussbereich des jeweiligen Akteurs stehen. Dies gilt sowohl für Fragen der proaktiven Kontrolle und Überwachung von Nutzern, die strikt abzulehnen ist, als auch für die Haftung für etwaig bestehende IT-Sicherheitslücken, die oftmals nur vom Hersteller der jeweiligen Software oder des jeweiligen Produkts bzw. der jeweiligen Komponente sinnvoll adressiert werden kann.

In beiden Fällen ist eine pauschale Zuweisung und Verlagerung der Verantwortung an einen Akteur, der gesamtschuldnerisch für alle Aktivitäten seiner Nutzer aber auch seiner Geschäftspartner in der Pflicht steht, nicht

sinnvoll darstellbar.

Unbeschadet davon kann im Fall der IT-Sicherheit darüber nachgedacht werden, in welchen Fällen eine Konkretisierung der bestehenden Haftungsregeln sinnvoll ist, so beispielsweise zur besseren Adressierung einer möglichen Fahrlässigkeit im Rahmen der Herstellerhaftung., Dies könnte exemplarisch wie im bestehenden Haftungsrecht für einen Mangel in IT-Systemen dargestellt werden, die per definitionem ebenfalls nie komplett fehlerfrei sein können.

Eine Haftung von Plattformbetreibern, Hostern oder Telekommunikationsunternehmen für die Handlungen von Nutzern, die über die in der e-Commerce Richtlinie definierten Maßgaben hinausgehen, und wie sie jetzt schon teilweise mit dem Netzwerkdurchsetzungsgesetz (NetzDG) und den dazu gehörigen Bußgeldleitlinien eröffnet worden sind, lehnen wir ab.

Sie illustrieren ebenfalls die Übertragung von Verantwortung der genannten Akteure für das Verhalten von Nutzern und nehmen Ermittlungsbehörden und Justiz aus der Verantwortung. Wir halten mit Blick auf die Maßgaben des Rechtsstaats und der geteilten Verantwortung daher die Neudefinition bestehender Probleme durch digitale Technologien für nicht sinnvoll.

Fazit:
Deutschland ist – auch geprägt durch europäische Debatten – vor die Frage gestellt, wie es seine Digitalisierung weiter vorantreiben möchte. Derzeit bestehen sowohl auf gesetzlicher als auch auf organisatorischer und operativer Ebene Spannungsgefüge zwischen verschiedenen Interessen. Im Sinne eines offenen und resilienten Internets bzw. einer darauf ausgerichteten Internet-Governance sollte daher darauf geachtet werden, dass das Interesse der Allgemeinheit für sichere und vertrauenswürdige Dienste und Kommunikation immer Vorrang vor den Interessen individueller Akteure für den Zugang zu IT-Systemen oder Endgeräten haben sollte. Weiterhin sollten Behörden, die diese Sicherheit und Integrität sicherstellen und ggf. auch regulieren sollen, unabhängig agieren können und nicht in diesem Spannungsgefüge sich diametral gegenüberstehender Aufgaben agieren, da dies am Ende die Glaubwürdigkeit aller Akteure nachhaltig beschädigt.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.