Dennis-Kenji Kipker, Dario E. Scholz

Das IT-Sicherheitsgesetz 2.0

Eine kritische Analyse

Am 5. Mai 2020 wurde ein neuer Referentenentwurf des IT-Sicherheitsgesetzes 2.0 veröffentlicht. Die wesentlichen Änderungen im Vergleich zum ersten Entwurf aus dem Jahr 2019 werden im Rahmen dieses Beitrages einer rechtlichen sowie rechtspolitischen Analyse und Bewertung unterzogen.

1 Einleitung

Am 5.5.2020 wurde ein neuer Referentenentwurf des IT-Sicherheitsgesetzes 2.0 veröffentlicht,[1] der bereits mehrfach Gegenstand juristischer Erörterung war.[2] Zusammengefasst sollen durch das Gesetz Änderungen und Erweiterungen von BSIG, TKG, TMG und der AWV vorgenommen werden. Vielfach diskutierte Regulierungsvorschläge sind dabei v. a. die Ergänzung des KRITIS-Sektors „Entsorgung", die Einführung der neuen Kategorie „Unternehmen im besonderen öffentlichen Interesse" und von „Garantieerklärungen für Kritische Komponenten". Überdies sind eine Fülle an Kompetenz- und Aufgabenerweiterungen des BSI und die Schaffung eines nationalen IT-Sicherheitskennzeichens vorgesehen. Anliegen dieses Beitrags ist eine rechtliche und rechtspolitische Analyse und Bewertung der wesentlichen Änderungen durch den aktuellen Entwurf des IT-SiG 2.0 im Vergleich zum ersten Entwurf aus dem Jahr 2019. Vorgezogen und erwähnenswert ist an dieser Stelle – wie auch bei der Diskussion um Änderungen zum NetzDG bezüglich des Umgangs mit Hassrede und Rechtsextremismus[3] – die noch fehlende Evaluierung der Wirksamkeit des bisherigen „IT-SiG 1.0", weshalb die Gesetzesbegründung und Kritik daran mangels Evidenz-Erhebung häufig einer gesicherten Erkenntnisgrundlage entbehren.[4] Gerade für die rechtspolitische Bewertung des IT-SiG 2.0 wäre eine solche, dem Gesetzgebungsprozess vorgelagerte Untersuchung zielführend und könnte der „Erforderlichkeitsfrage" hinsichtlich einiger vorgesehener Regelungen die Antwort liefern.

1 Referentenentwurf des IT-Sicherheitsgesetzes 2.0, abrufbar unter: https://intrapol.org/wp-content/uploads/2020/05/200507_BMI_RefE_IT-SiG20.pdf (Stand 9.9.2020); fortan als RefE zitiert.

2 Zusammenfassungen der inhaltlichen Änderungen beispielsweise bei *Kipker*, MMR-Aktuell 2020, 429348.

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen.

E-Mail: kipker@uni-bremen.de

Dario E. Scholz

Wissenschaftlicher Mitarbeiter am IGMR und Mitglied im Vorstand des Legal Future e.V.

E-Mail: dario.scholz@uni-bremen.de

2 Aufgaben und Befugnisse des BSI

Der aktuelle Gesetzentwurf sieht für das BSI eine Reihe neuer Aufgabenzuweisungen und Befugniserweiterungen vor. Zu nennen sind v. a. die Tätigkeit des BSI als Konformitätsbewertungsstelle nach § 3 Abs. 1 S. 2 Nr. 5a BSIG-E sowie als nationale Behörde für die Cybersicherheitszertifizierung gem. § 3 Abs. 1 S. 2 Nr. 5b BSIG-E, wobei letzteres der Ausgestaltung des Art. 58 der Verordnung (EU) 2019/881 vom 17. April 2019 (EU Cybersecurity Act) dienen soll[5] und sich grundsätzlich in die Cybersicherheitsstrategie der Bundesregierung einfügt[6]. In § 3 Abs. 1 S. 2 Nr. 19 und 20 BSIG-E wird dem BSI zudem die Entwicklung und Bewertung von Identifizierungs- und Authentisierungsverfahren einerseits und die Entwicklung und Veröffentlichung eines Stands der Technik bezüglich IT-sicherheitstechnischer Anforderungen von IT-Produkten andererseits als Aufgabe übertragen. Diese Übertragung wirft zunächst die Frage der Überschneidung mit Art. 42, 32 und 57 EU-DSGVO und des Anwendungsbereichs der EU eIDAS-VO auf. Die Gesetzesbegründung versteht § 3 Abs. 1 S. 2 Nr. 19 BSIG-E dabei als Klarstellung und Konkretisierung der eIDAS-VO auf nationaler Ebene. Der Gesetzgeber scheint keine

3 *Liesching*, Karneval der Jakobiner: „Zum Schutze der Freiheit – Schafft sie ab!", abrufbar unter: https://community.beck.de/2020/01/06/karneval-der-jakobiner-zum-schutze-der-freiheit-schafft-sie-ab (Stand 9.9.2020).

4 https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/ (Stand 9.9.2020); vgl. auch RefE, S. 40.

5 RefE, S. 42.

6 Cybersicherheitsstrategie 2016 des Bundes, S. 10 ff. abrufbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Stand 9.9.2020).

Probleme hinsichtlich des Anwendungsbereichs zu sehen.[7] Ungeklärt bleibt in dem Gesetzentwurf bisher hingegen, inwiefern das BSI nun hinsichtlich dieser Aspekte neben die bisher bestehenden datenschutzrechtlichen Behörden tritt und wie die Zertifizierung im Verhältnis zur Zertifizierung i. S. d. Art. 42 DSGVO stehen soll.

