(A) IT-Sicherheitsgesetz haben wir in Deutschland die meisten Vorgaben dieser Richtlinie erfüllt und sind mit gutem Beispiel vorangegangen.

Mit dem IT-Sicherheitsgesetz haben wir bereits eine gesetzliche Meldepflicht für Betreiber kritischer Infrastrukturen geschaffen. Diese Meldepflicht wird jetzt mit dem vorliegenden Gesetzentwurf auch auf digitale Dienste wie Onlinemarktplätze und Suchmaschinen ausgeweitet und erfüllt damit die Vorgaben der EU-Richtlinie. Gerade diese Meldepflicht ist zur Erstellung eines Lagebilds unabdingbar. Nur dadurch können wir nachvollziehen, wie umfangreich die Angriffe sind und welche neue Schadsoftware im Umlauf ist.

Durch den vorliegenden Gesetzentwurf werden die Befugnisse des BSI zur Überprüfung der technischen und organisatorischen Sicherheitsanforderungen erweitert und die rechtlichen Grundlagen für den Einsatz von Mobilen Incident Response Teams, MIRTs, geschaffen, die andere Stellen bei Bedarf, bei der Abwehr von Cyberangriffen mit besonders hoher technischer Qualität, vor Ort unterstützen können. Zusätzlich wird es dem BSI ermöglicht, die Einhaltung der Vorgaben bei Betreibern von kritischer Infrastruktur vor Ort zu kontrollieren. Damit stärken wir das BSI weiter bei der Bündelung der Kompetenzen im Cybersicherheitsbereich und verbessern den Schutz von Staat, Wirtschaft und der Bevölkerung vor Angriffen.

Diese Erweiterung der Befugnisse des BSI ist nach den Angriffen der letzten Jahre auch dringend notwendig. Dabei ist aber auch zu betonen: Die Befugniserweiterung des BSI darf den Datenschutz nicht untergraben. Um dies zu gewährleisten, werden daher auch weiterhin keine sensiblen Daten erfasst. Alle personenbezogenen Daten, die für die Wiederherstellung der Sicherheit bei Betreibern kritischer Infrastruktur wichtig sind, werden deshalb sofort gelöscht, wenn sie nicht mehr benötigt werden. Zudem verpflichten wir das BSI mit dem vorliegenden Entwurf, bei grenzüberschreitenden Vorfällen die Behörden des jeweiligen EU-Staates zu informieren. Diese internationale Kooperation ist für ein hohes Schutzniveau in der gesamten Union mitentscheidend und wird deshalb auch zu Recht in der EU-Richtlinie gefordert.

Neben den bereits erwähnten Maßnahmen zeigt auch die Einrichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, ZITiS, im Bundesinnenministerium, welche Bedeutung der Cybersicherheit von den Koalitionsfraktionen und der Bundesregierung zugemessen wird.

Bei der Diskussion über Cyberangriffe muss man aber auch immer erwähnen – und das ist durch die Angriffe in der Vergangenheit auch mehr als deutlich geworden –: Eine absolute Sicherheit vor solchen Angriffen gibt es nicht. Mit dem IT-Sicherheitsgesetz haben wir es aber geschafft, einheitliche Mindeststandards in der Bundesrepublik zu schaffen.

Die Umsetzung der Richtlinie ist für die europäische Zusammenarbeit im Bereich Cybersicherheit ein wichtiges Signal und zeigt, dass wir unserer Vorreiterrolle in Europa nun auch endlich im Bereich der Cybersicherheit gerecht werden. (C)

***Gerold Reichenbach*** *(SPD):* Die Digitalisierung durchdringt unser Leben immer weiter in nahezu allen Bereichen, ein Ende ist nicht absehbar. Das bereits heute bestehende Ausmaß an Vernetzung unserer Alltags- und Arbeitswelt, der Industrie und der Wirtschaft, dem Gesundheitswesen und vielem mehr macht uns in hohem Maße anfällig für Angriffe im und aus dem Cyberraum. Sicherheitslücken und Cyberangriffe können dramatische Folgen haben. Der Angriff auf Internetrouter Ende vergangenen Jahres, bei dem auch großflächig Router der Telekom ausfielen und circa 1 Million Kunden betroffen waren, oder auch der Hackerangriff, der das Krankenhaus Neuss Anfang 2016 lahmgelegt hat, lassen erahnen, was für ein Gefahrenpotenzial im Bereich unsicherer IT-Produkte schlummert und wie sehr ihr Ausfall das öffentliche Gemeinwesen schädigen kann. Um solche Situationen geht es bei der Umsetzung der Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Europäischen Union, über die wir hier in erster Lesung beraten.

