Rede von Martina Renner zu Protokoll gegeben am 27.04.2017

Rede von Martina Renner, 27. April 2017

Die Sicherheit der Informationstechnologie ist eine wichtige Aufgabe, die nicht nur in Deutschland, sondern auch in Europa und weltweit seit Jahren an Bedeutung gewinnt. Aufgrund der fortschreitenden Vernetzung durch Smartphones, IP-Telefonie, der Digitalisierung von Arbeit und Leben und des Internets der Dinge ist Politik gefordert. Es besteht eine staatliche Schutzpflicht gegenüber den Bürgerinnen und Bürgern, die sich nicht in der Einrichtung eines Cyberabwehrzentrums, eines Cyber-Sicherheitsrates oder Meldepflichten für kritische Infrastrukturen erschöpft. Und schon gar nicht durch das ständige Wiederholen von Cyber, Cyber, Cyber.

Tatsächlich ist dem vorgelegten Entwurf zur Umsetzung der Richtlinie zur Verbesserung der Netz- und Informationssicherheit anzumerken, dass Deutschland nicht – wie der Kollege Binninger in der ersten Beratung behauptete – vorangegangen ist. Die Bundesregierung hechelt hinterher!

Der Gesetzentwurf zum Umsetzungsgesetz bleibt sowohl in der Definition als auch in der Konkretisierung der Anforderungen für digitale

Diensteanbieter weiterhin völlig unbestimmt. Im Zweifel müssten sich diese Anbieter sowohl an die Regelungen für Anbieter von Telemediendiensten als auch für Anbieter von „digitalen Diensten“ halten. Eine solche Doppelregulierung und unklare Sicherheitspflichten für die Anbieter stärken die Netz- und Informationssicherheit im Ergebnis nicht. Eine nicht eindeutige Regelung widerspricht vielmehr dem Zweck der Richtlinie. Netz- und Informationssicherheit werden nicht erhöht, sondern Schlupflöcher geschaffen. Niemandem, weder den Verbrauchern noch den Anbietern, ist damit gedient. Der Systematisierung der IT-Sicherheitspflichten für alle Anbieter und Dienste geht die Bundesregierung aus dem Weg. Tatsächlich sind die Sicherheitsanforderungen von Telekommunikationsnetzen, Telemediendiensten, den sogenannten wesentlichen Diensten, den Vertrauensdiensten und den digitalen Diensten aufgesplittert. Dieses Manko wird nicht durch das vorliegende Umsetzungsgesetz beseitigt.

Mittels Änderungsantrag hat die Große Koalition zwischenzeitlich eine begleitende Ergänzung des Telekommunikationsgesetzes auf den Weg gebracht. Zur Begründung wird angeführt, dass Telekommunikationsanbieter neben den Bestandsdaten bei einer Störung auch die sogenannten Steuerungsdaten auswerten müssten. Allerdings ist auch dieser Vorschlag viel zu unbestimmt. Tatsächlich wird hier der Weg freigemacht, um bei späteren Gesetzänderungen draufsatteln zu können. Dass die Diensteanbieter gehalten sind, Störungen und deren Ursachen zu analysieren, ist das eine. Dass aber dabei aber die Möglichkeit eröffnet wird, die Steuerungsdaten auch für künftige Analysen greifbar zu machen, ist mit dem Datenschutz nicht vereinbar. Der Ausschluss der Inhaltsdaten dient hierbei nur der Kosmetik. Der

Zugriff auf die Steuerungsdaten erlaubt im Zusammenspiel mit den Bestandsdaten weitreichende Analysen der Betreiber und der Behörden.

Anders als behauptet wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht etwa für die kommenden Entwicklungen gerüstet. Tatsächlich wird das BSI weiter zu einer operativen Behörde ausgebaut. Demgegenüber bleibt der Geburtsfehler der Behörde bestehen, denn sie wird institutionell nicht gestärkt. Das BSI bleibt dem Bundesinnenministerium unterstellt. Seine Unabhängigkeit ist also nicht gewährleistet. Die Sensibilität der beim BSI gesammelten Informationen über Sicherheitslücken und -strukturen sowie der Umgang mit persönlichen Daten aus Unternehmen und von Privatpersonen erfordert aber zwingend, es als unabhängige Bundesbehörde mit unzweideutigem Sicherheitsauftrag aufzustellen. Nur so kann das unklare Verhältnis des BSI zu den polizeilichen Sicherheitsbehörden und den Geheimdiensten beseitigt werden. Es braucht diese klaren Zuständigkeiten. Andernfalls droht der Sicherheitsauftrag des BSI durch die intensive Zusammenarbeit mit BND, BfV und MAD national über das Cyber-Abwehrzentrum oder international in der Kooperation mit der NSA ins Leere zu laufen. Erst recht, wenn die Geheimdienste gleichzeitig Sicherheitslücken einkaufen oder erforschen, wie mit der Behörde ZITiS geplant. Das Vertrauensproblem in Bezug auf die für IT-Sicherheit hauptsächlich zuständige Bundesbehörde BSI wird auf diese Weise nicht gelöst.

Schließlich verzichtet die Bundesregierung erneut darauf, Regelungen zur Produktsicherheit und Produkthaftung für IT-Produkte und IT-Dienste einzuführen. Schon bei Verabschiedung des IT-Sicherheitsgesetzes 2015 wurde dies versäumt

und bis heute nicht nachgeholt. Ausgangspunkt von Sicherheitsproblemen aber sind in den allermeisten Fällen Sicherheitslücken in der eingesetzten Software. Aber auch Router und vernetzte Geräte sind eine besondere Gefahrenquelle. Zum Kern des Problems in der IT-Sicherheit vorzudringen, heißt daher, Haftungsverschärfungen für IT-Sicherheitsmängel im IT-Sicherheitsrecht aufzunehmen. Da entsprechende Regelungen fehlen, springt das Umsetzungsgesetz zu kurz.

Die fehlenden Verschärfungen im IT-Sicherheitsrecht und die Zersplitterung der Sicherheitsanforderung zeigen einmal mehr, dass die Bundesregierung keineswegs vorangeht, sondern Bruchstücke zur Strategie verklärt.

Aus diesen Gründen werden wir dem Umsetzungsgesetz im Ergebnis nicht zustimmen und den Gesetzentwurf ablehnen.