Auch die Entwicklung und Festlegung des Stands der Technik durch das BSI, der z. B. für die Pflichten von Kritischen Infrastruktur-Betreibern nach § 8a BSIG-E relevant wird, bietet weiter Angriffsfläche für Kritik. Der Referentenentwurf führt in der Begründung dazu aus, dass die Entwicklung des Stands der Technik in Verbindung mit der Konformitätsprüfung durch das BSI zum Zwecke des Verbraucherschutzes unerlässlich sei und so einheitliche Maßgaben geschaffen werden könnten.[8] Problematisch ist an dieser Konzeption, dass die Betreiber, die nach § 8a BSIG zur Einhaltung des Standes der Technik bei ihren IT-Sicherheitsvorkehrungen verpflichtet sind, direkt nicht zwingend in den Entwicklungsprozess des BSI eingebunden sind.[9] Auch die Beachtung internationaler Standards wird, jedenfalls unmittelbar dem Entwurf zufolge, nicht fest in den Entscheidungsprozess des BSI eingebunden, sodass sich jedenfalls aus rechtspolitischer und wirtschaftlicher Sicht das Problem der Zersplitterung der IT-Sicherheitsregulierung stellt.[10] Daran anknüpfend erscheint zumindest eine wesentliche Einbindung der Kritischen Infrastruktur-Betreiber in den Entwurfsprozess ratsam.

Zudem stellt sich die Frage der Notwendigkeit solcher nationalen Festlegungen des Stands Technik angesichts vielfältig bestehender technischer Normung auf internationaler Ebene. Rechtlich ist dies nicht zu beanstanden; rechtspolitisch wäre es durchaus wünschenswert, ein Rahmensystem zu schaffen, das eine derartige Zersplitterung der IT-Sicherheitsregulierung möglichst verhindert, auf bestehende internationale Normung zurückgreift und so Doppelaufwände vermeidet.

Überdies wird in § 4b BSIG-E vorgeschlagen, auch die Funktion des BSI als allgemeine Meldestelle für IT-Sicherheit auszubauen, wobei Abs. 3 die Möglichkeit der Weitergabe von erhaltenen Informationen regelt. Möglich ist dabei auch die Berichterstattung an die Bundesbehörde, was erneut die Forderung nach einer größeren institutionellen Unabhängigkeit des BSI unter Beachtung seiner allgemeinen Rolle in der IT-Sicherheitslandschaft in Deutschland laut werden lässt. Zudem ist Absatz 3 bisher als „Kann"-Vorschrift ausgestaltet. Damit die Cybersicherheit in Deutschland durch die Arbeit des BSI jedoch tatsächlich effektiv gestärkt wird, sollte die Meldung bedeutender Informationen an die dafür relevanten Akteure nicht im Ermessen des BSI stehen.

Wie auch der erste Entwurf sieht das IT-SiG 2.0 im BSIG Regelungen zu Krisenreaktionsplänen vor. Diese werden in § 5c BSIG-E als „Gesamtplan für Reaktionsmaßnahmen des Bundes" bezeichnet und durch das BSI im Einvernehmen mit dem BBK und den jeweiligen Aufsichtsbehörden entwickelt. Zu den betroffenen Betreibern von Kritischen Infrastrukturen, Unternehmen von besonderem öffentlichen Interesse und den Lieferanten von Kritischen Komponenten wird allerdings nur Benehmen hergestellt; gleichwohl wird diesen dadurch die Möglichkeit gegeben, ihre häufig schon aus wirtschaftlichem Eigeninteresse erstellten Krisenreaktionspläne in den Prozess einzubringen und ihre detaillierten Kenntnisse über ihre eigenen IT-Systeme auf diese Weise fruchtbar zu machen. Ohne hinreichende Einbindung der Betreiber wäre die Geeignetheit der extern durch das BSI entworfenen Krisenreaktionspläne fraglich, da die IT-Systeme solcher Unternehmen notwendigerweise komplex und von einer zur anderen Infrastruktur verschieden sind. Ohne solche Betreiber-Beteiligung ist eine effiziente Ausgestaltung von Krisenreaktionsplänen kaum denkbar. Insoweit dürfte aber, was angesichts einiger IT-Sicherheitsvorfälle ohne adäquate Reaktion von Wirtschaftsunternehmen[11] kaum bestreitbar ist, die Erforderlichkeit dieser Regelung jedenfalls unter der Einschätzungsprärogative des Gesetzgebers nicht anzugreifen sein.

Die in § 5c Abs. 4 BSIG-E vorgeschlagene Befugnis des BSI greift überdies schwerwiegend in unternehmenseigene Prozesse ein. Demgemäß hat das BSI für Fälle einer erheblichen Störung i. S. d. § 8b BSIG u. a. ein Anforderungsrecht für bestimmte (auch personenbezogene) Daten und eine Eingriffsbefugnis in die Systeme und unternehmerischen Prozesse dahingehend, dass das BSI informationstechnische Maßnahmen zur Wiederherstellung der Funktionsfähigkeit und Sicherheit der Systeme anordnen darf, wenn der Betroffene die Störung nicht selbst behebt bzw. beheben kann.