Wir begrüßen daher diese vom Europäischen Parlament vorgelegte Richtlinie. Sie bildet die Grundlage für einen einheitlichen europäischen Rechtsrahmen, einen EU-weiten Ausbau nationaler Kapazitäten für die Cybersicherheit und eine stärkere Zusammenarbeit der Mitgliedstaaten in diesem Bereich. Dies ist wichtig, denn IT-Sicherheit ist längst keine nationale Frage mehr. Es werden außerdem Mindestanforderungen und Meldepflichten nicht nur für die Betreiber wesentlicher Dienste, also für Betreiber kritischer Infrastrukturen, sondern auch für die Betreiber bestimmter digitaler Dienste geschaffen. Deutschland ist mit dem IT-Sicherheitsgesetz von 2015 bereits gut aufgestellt. Vorausschauend haben wir hier bereits mit Blick auf die NIS-Richtlinie viele Regelungen, die die Richtlinie nun vorgibt, umgesetzt, sodass die jetzt nötigen Änderungen gering gehalten werden können. (D)

Die Anforderungen der Richtlinie, die über das bestehende IT-Sicherheitsgesetz hinausgehen, sind sinnvoll. Die Meldepflichten und stärkeren materiellen Vorgaben für Unternehmen, die nun beispielsweise Konzepte zur Bewältigung von Sicherheitsvorfällen vorlegen müssen, erachten wir als dringend erforderlich. Aktuelle Cyberangriffe im Telekommunikationsbereich haben gezeigt, dass die Meldewege von der Bundesnetzagentur zum BSI bei Vorfällen in Telekommunikationsnetzen nicht mehr gerecht werden. Insbesondere der Telekom-Vorfall hat gezeigt, dass Meldewege optimiert werden müssen. Wir begrüßen daher auch die mit dem Umsetzungsgesetz eingeführte Doppelmeldepflicht von Sicherheitsvorfällen beim Bundesamt für Sicherheit in der Informationstechnik und bei der Bundesnetzagentur. Durch die parallele Meldung wird es dem BSI ermöglicht, seine Ressourcen und Kompetenzen zeitnah und besser einzusetzen. Zur Erhöhung des Niveaus der Cybersicherheit wird das BSI insbesondere durch die Nachweis- und Meldepflichten der Betreiber kritischer Infrastrukturen weiter gestärkt.

(A) Fortan müssen zudem nicht nur Ausfälle, sondern auch erhebliche Störungen gemeldet werden.

Wir wollen uns den vorliegenden Gesetzentwurf noch näher anschauen mit Blick auf die Frage, wo sich aus den jüngsten Sicherheitsvorfällen noch weiterer Bedarf zur gesetzlichen Reaktion ergibt. Besonderes Augenmerk liegt dabei darauf, wie Sicherheitslücken in IT-Endgeräten, wie beispielsweise jene im genannten Router-Vorfall, vermieden werden können, aber auch, welche Möglichkeiten Netzbetreiber benötigen, um künftig Angriffe schneller abwehren oder sogar verhindern zu können. Denn je mehr beispielsweise die klassische Telefonie auf Voice-over-IP übergeht – und in wenigen Jahren wird Telefonie flächendeckend über Voice-over-IP laufen –, desto mehr ist auch die Möglichkeit der Absetzung eines Notrufs von einer funktionierenden Internetverbindung abhängig. So werden zum Beispiel Router Teil einer sicherheitsrelevanten Infrastruktur. Aus Sicht der SPD-Bundestagsfraktion besteht darum auch im Bereich der Produkthaftung und der Einführung eines verlässlichen Gütesiegels Handlungsbedarf. Da zunehmend alles mit allem vernetzt ist – Stichwort Internet der Dinge/Internet of Things, IoT –, stellt sich immer drängender die Frage, wie die IT-Sicherheit der vernetzten Dinge sichergestellt werden kann und wer in der Haftung ist. Denn nicht nur offensichtlich internetfähige Geräte wie Computer, Smartphones und Tablets sind heutzutage vernetzt und eine potenzielle Gefahrenquelle, auch Alltagsgegenstände wie Wecker, Zahnbürsten, Babyphones, Kaffeemaschinen und Kühlschränke sind heute mit einer IP-Adresse ausgestattet und damit internetfähig. Das In-
(B) ternet der Dinge hat in einem sehr kurzen Zeitraum eine enorme Größe erreicht. Selten finden bei diesen Geräten Softwareupdates statt – oft weil die Hersteller keine sicheren Produkte auf den Markt bringen, oft weil die Nutzerinnen und Nutzer keine Softwareupdates durchführen oder diese auch nicht mehr zur Verfügung stehen. So entstehen weltweit bei Millionen Geräten Sicherheitslücken. Diese Geräte können leichter gehackt und für den Aufbau von Bot-Netzen und DDoS-Angriffe genutzt werden, die zu weiteren Ausfällen von Diensten und von ganzen Infrastrukturteilen führen können. So werden Massenwaren, die von jeder Privatperson gekauft werden können, zum Bestandteil einer kritischen Infrastruktur. Sicherheitsmängel bei privat erworbenen und genutzten Geräten werden so zu einem Sicherheitsrisiko für ganze Teile der Bevölkerung, wenn diese Geräte gehackt als Teil eines Bot-Netzes beispielsweise für den Angriff auf einen Wasserversorger genutzt werden können. Ein Gütesiegel, basierend auf BSI-Mindeststandards halten wir daher für einen wichtigen ersten Schritt, um die Angreifbarkeit von IT-Produkten einzudämmen.