Prima facie ließe sich die Herausgabepflicht bezogen auf die zur Bewältigung der Störung erforderlichen Daten dahingehend kritisieren, dass diese durch den Wortlaut nicht weiter eingegrenzt werden und auch in der Gesetzesbegründung keine Abwägung mit den Interessen Dritter angedacht ist.[12] Dem ist indes zu entgegnen, dass es sich um eine Ermessensentscheidung des BSI handelt. Diese muss zwangsläufig eine Abwägung mit rechtlich geschützten Interessen der Betroffenen beinhalten.[13]

Problematisch ist dagegen das Recht des BSI zur „Selbstvornahme" der erforderlichen Maßnahmen, da die bereits von den Betreibern erarbeiteten Reaktionspläne teils selbst Gegenstand erfolgreicher Zertifizierungsverfahren sind und regelmäßig internationalen Standards wie beispielsweise ISO/IEC 27001 entsprechen. Zudem lässt sich gegen die Eingriffsbefugnis anführen, dass Betreiber von Kritischen Infrastrukturen ein eigenes Interesse an der raschen Wiederherstellung der Funktionsfähigkeit ihrer Systeme haben, wobei dieses Argument dadurch insoweit an „Schusskraft" verliert, als dass das BSI solche Anordnungen nur treffen darf, wenn eine rechtzeitige Reaktion durch den Betreiber nicht möglich oder zu erwarten ist; eine Unverhältnismäßigkeit ist jedenfalls deshalb nicht zu begründen. Auch lässt sich gegen die Eingriffsbefugnis rechtlich – wie aber teils angenommen[14] – ebenso wenig anführen, dass keine spezielle Haftungsregelung für Anordnungen des BSI eingeführt wird. Ein Ausgleich lässt sich im Haftungsfall durch die (überwiegend richterrechtlich anerkannten) Instrumente des Staatshaftungsrechts gewähr-

7 RefE, S. 45.

8 RefE, S. 45.

9 BDEW, Stellungnahme zum RefE, S. 5, abrufbar unter: https://www.bdew.de/media/documents/Stn_20190902_Referentenentw-eines-Zweiten-Gesetzes-zur-Erhoehung-der-Sicherhei_VGEO79v.pdf (Stand 9.9.2020).

10 VDE-Stellungnahme zum RefE, abrufbar unter: https://www.vde.com/topics-de/digital-security/aktuelles/cybersecurity-recht/stellungnahme-it-sig-2-0-mai-2020 (Stand 9.9.2020); fortan als VDE-Stellungnahme zitiert.

11 Vgl. z. B. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2018, 13.

12 BDI, Stellungnahme zum RefE, S. 25, abrufbar unter: https://bdi.eu/media/themenfelder/digitalisierung/publikationen/20200703_BDI_Stellungnahme_IT-SiG.pdf (Stand 9.9.2020), fortan als BDI zitiert.

13 Vgl. *Sachs,* in: Stelkens/Bonk/Sachs VwVfG, 9. Auflage 2019, § 40 Rn. 82 ff.

14 Stellungnahme des BDI zum ursprünglichen RefE von 2019, S. 16, abrufbar unter: https://bdi.eu/media/user_upload/20190628_Stellungnahme_BDI_IT-SiG_2.0-Leak.pdf (Stand 9.9.2020).

leisten. Das Nichtvorhandensein einer ausdrücklichen Regelung ist daher zwar aus unternehmerischer Sicht durchaus zu missbilligen, entspricht jedoch der bisherigen Handhabung potentieller Haftungsfälle durch den Gesetzgeber.

In den Medien mehrfach aufgegriffen wurde zudem § 7b BSIG-E als sog. „Hackerparagraf", der dem BSI die Detektion von Sicherheitslücken in öffentlich erreichbaren Systemen ermöglicht und dieses so umgangssprachlich zur „Hackerbehörde" qualifiziert.[15] Definiert wird dazu in § 7b Abs. 2 BSIG-E, wann ein solches System ungeschützt ist; eine Definition des Begriffs des „öffentlichen Zugangs" lässt der Entwurf dagegen vermissen. In diesem Zusammenhang muss auch der § 7a BSIG-E als Untersuchungs- und Auskunftsanspruch des BSI gegenüber den jeweiligen Unternehmen gesehen werden, wobei auch hier als Ermessenvorschrift die Interessen der Unternehmen und etwaiger Dritter, auch bezogen auf Geschäftsgeheimnisse, gewahrt werden können. Wünschenswert ist in diesem Zusammenhang, dass gesonderte Sicherheitsanforderungen an das Übermittlungsverfahren normiert werden. Die Befugnis zur Detektion von Sicherheitslücken in öffentlich erreichbaren Systemen soll nur bestehen, um den Betreiber auf etwaige Sicherheitslücken hinzuweisen und diesen darüber zu informieren, wobei v. a. Portscans, Sinkholes und Honeypots eingesetzt werden sollen.[16] Insbesondere Penetrationstests und Red-Teaming-Aktivitäten werden jedoch nicht explizit ausgeschlossen, obwohl diese die Kritische Infrastruktur selbst gefährden können und damit die Sicherheit nicht zwangsweise erhöhen, sondern unter Umständen selbst eine Gefahr begründen.[17] Denkbar wäre hier, dieses Risiko eines Ausfalls durch eine etwaige Ankündigungspflicht des BSI zu minimieren.[18]

3 Pflichten für Betreiber

Auch für Betreiber Kritischer Infrastrukturen sollen neue Pflichten Einzug in das BSIG finden. § 8a Abs. 1a, c BSIG-E beinhaltet die Pflicht zur Implementierung eines Systems zur Angriffserkennung mit dem Ziel der Störungsvermeidung, wobei dabei anfallende Daten, die zur Aufklärung und Strafverfolgung eines Angriffs erforderlich sind oder dem Schutz vor Angriffen dienen, an das BSI gemeldet werden sollen.