Selbstverständlich macht das Internet nicht an nationalen Grenzen Halt. Insofern gilt es, europäische und internationale Lösungen und Standards für diesen Bereich zu finden und durchzusetzen. Deutschland sollte hier mit gutem Beispiel vorangehen und eine Vorreiterrolle einnehmen. Denn ein hohes Maß an IT-Sicherheit bedeutet nicht nur eine Erhöhung der öffentlichen Sicherheit, sondern auch einen Standortvorteil für Wirtschaft und Unternehmen. Wir sollten Regelungen für die Erhöhung der Sicherheit von IT-Produkten durch die Einführung eines Gütesiegels im weiteren gesetzgeberischen Verfahren daher prüfen. (C)

***Martina Renner*** *(DIE LINKE):* Die Bundesregierung hat sich vorgenommen, die Richtlinie zur Verbesserung der Netz- und Informationssicherheit, NIS-Richtlinie, in nationales Recht zu überführen. Wesentliche Regelungen der sogenannten NIS-Richtlinie allerdings wurden bereits mit dem im Sommer 2016 in Kraft getretenen deutschen IT-Sicherheitsgesetz umgesetzt. Dies betraf beispielsweise die sogenannten wesentlichen Dienste, sprich: Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Seinerzeit nicht adressiert wurden die von der europäischen Richtlinie bereits erfassten „digitalen Dienste“. Das sind Onlinemarktplätze, Suchmaschinen und Cloud-Computing-Dienste. Diese Regelungslücke soll nun geschlossen werden. So weit, so scheinbar unspektakulär. Doch werden bei näherem Hinsehen drei grundlegende Mängel im Regierungsentwurf deutlich.

Erstens. Rechtssicherheit für die Anbieter von „digitalen Diensten“ wird nicht erreicht. Der Regierungsentwurf zum Umsetzungsgesetz bleibt sowohl in der Definition als auch in der Konkretion der Anforderungen für digitale Diensteanbieter völlig unbestimmt. Insbesondere bleibt unbeantwortet, wie diese von den bereits im Rahmen des IT-Sicherheitsgesetzes regulierten Anbietern von Telemediendiensten abzugrenzen sind. Im Zweifel müssten sich die Anbieter an beide Regelungen halten. Geschaffen wird so eine Doppelregulierung und ein undurchsichtiges Dickicht an Sicherheitspflichten. Beides läuft der Gewährleistung der Netz- und Informationssicherheit und damit dem Zweck der Richtlinie zuwider. Weder Verbrauchern noch Anbietern ist damit gedient. Dringend notwendig ist es daher, eine inhaltliche Systematisierung der IT-Sicherheitspflichten für alle Anbieter und Dienste vorzunehmen. (D)

Zweitens. Das Bundesamt für Sicherheit in der Informationstechnik, BSI, wird mit dem Umsetzungsgesetz weiter zu einer operativen Behörde ausgebaut. Erstmals erhält es operative Befugnisse zur Cyberabwehr, um mit eigenen Kräften – wie es im Entwurf des Gesetzestextes heißt – bei der „Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme“ mitwirken zu können. Zum Ausdruck kommt die Ausweitung des Aufgabenbereichs auch in einem erneuten Stellenaufwuchs. Wurden dem BSI mit Verabschiedung des IT-Sicherheitsgesetzes bereits 220 Stellen zusätzlich zugewiesen, so kommen nun noch einmal 181,5 Stellen hinzu.

Zugleich wird die Behörde allerdings nicht institutionell gestärkt, sondern bleibt dem Bundesinnenministerium unterstellt. Die Unabhängigkeit des BSI ist nicht gewährleistet. Der Präsident des BSI hat gerade erst erklärt, bei Ermittlungen zu Cyberattacken müssten am Ende Indizien interpretiert werden. Dies bedarf natürlich einer Unabhängigkeit der Untersuchungsbehörde. Zudem wird das schwammige Verhältnis des BSI zu den polizeilichen Sicherheitsbehörden und den Geheimdiensten von der