Gem. § 8a Abs. 3 S. 4 BSIG-E soll überdies eine Liste aller IT-Produkte mit Bedeutung für die Funktionsfähigkeit der Kritischen Infrastruktur an das BSI übermittelt werden. Aus Gesetzentwurf und Begründung geht dabei aber nicht hervor, wofür diese Liste konkret genutzt werden soll. Angesichts dieser „Grundlosigkeit" der Akkumulation von sensiblen Inhalten beim BSI, wird letztlich eine eigene Gefahrenquelle geschaffen, die die Behörde damit noch stärker als bisher selbst zu einer „Zielscheibe" etwaiger Cyberangriffe machen könnte. Von datenschutzrechtlichen Bedenken einmal abgesehen, sollte angesichts dieser Gefahr jedenfalls die Aufnahme einer Regelung der IT-sicherheitsrechtlichen Anforderungen an das BSI selbst angedacht werden. Sinnvoller als eine entschärfte Datenübermittlung ist natürlich, eine Datenübermittlung gar nicht erst einzuführen. Im Rahmen von ISMS-Systemen, die bereits jetzt zum Stand der Technik im Adressatenkreis des Gesetzes gehören, müssen sich Kritische Infrastruktur-Betreiber in der Regel ihrer Komponenten, Strukturen und Prozesse bewusst sein, sodass die Zusammenstellung der Liste für die Unternehmen selbst keinen nennenswerten Mehrwert bieten dürfte. Die Zusammenstellung der genutzten IT-Produkte ist jedenfalls auch ein potenzielles Geschäftsgeheimnis, sodass eine anlass- und grundlose Übermittlung den Unternehmen auch unter diesem Gesichtspunkt nicht zumutbar ist.

In § 2 Abs. 14 BSIG-E plant der Gesetzgeber zudem eine neue Kategorie von Unternehmen neben den Kritischen Infrastrukturen in das BSIG aufzunehmen: die sog. „Unternehmen in besonderem öffentlichen Interesse". Bereits im ersten Entwurf aus dem Jahr 2019 war die Erweiterung der für Kritische Infrastrukturen bestehenden Regelungen auf weitere Unternehmen angedacht, jedoch wies der damalige Entwurf diesbezüglich keine klare Definition auf.[19] Der neue Entwurf unterscheidet in den § 2 Abs. 14 Nr. 1-3 BSIG-E der Nummerierung nach drei unterschiedliche Kategorien solcher Unternehmen: Rüstungs- und Raumfahrtunternehmen, die über einen Verweis in das AWV aufgenommen werden; Unternehmen, die „aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind"; sowie vermittels eines Verweises in die Gefahrstoffverordnung (Gefahrstoff-VO) Chemieunternehmen. Unternehmen der zweiten Gruppe sollen im Rahmen einer Rechtsverordnung näher bestimmt werden. Für die Einbeziehung dieser Unternehmen bestehe für Teile der Anforderungen und Pflichten von Kritischen Infrastrukturen ein Bedürfnis, da es für deren besondere Sicherheit – auch ohne gesetzlich definierte Kritische Infrastruktur zu sein – ein erhebliches gesellschaftliches Interesse gebe.[20] Aus dem Entwurf ergibt sich dabei in Summe, dass vorgenannte Unternehmen im Vergleich zu Kritischen Infrastrukturen minimal niedrigeren Anforderungen unterliegen. Beispielsweise besteht nach § 8f BSIG für die ersten beiden Subkategorien die Pflicht, alle zwei Jahre ein IT-Sicherheitskonzept vorzulegen, wobei allerdings seitens des BSI kein tiefgreifendes Audit erfolgt, sondern nach § 8f Abs. 3 BSIG-E lediglich Hinweise erteilt werden. Auch eine Meldepflicht für Störungen, wie sie vergleichbar für Kritische Infrastrukturen existiert, wird durch § 8b Abs. 4a, b BSIG-E auf die Unternehmen im öffentlichen Interesse ausgeweitet, wobei zur Auslösung der Meldepflicht für die verschiedenen Subkategorien der Unternehmen unterschiedliche Voraussetzungen bestehen. Eine anonyme Meldung ist dabei allerdings, ohne weitere Begründung im Gesetzentwurf und anders als bei Kritischen Infrastrukturen, nicht vorgesehen.

Auch bei diesem Versuch, die Pflichten aus dem BSIG auf weitere Unternehmen jenseits der klassisch verstandenen Kritischen Infrastruktur auszuweiten, bestehen erneut Abgrenzungsschwierigkeiten. Zwar erfolgt nun eine prima facie präzise Definition der Unternehmen im besonderen öffentlichen Interesse, allerdings ist diese nun mit bisher unbekannten Rechtsbegriffen, v. a. der „volkswirtschaftlichen Bedeutung", geprägt. Ohne Abwarten der zugehörigen Rechtsverordnung ist so keine genaue Bestimmung der Unternehmen der zweiten Gruppe möglich. Angesichts der im Rahmen der Covid-19-Beschränkungen hervor-

15 https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/;
https://www.br.de/nachrichten/netzwelt/it-sicherheitsgesetz-2-0-bsi-soll-aufgeruestet-werden,Rys3BIX (Stand 9.9.2020).

16 RefE, S. 51 f.

17 MMR-Aktuell 2020, 429792; BDI, S. 29.

18 BDI, S. 30.

19 *Kipker/Scholz,* MMR 2019, 431 (433 f.).

20 RefE, S. 41 f.

getretenen systemrelevanten Berufe und Arbeitgeber erscheint eine Abgrenzung besonders schwierig dahingehend, dass eine Vielzahl an Berufen und Diensten jedenfalls eine gewisse volkswirtschaftliche Bedeutung mit sich bringt, ohne selbst Kritische Infrastruktur zu sein.[21] Unbefriedigend und eventuell ungewollt scheint auch der Verweis auf die GefahrstoffVO für Unternehmen der dritten Gruppe, da unter Umständen auch kleine Betriebe, die Reinigungsmittel am Arbeitsplatz verwenden, einer Regulierung durch die GefahrstoffVO unterfallen und damit potenziell durchaus Unternehmen im besonderen öffentliche Interesse gemäß der dritten Gruppe sein können. Solche Fälle ließen sich i. e. L. dadurch vermeiden, indem der Verweis statt auf die GefahrstoffVO auf die StörfallVO gelegt wird, die sich in ihrer Anwendbarkeit gerade auch auf bestimmte mengenmäßige Schwellen von Gefahrenstoffen bezieht.[22]

Zudem stellt sich, Kapazitätsgründe außer Acht gelassen, die Frage, warum gerade kleinere Betriebe, die selbst tendenziell weniger finanzielle und Know-How-technische Ressourcen zur Verfügung haben, nicht die Möglichkeit eröffnet bekommen, Hinweise zu ihren Sicherheitskonzepten durch das BSI zu erhalten. Diese, auf die Sinnhaftigkeit der Regelung bezogene Frage, stellt sich in abgewandelter Form auch für die Existenz der neuen Unternehmenskategorie. Denn im Wesentlichen bestehen viele der (ressourcenintensiven) Pflichten und Aufgaben von Kritischen Infrastrukturen auch für diese. Ohne klare Grenzziehung des potenziell weiten Verständnisses durch eine Rechtsverordnung droht jedenfalls für kleinere Betriebe bei Zugehörigkeit zu dieser Unternehmenskategorie die Überforderung mit den neuen Pflichten und Aufgaben. Im Übrigen ist eine Ausgestaltung durch untergesetzliche Normen wie der Rechtsverordnung auf ein erforderliches Minimum zu reduzieren und stattdessen nach Möglichkeit im Gesetz selbst mehr Klarheit und die damit notwendige Rechtssicherheit zu schaffen.[23]

4 Regulierung der Hersteller

Auch steht neuerdings im Entwurf zum IT-SiG 2.0 die Regulierung der IT-Hersteller im Fokus. Durch § 9a BSIG-E soll, wie bereits in der ersten Entwurfsfassung angedacht, ein nationales und freiwilliges IT-Sicherheitskennzeichen für Hersteller von IT-Produkten eingeführt werden. Für die Herstellerdefinition wird auf § 2 Abs. 1 Nr. 14 des ProdSG verwiesen. Nach abgegebener Herstellererklärung ist daraufhin eine Plausibilitätsprüfung durch das BSI und die regelmäßige Überprüfung der Vorgaben durch die Behörde vorgesehen. Letztendlich wird damit in Abgrenzung zur Zertifizierung nach EU CSA auf der Stufe „niedrig" und/oder auf Basis einer Konformitätserklärung des Herstellers eine weitere „Zertifizierungsinstanz" geschaffen, die neben eine europäisch induzierte Zertifizierung tritt und ebenfalls maßgeblich auf der Erklärung des Herstellers aufbaut. Problematisch ist in diesem Zusammenhang auch, dass das BSI als Stelle für Konformitätsbewertungen i. S. d. § 3 Abs. 1 S. 5a BSIG-E eingerichtet wird, obwohl die Erteilung durch eine Behörde nach Art. 56 CSA nur für das Sicherheitsniveau „hoch" – bis auf wenige Ausnahmen – vorgesehen ist. Letzten Endes wird hier ebenso die Kompetenz des BSI in größerem Umfang als nötig erweitert und um ein „Sicherheitskennzeichen" ergänzt. Dabei stellt sich erneut die Frage der Sinnhaftigkeit eines freiwilligen nationalen Sicherheitskennzeichens, das laut Gesetzentwurf auch dem Verbraucherschutz zuträglich sein soll,[24] gleichzeitig aber in Konkurrenz zur europäischen Zertifizierung mehr Verwirrung beim Verbraucher stiften könnte. Im Übrigen droht durch die „Nationalisierung" der Zertifizierung eine – auch gegen die EU Cybersicherheitsstrategie gerichtete – Zersplitterung der IT-Sicherheitslandschaft in Europa, ohne dass dadurch letztendlich ein Mehrwert für Unternehmen und Verbraucher geschaffen wird.[25] Die damit einhergehende Unklarheit wird für das IT-Sicherheitskennzeichen überdies durch mehrere Verweise auf die Ausgestaltung durch Rechtsverordnung für Unternehmen zu einem bis dato kaum kalkulierbarem Aufwandsposten.

Wie zuvor bereits im Rahmen des § 8a Abs. 3 S. 4 BSIG-E dargelegt, müssen Betreiber von Kritischen Infrastrukturen die für den Betrieb ihrer Infrastruktur relevanten IT-Produkte an das BSI melden. Wird für eine Kritische Komponente durch ein gesondertes Gesetz die Zertifizierung zur Pflicht, muss der Betreiber der Kritischen Infrastruktur die (potenzielle) Nutzung der Komponente überdies dem BMI anzeigen, siehe § 9b BSIG-E. Neben die Anzeige und die angeordnete Zertifizierung tritt zudem die Einholung einer Garantieerklärung des Herstellers, die sich gem. § 9b Abs. 2 BSIG-E auf die gesamte Lieferkette des Produktes beziehen muss. Was eine Kritische Komponente in diesem Sinn ist, wird in § 2 Abs. 13 BSIG-E definiert. Ein Teil der Definition rekurriert dabei auch auf die Gefahr für die öffentliche Sicherheit durch Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte oder darauf, ob die Kritische Infrastruktur selbst durch das Produkt gefährdet wird. Wie weitreichend der Begriff der Lieferkette tatsächlich zu verstehen ist, wird jedoch nicht dargestellt.

Ferner ist die Verwendung von Komponenten von ausschließlich vertrauenswürdigen Herstellern im Grunde zwar eine notwendige und sinnvolle Konzeption, da insbesondere auch die Hersteller und nicht nur Betreiber adressiert werden, allerdings besteht bei Ausgestaltung als Garantieerklärung durch die Hersteller die Gefahr, dass diese eine solche ausstellen, ohne dass die Voraussetzungen dafür tatsächlich vorliegen.[26] Dies wird insbesondere relevant durch die Erstreckung der Pflicht auf die gesamte Lieferkette, welche in der Nachvollziehung im globalen Geflecht mit großem Aufwand und Unsicherheit für die Unternehmen verbunden ist – und das bis hin zur faktischen Unmöglichkeit.[27] Durch die Ausdehnung der Pflicht auf die gesamte Lieferkette des Herstellers besteht zudem die Gefahr, dass, jedenfalls mittelbar, viele Anforderungen des BSIG auch auf nicht-kritische Unternehmen und Unternehmen, die nicht in besonderem öffentlichen Interesse stehen, bezogen werden. Zudem besteht das Problem, dass z. B. bei der Verwendung von (kollaborativ entwickelten) Open-Source-Produkten regelmäßig kein einzelner Hersteller existiert und damit in strenger Auslegung eine Verwendung solcher Software in diesen Konstellationen unmöglich würde.[28]

In § 9b Abs. 3 BSIG-E ist zudem unter weiteren Voraussetzungen die Untersagung des Einsatzes solcher Komponenten gere-

21 BDI, S. 37.
22 BDI, S. 17.
23 Vgl. *Kipker/Scholz*, MMR 2019, 431 (433).
24 RefE, S. 44.
25 BDI, S. 37f.
26 BDI, S. 39.
27 BDI, S. 39.
28 VDE-Stellungnahme; BDI, S. 39.

gelt. Wer die Kosten für den Austausch der untersagten Komponenten trägt, ist nicht explizit geregelt. Besonders strittig ist dies hinsichtlich von vor der Untersagung oder dem Inkrafttreten des Gesetzes eingebauten Komponenten.[29]

Denkbar wäre in diesem Fall die Lösung über einen – womöglich eingeschränkten und vorübergehenden – Bestandsschutz. Eine andere Möglichkeit der Ausgestaltung könnte in der Bestimmung einer Frist zum Austausch zu sehen sein. Ansonsten besteht das Problem einer faktischen Rückwirkung, die insbesondere kleinere Betreiber aus kostentechnischer Sicht existenziell treffen könnte. In diesem Zusammenhang wäre eine Milderung auch dadurch zu erreichen, dass die Pflicht zur Kostentragung bei Untersagung des Einsatzes explizit den Herstellern auferlegt würde und insoweit für die Betreiber keine weitere Unsicherheit bestünde.

Auch hier stellt sich aber erneut die Frage, ob die Einführung dieses Verbotsvorbehalts der Verwendung von IT-Komponenten angesichts der Entwicklungen auf europäischer Ebene tatsächlich zielführend ist. Der Gesetzesbegründung nach wurde der § 9b BSIG-E gerade auch deshalb angedacht, um der Diskussion und Problematik über „5G-Sicherheit" unter Hinzuziehung ausländischer Ausrüster wie Huawei Herr zu werden und einer rein technischen Zertifizierung, wie sie auch im EU CSA europäisch verfolgt wird, ein nationales Gewicht entgegenzusetzen, das die technische Sicht noch um die „Vertrauensfrage" erweitert und nicht an die Anerkennung der Zertifizierung in einem anderen EU-Mitgliedsstaat gebunden ist.[30]

5 Verbund der neuen Aufgaben und Kompetenzen – mehr Unabhängigkeit für das BSI

Auch aus der Gesamtschau der zuvor untersuchten Änderungen ergeben sich weitere Anknüpfungspunkte zur Kritik am gegenwärtigen Entwurf zum IT-SIG 2.0.

So soll das BSI eine noch bedeutendere Rolle als bisher einnehmen, sowohl als Aufsichtsbehörde als auch auf Regulierungs- und Standardisierungsebene, über den gesamten Produktkreislauf von Herstellern, über Intermediäre, bis hin zu den Betreibern als Nutzer solcher Produkte. Das BSI würde daher noch mehr als zuvor zur zentralen „Sammelstelle" IT-sicherheitsrelevanter Daten von Kritischen Infrastruktur-Betreibern und anderen Unternehmen werden.[31] An verschiedenen Stellen im IT-SiG 2.0 werden überdies Weiterleitungspflichten und Anforderungsermächtigungen für andere Bundesbehörden geschaffen, so beispielsweise in § 4b Abs. 3 BSIG-E hinsichtlich gemeldeter Schwachstellen. Weiter intensiviert wird dieses Problem auch im Rahmen der „Hacking-Befugnisse", spätestens in Gesamtbetrachtung zusammen mit § 7c BSIG-E, wonach das BKA über das BSI durch die Offenlegung von Schwachstellen Unterstützung zum Schutz von Mitgliedern der Verfassungsorgane erhalten kann. Dies ist widersprüchlich, da dem BSI gerade die gesetzlich normierte Zwecksetzung einer Stärkung der IT-Sicherheit zukommt. Der Widerspruch wiegt umso schwerer, als dass mit der Übermittlung einer Liste von genutzten IT-Produkten ohne Nennung eines signifikanten Grundes,[32] aber auch im Rahmen der anderen Aufgaben und Befugnisse des BSI, besonders sicherheitsrelevante und teils im Rahmen von Geschäftsgeheimnissen geschützte Daten akkumuliert werden. Zentrales Problem im IT-SiG 2.0 ist in diesem Zusammenhang weiterhin, dass das BSI der Rechts- und Fachaufsicht durch das BMI untersteht. Das führt angesichts ausführlicher Befugnisse und der Rolle des BSI als die IT-Sicherheit stärkende Behörde fast zwangsläufig zu Interessenskonflikten. Angesichts der Mitarbeit des BSI auf Weisung des BMI u. a. am Bundestrojaner[33] sind solche Befürchtungen auch nicht durch Verweis auf eine lediglich abstrakte Gefahr von der Hand zu weisen, oder durch eine lediglich innere Ressorttrennung innerhalb des BMI zu entkräften. Im Ergebnis droht durch den zunehmenden Befugnisausbau folglich die Gefahr einer Zwitterstellung des BSI.[34] Der Unabhängigkeit der Behörde förderlich wäre es demgegenüber, wenn dem BMI lediglich die Rechtsaufsicht über das BSI zukäme, und damit keine inhaltliche Weisungsbefugnis mehr bestünde. Alternativ denkbar wäre auch die Ausgliederung des BSI aus dem zuständigen Ressort des BMI heraus hin zu einer selbstständigen obersten Bundesbehörde.

6 Neue Pflichten der TK- und TM-Diensteanbieter

Der neue § 109 Abs. 2 TKG-E bestimmt u. a. eine Zertifizierungspflicht für bestimmte Telekommunikationstechnik und führt damit gleichzeitig zur Vertrauenswürdigkeitsprüfung durch das BSI. Er ist dabei, im Zusammenspiel mit § 9b BSIG-E, ebenfalls als Reaktion auf die auch in Deutschland geführte 5G-Debatte um den chinesischen TK-Ausrüster Huawei und dessen Vertrauenswürdigkeit zu sehen.[35]

Neben einigen weiteren Änderungen wird zudem mit § 109a Abs. 1a TKG-E und § 15 Abs. 2 S. 2 TMG-E für Telekommunikations- und Telemediendienstanbieter eine Melde- und Übermittlungspflicht dahingehend eingeführt, dass diese den Sachverhalt zu unrechtmäßigen Übermittlungen an oder unrechtmäßigen Kenntniserlangungen von Daten durch Dritte unverzüglich an das BKA melden müssen, wenn Tatsachen die Annahme rechtfertigen bzw. darauf hindeuten, dass dies nicht fahrlässig erfolgte und dafür die Systeme der Anbieter ohne Erlaubnis oder Billigung verändert wurden, darauf eingewirkt wurde oder Zugangseinrichtungen überwunden wurden. Problematisch an der Meldepflicht ist zuvorderst deren verfassungsrechtliche Zulässigkeit.[36] Ein Verstoß gegen das Bestimmtheitsgebot, abgeleitet aus Art. 20 Abs. 3 GG, ist indes nicht ersichtlich: Der Gesetzgeber darf unbestimmte Rechtsbegriffe verwenden, wobei die zulässige Grenze erst überschritten wird, soweit sich die verwendeten Begriffe nicht mehr mit den Mitteln der Gesetzesauslegung bestimmen lassen.[37] Das ist hier indes nicht der Fall. Letztlich lassen sich die Begriffe der „Tatsachen, die die Annahme rechtfer-

29 BDI, S. 42 f.

30 RefE, S. 59 f.

31 Vgl. https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/ (Stand 9.9.2020).

32 BDI, S. 32.

33 Z. B. https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/ (Stand 9.9.2020).

34 Vgl. auch MMR-Aktuell 2020, 429792.

35 https://www.cr-online.de/blog/2020/06/15/it-sicherheitsgesetz-2-0-neuer-entwurf-veroeffentlicht/ (Stand 9.9.2020).

36 BDI, S. 47 f.

37 In diese Richtung auch *BVerfG*, NJW 2004, 2213 (2216).

tigen", verbunden mit dem Begriff der „hinreichenden Anhaltspunkte" in § 149 Abs. 1 Nr. 21g TKG-E für die Strafbewährung der Unterlassung, mit den herkömmlichen Auslegungsmethoden und unter Einbeziehung der verfassungskonformen Auslegung in einem ausreichenden Mindestmaß bestimmen. Dabei ist auch zu berücksichtigen, dass sich gerade im Zusammenhang zu den Landespolizeigesetzen eine ausgeprägte Judikatur zum „Gefahrenverdacht" herausgebildet hat,[38] die ggf. zur Konkretisierung der Rechtsbegriffe herangezogen werden kann und Unternehmen so jedenfalls nicht vor unbestimmbare Herausforderungen stellt.

Außerdem bezieht sich weitere Kritik an der Meldepflicht darauf, dass so eine Auslagerung der Strafverfolgung an TM- und TK-Dienstanbieter erfolge.[39] Diese werden auf Basis ihrer eigenen Rechtmäßigkeitseinschätzung zur Meldung des Sachverhalts an das BKA verpflichtet und seien damit zur Verdachtsgewinnung zentrale Instanz – letztendlich drohe also das Outsourcing einer hoheitlichen Aufgabe. In dieser Auslagerung wird teils eine unrechtmäßige Abkehr von der bisherigen Konzeption einer strafrechtlichen Anzeigepflicht lediglich bei besonders gravierenden Delikten gesehen.[40] Entkräftet werden kann diese Kritik dabei jedoch nicht einfach durch einen Vergleich zu § 138 StGB als zweifelsfrei verfassungsgemäße Norm, da diese die unterlassene Anzeige im Bereich der präventiven Gefahrenabwehr bestraft.[41] Die hier diskutierte Meldepflicht hat aber die repressive Gefahrenbekämpfung zum Ziel und ist deswegen vom Sinn und Zweck her nicht damit vergleichbar. Als dogmatischer Anknüpfungspunkt für die Kritik der unrechtmäßigen Übertragung von Hoheitsbefugnissen kommt dabei, neben dem allgemeinen Rechtsstaatsprinzip, v. a. der Funktionsvorbehalt aus Art. 33 Abs. 4 GG in Betracht.[42]

Hoheitliche Befugnisse i. S. d. Art. 33 Abs. 4 GG liegen v.a. dann vor, wenn wesentliche Entscheidungen des Gesetzgebers im Sinne der Wesentlichkeitstheorie vollzogen werden und diese grundrechtsrelevant sind; eine Beschränkung auf Fälle der Eingriffsverwaltung ist dabei freilich nicht geboten.[43] Aus Literatur und Rechtsprechung lässt sich dazu entnehmen, dass die „systematische Aufklärung von Verstößen [gegen das OWIG/StVG] durch Private"[44] über das jedem zustehende Recht der Anzeigeerstattung deutlich hinausgeht und so als hoheitliche Befugnis zu qualifizieren ist. Durch die in Frage stehende Meldepflicht erfolgt aber gerade keine systematische Aufklärung und auch kein Handeln im Quasi-Hoheitsverhältnis, sondern lediglich eine erste Rechtswidrigkeitseinschätzung auf Basis bekannt gewordener Tatsachen; besondere Aufklärungsbefugnisse überträgt das Gesetz den Dienstanbietern hingegen nicht.

Gegen eine mit Art. 33 Abs. 4 GG nicht vereinbare Übertragung spricht zudem dessen Telos, nachdem v. a. das Berufsbeamtentum als Institution geschützt werden soll,[45] da Beamte sich durch besondere Qualifikation auszeichnen würden und somit der Grundsatz der Gesetzmäßigkeit der Verwaltung gesichert wird.[46] In der hier diskutierten Ausgestaltung der Meldepflicht liegt das eigentliche Strafverfahren jedoch weiterhin in den Händen des Staates und auch die Initiierung der Strafverfolgung, beispielsweise durch Gewinnung eines Anfangsverdachts, wird hier nicht vollends auf Private übertragen. Mit anderen Worten: Der Staat gibt vorliegend kein wesentliches Stück seiner Herrschaftsgewalt über das Strafverfahren an Private ab, sodass eine Verfassungswidrigkeit der Meldepflicht wegen Verstoß gegen Art. 33 Abs. 4 GG ausscheidet.

7 Fazit und Ausblick

Der gegenwärtig vorliegende Referentenentwurf des IT-SiG 2.0 enthält auf den ersten Blick zwar einige sinnvolle Regelungsansätze, wirft in einer Gesamtschau aber mehr Schatten als Licht. Dies vornehmlich auch deshalb, weil verschiedene - für sich genommen grundsätzlich begrüßenswerte - Neuerungen noch nicht zu Ende gedacht scheinen. Die teils erhebliche Kritik am ersten Entwurf aus 2019 – so der Eindruck – ist beim Gesetzgeber bisher offenbar weitestgehend auf „taube Ohren" gestoßen. Die Evaluierung bereits bestehender gesetzlicher Maßnahmen zur IT-Sicherheit in Deutschland ist vor diesem Hintergrund wünschenswerter denn je. Auch sollte deutlich stärker als bisher eine einheitliche europäische Lösung in Sachen IT-Sicherheit angestrebt werden und von nationalen Alleingängen, wie z. B. beim IT-Sicherheitskennzeichen, abgesehen werden. Bestehende EU-Instrumentarien, wie beispielsweise die 5G Toolbox,[47] sowie europäische und internationale technische Normen und Standards bieten hier vielfache Anknüpfungspunkte auch für den deutschen Gesetzgeber.

38 z. B. *BVerfG*, NJW 2016, 1781 (1791ff.) oder *Neuhäuser* in BeckOK PolR Nds NPOG, § 22 Rn. 17 ff.

39 BDI, S. 48.

40 BDI, S. 48.

41 *Heuchemer,* in: BeckOK StGB, § 138 StGB Rn. 1; *Liesching*, Karneval der Jakobiner: „Zum Schutze der Freiheit – Schafft sie ab!", abrufbar unter: https://community.beck.de/2020/01/06/karneval-der-jakobiner-zum-schutze-der-freiheit-schafft-sie-ab (Stand 9.9.2020).

42 Siehe auch Google Stellungnahme zum RefE des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 33 ff., abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_google_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf;jsessionid=9050DB5DB9184037825387727EF98E53.2_cid324?__blob=publicationFile&v=3 (Stand 9.9.2020).

43 *Thiele*, Der Staat 2010, 274 (283 ff.).

44 *Waechter*, NZV 1997, 329 (337); so auch *Scholz*, NJW 1997, 14 f.

45 *Battis* in Sachs/Grundgesetz, Art. 33, Rn. 45.

46 *Thiele* in Der Staat 2010, 274 (288).

47 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (Stand 9.9.2020).